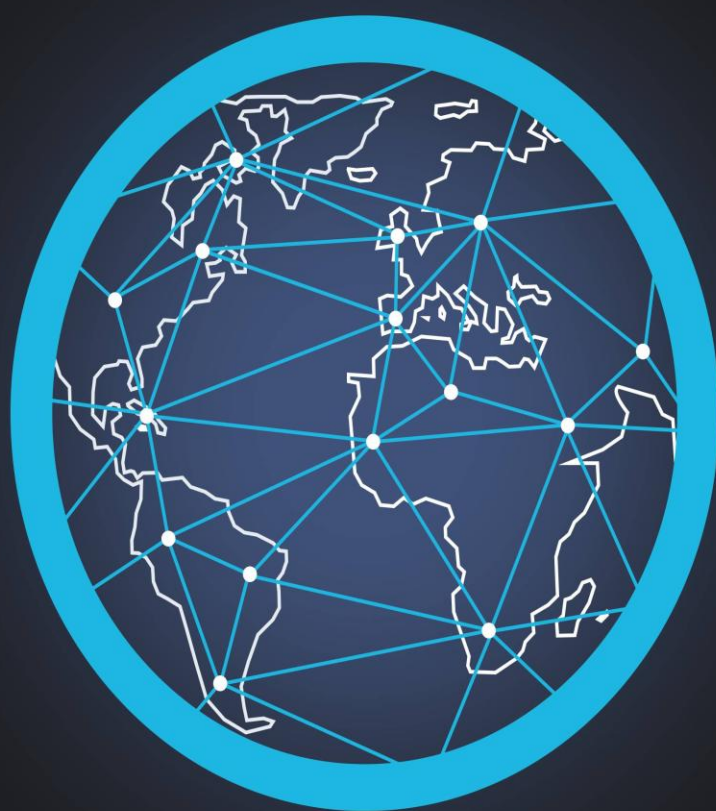


# Международный журнал информационных технологий и энергоэффективности



Том 10 Номер 7(57)



2025



## СОДЕРЖАНИЕ / CONTENT

### ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

1.	<b>Сулимов П.В.</b> Анализ уязвимостей в SMART-контрактах с позиции пентестера	6
	<b>Sulimov P.V.</b> Vulnerability analysis in SMART contracts from a pentester's perspective	
2.	<b>Сулимов П.В.</b> Как GDPR и NIS2 влияют на процессы расследования инцидентов в SOC	10
	<b>Sulimov P.V.</b> How GDPR and NIS2 affect incident investigation processes in SOC	
3.	<b>Сулимов П.В.</b> Оптимизация ФЛАККИ-тестов: методы снижения ложных падений в SELENIUM-фреймворках	14
	<b>Sulimov P.V.</b> Optimization of FLAK tests: methods for reducing false crashes in SELENIUM frameworks	
4.	<b>Вдовченко Г.П.</b> Метод и анализ вредоносных программ	18
	<b>Vdovchenko G.P.</b> Method and analysis of malware	
5.	<b>Вдовченко Г.П.</b> Принципы HARDENING'А ОС: WINDOWS, LINUX и MACOS минимизация поверхности атаки через отключение сервисов, аудит событий и контроль прав пользователей	23
	<b>Vdovchenko G.P.</b> Principles of operating system HARDENING: WINDOWS, LINUX, and MACOS minimizing the attack surface through service disabling, event auditing, and user rights management	
6.	<b>Гаджиев Г.К.</b> Информационная безопасность в промышленном интернете вещей (IOT): специфика угроз на уровне производственных систем	29
	<b>Gadzhiev G.K.</b> Information security in the industrial internet of things (IOT): the specifics of threats at the level of production systems	
7.	<b>Естехина С.С.</b> Повышение лояльности клиентов с помощью искусственного интеллекта	33
	<b>Estekhina S.S.</b> Enhancing customer loyalty through artificial intelligence	
8.	<b>Маркевич Д.В.</b> Анализ и перспективы применения машинного обучения и нейросетевых технологий для защиты информационных систем	42
	<b>Markevich D.V.</b> Analysis and prospects of using machine learning and neural network technologies to protect information systems	
9.	<b>Заозерский А.А.</b> Интеграция DLP и CASB для защиты критически важных данных в облаке	50
	<b>Zaozersky A.A.</b> Integration of DLP and CASB for the protection of critical data in the cloud	

10.	<b>Заозерский А.А.</b> Нейросети в задачах прогнозирования угроз информационной безопасности	<b>54</b>
	<b>Zaozersky A.A.</b> Neural networks in threat prediction for information security	
11.	<b>Заозерский А.А.</b> Методы противодействия фишингу и социальной инженерии в корпоративной среде	<b>58</b>
	<b>Zaozersky A.A.</b> Methods of countering phishing and social engineering in the corporate environment	
12.	<b>Голубкова И.Л., Зеленина Л.И.</b> Искусственный интеллект в моде: влияние искусственного интеллекта на индустрию моды	<b>62</b>
	<b>Golubkova I.L., Zelenina L.I.</b> Artificial intelligence is in fashion: the influence of artificial intelligence on the fashion industry	
13.	<b>Волков М.Д.</b> Архитектура системы выявления и противодействия вредоносным deepfakes	<b>70</b>
	<b>Volkov M.D.</b> Architecture of the system for detecting and countering malicious deepfakes	
14.	<b>Кравцова Е.Ю., Болбаков Р.Г.</b> Адаптивная генерация пользовательского интерфейса с помощью обучения с подкреплением	<b>79</b>
	<b>Kravtsova E.Y., Bolbakov R.G.</b> Adaptive user interface generation using reinforcement learning	
15.	<b>Часов П.С., Маштаков Н.С.</b> Анализ санкционных данных для классификации по странам	<b>85</b>
	<b>Chasov P.S., Mashtakov N.S.</b> Analysis of sanctions data for classification by country	
16.	<b>Николенко А.А., Юшков Е.С.</b> Идентификация проблемных областей в использовании элементов искусственного интеллекта для управления сложноструктурированными организационными системами	<b>93</b>
	<b>Nikolenko A.A., Yushkov E.S.</b> Identification of problem areas in the use of artificial intelligence elements for managing complex structured organizational systems	
17.	<b>Васильев Б.А.</b> Атаки с помощью "PROMPT INJECTION" в голосовых LLM: формирование опасных аудио-команд	<b>106</b>
	<b>Vasiliev B.A.</b> PROMPT INJECTION attacks in voice llms: generating dangerous audio commands	
18.	<b>Васильев Б.А.</b> Эксплуатация LATENCY в METABEPC-среде как канал утечки информации	<b>110</b>
	<b>Vasiliev B.A.</b> Exploitation of LATENCY in the METAVERSE environment as an information leakage channel	
19.	<b>Маштаков Н.С., Часов П.С.</b> Сегментация клиентов банка на основе демографических характеристик с применением методов кластеризации	<b>113</b>
	<b>Mashtakov N.S., Chasov P.S.</b> Segmentation of bank clients based on demographic characteristics using clusterization methods	
20.	<b>Кипилова А.</b> Методы прогнозирования посещаемости веб-сайтов: критерии выбора и практические рекомендации	<b>122</b>

	<b>Kipilova A.</b> Web site traffic forecasting methods: selection criteria and practical recommendations	
21.	<b>Васильев Б.А.</b> Оптимизация механизма виртуализации в операционных системах для работы с многозадачными графическими интерфейсами	<b>127</b>
	<b>Vasiliev B.A.</b> Optimization of the virtualization mechanism in operating systems for working with multitasking graphical interfaces	
22.	<b>Соловьев В.А., Мухамеджанов Т.М., Гамируллина Д.Р., Орлова О.Д.</b> Датчики на чипе для диагностики и терапии	<b>131</b>
	<b>Soloviev V.A., Mukhamedzhanov T.M., Gamirullina D.R., Orlova O.D.</b> Sensors on a chip for diagnostics and therapy	
<b>ЭНЕРГЕТИКА И ЭНЕРГОЭФФЕКТИВНОСТЬ</b>		
23.	<b>Шаренков А.С., Евстафьев С.С.</b> Сравнительный анализ активной элементной базы, используемой в ячейках тракта обработки сигнала для оптоэлектронных преобразователей	<b>144</b>
	<b>Sharenkov A.S., Evstafyev S.S.</b> Comparative analysis of the active element base used in signal processing cells for optoelectronic converters	
24.	<b>Роботко А.А.</b> Интеграция водородных комплексов с АЭС: использование избыточной мощности на примере Кольской АЭС	<b>153</b>
	<b>Robotko A.A.</b> Integration of hydrogen complexes with nuclear power plants: using excess capacity on the example of the Kola NPP	
25.	<b>Капланович Л.А.</b> ENERGIEWENDE: парадоксы немецкого энергоперехода	<b>166</b>
	<b>Kaplanovich L.A.</b> ENERGIEWENDE: the paradoxes of the german energy transition	
26.	<b>Мамаев Ю.А.</b> Принципы и сценарии двухкомпонентной ядерной энергетики	<b>172</b>
	<b>Mamaev Yu.A.</b> Principles and scenarios of two-component nuclear power	
27.	<b>Калёнов А.Д., Сурков А.И.</b> Разработка схемы сброса по технологии КМОП 180 НМ	<b>184</b>
	<b>Kalenov A.D., Surkov A.I.</b> Development of a power on reset scheme 180 NM CMOS technology	
<b>ПРОМЫШЛЕННАЯ БЕЗОПАСНОСТЬ</b>		
28.	<b>Пасечник В.С.</b> Проблемы коммутации и проектирования системы управления погружным подводным мобильным роботом, конфигурация адаптивного управления под задачи инспекции труднодоступных подводных районов	<b>192</b>
	<b>Pasechnik V.S.</b> Challenges of control system design and switching for an underwater mobile submersible robot: adaptive control configuration for inspection of hard-to-reach subaquatic areas	
29.	<b>Акчурин И.А., Мокряк А.В.</b> Экологическая оценка эффективности очистных сооружений водоканала: сравнительный анализ химических и бактериологических показателей до и после очистки	<b>202</b>
	<b>Akchurin I.A., Mokryak A.V.</b> Ecological assessment of the efficiency of water treatment plants: comparative analysis of chemical and bacteriological indicators before and after cleaning	



---

30.	<b>Акчурин И.А., Мокряк А.В.</b> Экологические аспекты повторного использования очищенных сточных вод в системах водоканала: возможности и ограничения	<b>208</b>
-----	--	------------

**Akchurin I.A., Mokryak A.V.** Ecological aspects of the reuse of treated wastewater in water channel systems: opportunities and limitations

---



Международный журнал информационных технологий и энергоэффективности

Сайт журнала:

<http://www.openaccessscience.ru/index.php/ijcse/>



УДК 004.056

## АНАЛИЗ УЯЗВИМОСТЕЙ В SMART-КОНТРАКТАХ С ПОЗИЦИИ ПЕНТЕСТЕРА

**Сулимов П.В.**

ФГБОУ ВО САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФЕССОРА М. А. БОНЧ-БРУЕВИЧА, Санкт-Петербург, Россия (193232, г. Санкт-Петербург, просп. Большевиков, 22, корп. 1), e-mail: [wrk.pa.su@gmail.com](mailto:wrk.pa.su@gmail.com)

С ростом популярности блокчейн-технологий и децентрализованных приложений (dApps) всё больше внимания уделяется безопасности smart-контрактов. Эти автономные программы, выполняющиеся в блокчейне, могут содержать критические уязвимости, приводящие к утрате миллионов долларов. В данной статье рассматриваются наиболее распространённые типы уязвимостей в smart-контрактах, методы их выявления с позиции пентестера, а также принципы разработки безопасного кода. Обсуждаются реальные кейсы взломов, инструменты анализа, и подходы к автоматизации аудита безопасности.

Ключевые слова: Smart-контракты, блокчейн, уязвимости, аудит безопасности, pentest, solidity, dApps, эксплойты, безопасность Ethereum.

## VULNERABILITY ANALYSIS IN SMART CONTRACTS FROM A PENTESTER'S PERSPECTIVE

**Sulimov P.V.**

ST. PETERSBURG STATE UNIVERSITY OF TELECOMMUNICATIONS NAMED AFTER PROFESSOR M. A. BONCH-BRUEVICH, St. Petersburg, Russia (193232, St. Petersburg, ave. Bolshhevikov, 22, bldg. 1), e-mail: [wrk.pa.su@gmail.com](mailto:wrk.pa.su@gmail.com)

With the growing popularity of blockchain technologies and decentralized applications (dApps), increasing attention is being paid to the security of smart contracts. These autonomous programs running on the blockchain may contain critical vulnerabilities that can lead to the loss of millions of dollars. This article reviews the most common types of vulnerabilities in smart contracts, methods for identifying them from a pentester's perspective, and principles for writing secure code. It also explores real-world hacking cases, analysis tools, and approaches to automating security auditing.

Keywords: Smart contracts, blockchain, vulnerabilities, security audit, pentest, solidity, dApps, exploits, Ethereum security.

### Введение

С момента появления технологии блокчейн и децентрализованных приложений концепция smart-контрактов произвела настоящую революцию в сфере цифровых финансов, логистики, управления идентификацией и даже искусства. Эти контракты — автономные фрагменты кода, выполняемые в блокчейне, — обеспечивают выполнение логики программ без участия третьей стороны. Однако с ростом их популярности стало очевидно, что безопасность smart-контрактов — это не просто вопрос надёжного программирования, а одна из самых критичных проблем всей индустрии Web3.

В отличие от традиционных серверных приложений, smart-контракты обладают рядом особенностей: они неизменяемы после деплоя, открыты для всех пользователей, и часто управляют крупными объёмами криптовалюты. Даже небольшая ошибка в коде может привести к катастрофическим последствиям, как это уже происходило неоднократно — DAO, Parity Wallet, bZx и другие стали печально известными примерами того, как один баг может стоить миллионы долларов.

Пентестер, работающий в контексте Web3, сталкивается с уникальными задачами. Его цель — не просто проверить безопасность веб-приложения или API, а оценить устойчивость кода, который не может быть изменён после загрузки в блокчейн. В этой статье мы рассмотрим подход к анализу уязвимостей smart-контрактов глазами пентестера: какие ошибки совершают разработчики, как их искать, какие инструменты использовать, и как минимизировать риски при разработке контрактов.

### **Анализ уязвимостей в smart-контрактах с позиции пентестера**

Анализ уязвимостей smart-контрактов требует комплексного подхода, сочетающего ручной аудит, автоматический анализ, тестирование и знание архитектуры децентрализованных приложений. В отличие от традиционного пентеста, в Web3 нельзя положиться на модели защиты perimetric security или политики контроля доступа — вся логика уже внутри контракта, и если она ошибочна, никакие внешние защиты не помогут[1].

Наиболее частыми уязвимостями smart-контрактов остаются повторное вхождение (reentrancy), арифметические переполнения и недостаточная проверка условий выполнения. Например, атака повторного вхождения, прославившаяся на примере DAO в 2016 году, эксплуатирует возможность повторного вызова контракта до завершения предыдущей операции. Пентестеру важно проверить каждую функцию, отправляющую средства, и удостовериться, что порядок операций не позволяет такому поведению. Это достигается как статическим анализом, так и эмуляцией атаки в среде вроде Hardhat или Ganache[2].

Кроме reentrancy, широко распространены ошибки, связанные с неверным использованием типа tx.origin вместо msg.sender, что позволяет злоумышленникам подменить инициатора вызова и провести атаки через промежуточные контракты. Отдельного внимания заслуживают арифметические ошибки, особенно до внедрения SafeMath по умолчанию в новых версиях Solidity. Несмотря на то, что компилятор теперь отслеживает переполнения, во многих старых контрактах эта проблема остаётся актуальной[3].

Важным аспектом анализа является понимание бизнес-логики контракта. Нередко уязвимости возникают не на уровне кода, а в логике распределения средств или механизма голосования. Пентестеру необходимо моделировать сценарии использования контракта, включая недобросовестное поведение, попытки манипуляции параметрами или таймингом транзакций (например, front-running)[4].

Современные инструменты помогают автоматизировать часть аудита. Среди них наиболее популярны Mythril, Slither, Oyente и Manticore. Они позволяют выявлять потенциальные уязвимости и предоставляют отчёты, но не заменяют ручной анализ. Профессиональный пентестер всегда проверит критические участки вручную: наличие уязвимых delegatecall, открытых selfdestruct, неконтролируемых fallback-функций и логики хранения критических данных. Отдельно стоит упомянуть про fuzzing — метод случайной

генерации входных данных, позволяющий выявить сбои и непредвиденное поведение контракта[5].

Особое внимание уделяется вопросам приватности: несмотря на иллюзию анонимности в блокчейне, весь код и все транзакции публичны. Это открывает поле для анализа поведения пользователей и последующего таргетинга. Пентестер может исследовать, нет ли в контракте утечек данных, например, логов, содержащих приватную информацию, или открытых переменных, которые позволяют сторонним наблюдателям предугадывать поведение контракта.

Реальные кейсы, такие как атака на bZx с использованием flash loan, демонстрируют, насколько комплексными могут быть угрозы. Там атака не касалась конкретной уязвимости в коде, а была результатом комбинирования легитимных возможностей контракта в цепочку, которая позволила злоумышленнику вывести средства. Это подчёркивает важность моделирования угроз и анализа всей архитектуры dApp, а не только самого контракта.

Помимо анализа уязвимостей, пентестеру важно предложить рекомендации: использовать шаблоны надёжного кода (например, OpenZeppelin), ограничивать права доступа (через модификаторы onlyOwner, require, AccessControl), внедрять паузы (circuit breakers), а также логировать критические действия для последующего аудита.

Закаливание смарт-контрактов — это процесс, требующий как технической экспертизы, так и глубокого понимания угроз. Хороший пентестер работает не только на уровне байткода, но и с учётом пользовательских сценариев, поведения внешних контрактов, сетевых особенностей Ethereum и Layer-2 решений.

## **Заключение**

Анализ уязвимостей в smart-контрактах — одна из самых сложных и ответственных задач в современном мире информационной безопасности. Ошибки здесь стоят дорого: одна уязвимость может обернуться миллионами долларов потерь, подорванным доверием к проекту и юридическими последствиями. Работа пентестера в Web3 требует не только технической подготовки, но и гибкости мышления, способности мыслить как злоумышленник и видеть цепочки атаки там, где большинство видит просто код.

Развитие инструментов аудита, таких как Slither и Mythril, делает процесс эффективнее, но не заменяет ручного анализа. Понимание архитектуры блокчейна, особенностей EVM, уязвимостей бизнес-логики и межконтрактных взаимодействий — всё это должно быть в арсенале каждого специалиста. Чем раньше проводится аудит — тем выше шанс, что проект не станет жертвой эксплойта.

Безопасность smart-контрактов начинается с осознанной разработки, но продолжается на этапе аудита и пентеста. Эта статья демонстрирует, как можно подойти к анализу таких контрактов с позиции пентестера, чтобы обеспечить защиту пользовательских средств, доверие к продукту и устойчивость к атакам в постоянно развивающейся экосистеме Web3.

## **Список литературы**

1. Красов А. В., Сахаров Д. В., Тасюк А. А. Проектирование системы обнаружения вторжений для информационной сети с использованием больших данных //Научные технологии в космических исследованиях Земли. – 2020. – Т. 12. – №. 1. – С. 70-76.

2. Миняев А. А. Метод оценки эффективности системы защиты информации территориально-распределенных информационных систем персональных данных //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2020). – 2020. – С. 716-719.
3. Чмутов М. В. и др. Исследование действующей ИТ-инфраструктуры организации для последующего перехода к облачной архитектуре //Информационная безопасность регионов России (ИБРР-2017). Материалы конференции. – 2017. – С. 535-537.
4. Петрова Т. В. и др. Подходы обнаружения беспроводной точки доступа злоумышленника в локальной вычислительной сети //Региональная информатика (РИ-2022). – 2022. – С. 572-573.
5. Казанцев А. А., Прохоров М. В., Худякова П. С. Обзор подходов к классификации текстов актуальными методами //Экономика и качество систем связи. – 2021. – №. 1 (19). – С. 57-67.

## References

1. Krasov A.V., Sakharov D. V., Tasyuk A. A. Designing an intrusion detection system for an information network using big data //High-tech technologies in Earth space research. 2020. – Vol. 12. – No. 1. – pp. 70-76.
  2. Minyaev A. A. A method for evaluating the effectiveness of an information security system geographically distributed personal data information systems //Actual problems of infotelec communications in science and education (APINO 2020), 2020, pp. 716-719.
  3. Chmutov M. V. and others. A study of the current IT infrastructure of an organization for the subsequent transition to a cloud architecture //Information security of the regions of Russia (IBRD-2017). Conference materials. 2017. pp. 535-537.
  4. Petrova T. V. et al. Approaches to detecting an attacker's wireless access point on a local computer network //Regional Informatics (RI-2022). – 2022. – pp. 572-573.
  5. Kazantsev A. A., Prokhorov M. V., Khudyakova P. S. Review of approaches to text classification by current methods //Economics and quality of communication systems. – 2021. – №. 1 (19). – pp. 57-67.
-



Международный журнал информационных технологий и  
энергоэффективности

Сайт журнала:

<http://www.openaccessscience.ru/index.php/ijcse/>



УДК 004.056

## КАК GDPR И NIS2 ВЛИЯЮТ НА ПРОЦЕССЫ РАССЛЕДОВАНИЯ ИНЦИДЕНТОВ В SOC

**Сулимов П.В.**

ФГБОУ ВО САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ  
ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФЕССОРА М. А. БОНЧ-БРУЕВИЧА, Санкт-Петербург,  
Россия (193232, г. Санкт-Петербург, просп. Большевиков, 22, корп. 1), e-mail:  
[wrk.pa.su@gmail.com](mailto:wrk.pa.su@gmail.com)

В статье рассматривается влияние современных регуляторных требований, таких как Общий регламент по защите данных (GDPR) и Директива по безопасности сетей и информации (NIS2), на процессы расследования инцидентов в центрах безопасности (SOC). Анализируются ключевые изменения в подходах к сбору, обработке и хранению данных, а также их влияние на скорость и эффективность реагирования на киберугрозы. Особое внимание уделяется вопросам соответствия нормативным требованиям и оптимизации рабочих процессов в SOC. Рассматриваются практические кейсы внедрения новых процедур, оценивается их эффективность и предлагаются рекомендации по адаптации существующих методик расследования к новым регуляторным реалиям.

Ключевые слова: GDPR, NIS2, SOC, расследование инцидентов, кибербезопасность, соответствие требованиям, защита данных, нормативные документы.

## HOW GDPR AND NIS2 AFFECT INCIDENT INVESTIGATION PROCESSES IN SOC

**Sulimov P.V.**

ST. PETERSBURG STATE UNIVERSITY OF TELECOMMUNICATIONS NAMED AFTER  
PROFESSOR M. A. BONCH-BRUEVICH, St. Petersburg, Russia (193232, St. Petersburg, ave.  
Bolshevikov, 22, bldg. 1), e-mail: [wrk.pa.su@gmail.com](mailto:wrk.pa.su@gmail.com)

The article examines the impact of modern regulatory requirements, such as the General Data Protection Regulation (GDPR) and the Network and Information Security Directive (NIS2), on incident investigation processes in Security Operations Centers (SOC). Key changes in data collection, processing, and storage approaches are analyzed, along with their impact on the speed and efficiency of cyber threat response. Special attention is paid to compliance issues and workflow optimization in SOC. The study includes practical implementation cases of new procedures, evaluates their effectiveness and provides recommendations for adapting existing investigation methodologies to new regulatory realities.

Keywords: GDPR, NIS2, SOC, incident investigation, cybersecurity, compliance, data protection, regulatory frameworks.

### Введение

Современные центры безопасности (SOC) сталкиваются с беспрецедентным давлением со стороны регуляторов, требующих соблюдения постоянно ужесточающихся норм защиты данных и информационной безопасности. Введение GDPR в 2018 году и обновление директивы NIS до NIS2 в 2022 году создали принципиально новые условия работы для специалистов по кибербезопасности. Эти нормативные акты не просто добавили новые обязательства для организаций, но и кардинально изменили сам подход к построению

процессов расследования инцидентов, которые являются ключевой функцией любого современного SOC.

GDPR, изначально разработанный для защиты персональных данных граждан ЕС, фактически стал глобальным стандартом, влияющим на компании по всему миру. Его требования к прозрачности обработки данных, обязательности уведомлений о нарушениях и правам субъектов данных создали новые вызовы для процессов расследования. NIS2, в свою очередь, расширил сферу регулирования, включив в нее большее количество организаций из различных секторов экономики, и ужесточил требования к их способности предотвращать, обнаруживать и реагировать на кибератаки.

Особую сложность представляет необходимость соблюдения требований обоих регуляторных документов одновременно, что зачастую приводит к возникновению противоречий в рабочих процессах SOC. Например, требование GDPR о минимизации данных может конфликтовать с необходимостью NIS2 сохранять подробные логи для расследования сложных атак. Эти противоречия требуют тщательного анализа и разработки сбалансированных решений, что становится одной из ключевых задач современных специалистов по кибербезопасности.

### **Как GDPR и NIS2 влияют на процессы расследования инцидентов в SOC**

Реализация требований GDPR и NIS2 потребовала от SOC фундаментального пересмотра традиционных подходов к расследованию инцидентов. Одним из наиболее заметных изменений стало внедрение принципа "privacy by design" в процессы сбора и анализа данных. Теперь на этапе проектирования систем мониторинга необходимо заранее предусматривать механизмы защиты персональных данных, что существенно усложняет архитектуру SOC. Например, многие организации были вынуждены внедрять системы динамической маскировки данных, которые автоматически скрывают персональную информацию в логах и отчетах, сохраняя при этом их аналитическую ценность [1].

Требование GDPR о 72-часовом сроке уведомления регуляторов о нарушениях создало необходимость разработки новых методологий экспресс-анализа инцидентов. В ответ на этот вызов многие SOC разработали многоуровневые системы классификации инцидентов, где первоначальная оценка проводится по упрощенной методике в течение первых часов после обнаружения, а затем уточняется по мере получения дополнительных данных. Такой подход позволяет соблюсти регуляторные сроки, не жертвуя качеством расследования. Однако он требует значительных ресурсов для обучения персонала и может приводить к увеличению количества ложных срабатываний на начальных этапах анализа [2].

NIS2 ввел принципиально новые требования к взаимодействию SOC с национальными органами кибербезопасности. Теперь для определенных категорий инцидентов необходимо не только проводить внутреннее расследование, но и обеспечивать прозрачность процесса для внешних аудиторов. Это привело к появлению новых должностей в составе SOC - специалистов по регуляторному соответствию, которые выступают связующим звеном между техническими специалистами и надзорными органами. Их работа включает подготовку специальных версий отчетов, адаптированных для не технических специалистов, и организацию процедур совместного расследования [3].

Особую сложность представляет требование GDPR о праве субъектов данных на забвение в контексте расследования инцидентов. В случаях, когда персональные данные



фигурируют в материалах расследования, SOC сталкиваются с дилеммой: сохранить полную информацию для возможных будущих расследований или выполнить требование о удалении данных. Некоторые организации решают эту проблему путем разработки специальных политик хранения, где данные автоматически анонимизируются по истечении определенного срока, но при этом сохраняются ключевые параметры инцидента, важные для аналитики угроз [4].

Автоматизация процессов расследования стала не просто инструментом повышения эффективности, а необходимостью для соответствия требованиям как GDPR, так и NIS2. Современные SOC активно внедряют системы машинного обучения для первичной классификации инцидентов, что позволяет сократить время реакции и уменьшить нагрузку на аналитиков. Однако это создает новые вызовы с точки зрения объяснимости принимаемых решений, особенно в контексте регуляторных проверок. Разработка "объяснимых" алгоритмов ИИ, чьи решения могут быть легко интерпретированы как техническими специалистами, так и регуляторами, становится новым направлением развития технологий для SOC [5].

Требования NIS2 к регулярному тестированию систем защиты привели к появлению нового типа инцидентов - "плановых" инцидентов, возникающих в ходе учебных тревог и тестов на проникновение. Их расследование требует таких же ресурсов, как и работа с реальными угрозами, но при этом должно четко отделяться в отчетности. Это потребовало создания параллельных систем документирования и новых протоколов разграничения реальных и учебных событий, что значительно усложнило инфраструктуру современных SOC.

### **Заключение**

Анализ влияния GDPR и NIS2 на процессы расследования инцидентов в SOC показывает, что современные регуляторные требования создают как значительные вызовы, так и новые возможности для развития центров безопасности. С одной стороны, они существенно увеличили бюрократическую нагрузку и потребовали значительных инвестиций в модернизацию инфраструктуры. С другой - привели к стандартизации процессов, повышению прозрачности и, как следствие, к улучшению общего уровня кибербезопасности.

Ключевым трендом становится интеграция требований регуляторов в архитектуру SOC на этапе проектирования, а не как дополнительный слой контроля. Это требует тесного взаимодействия между юристами, специалистами по соответствию и техническими экспертами на всех этапах разработки и внедрения систем безопасности. Будущее расследования инцидентов, по-видимому, будет связано с дальнейшей автоматизацией, разработкой интеллектуальных систем поддержки принятия решений и созданием унифицированных стандартов отчетности, удовлетворяющих как оперативные потребности SOC, так и регуляторные требования.

### **Список литературы**

1. Красов А. В., Сахаров Д. В., Тасюк А. А. Проектирование системы обнаружения вторжений для информационной сети с использованием больших данных //Наукоемкие технологии в космических исследованиях Земли. – 2020. – Т. 12. – №. 1. – С. 70-76.
2. Миняев А. А. Метод оценки эффективности системы защиты информации территориально-распределенных информационных систем персональных данных

//Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2020). – 2020. – С. 716-719.

3. Чмутов М. В. и др. Исследование действующей ИТ-инфраструктуры организации для последующего перехода к облачной архитектуре //Информационная безопасность регионов России (ИБРР-2017). Материалы конференции. – 2017. – С. 535-537.
4. Петрова Т. В. и др. Подходы обнаружения беспроводной точки доступа злоумышленника в локальной вычислительной сети //Региональная информатика (РИ-2022). – 2022. – С. 572-573.
5. Казанцев А. А., Прохоров М. В., Худякова П. С. Обзор подходов к классификации текстов актуальными методами //Экономика и качество систем связи. – 2021. – №. 1 (19). – С. 57-67.

## References

1. Krasov A.V., Sakharov D. V., Tasyuk A. A. Designing an intrusion detection system for an information network using big data //High-tech technologies in Earth space research. 2020. – Vol. 12. – No. 1. – pp. 70-76.
  2. Minyaev A. A. A method for evaluating the effectiveness of an information security system geographically distributed personal data information systems //Actual problems of infotelec communications in science and education (APINO 2020), 2020, pp. 716-719.
  3. Chmutov M. V. and others. A study of the current IT infrastructure of an organization for the subsequent transition to a cloud architecture //Information security of the regions of Russia (IBRD-2017). Conference materials. 2017. pp. 535-537.
  4. Petrova T. V. et al. Approaches to detecting an attacker's wireless access point on a local computer network //Regional Informatics (RI-2022). – 2022. – pp. 572-573.
  5. Kazantsev A. A., Prokhorov M. V., Khudyakova P. S. Review of approaches to text classification by current methods //Economics and quality of communication systems. – 2021. – №. 1 (19). – pp. 57-67.
-



Международный журнал информационных технологий и  
энергоэффективности

Сайт журнала:

<http://www.openaccessscience.ru/index.php/ijcse/>



УДК 004.4: 004.43: 004.05

## ОПТИМИЗАЦИЯ ФЛАККИ-ТЕСТОВ: МЕТОДЫ СНИЖЕНИЯ ЛОЖНЫХ ПАДЕНИЙ В SELENIUM-ФРЕЙМВОРКАХ

**Сулимов П.В.**

ФГБОУ ВО САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ  
ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФЕССОРА М. А. БОНЧ-БРУЕВИЧА, Санкт-Петербург,  
Россия (193232, г. Санкт-Петербург, просп. Большевиков, 22, корп. 1), e-mail:  
[wrk.pa.su@gmail.com](mailto:wrk.pa.su@gmail.com)

Флакки-тесты представляют собой одну из наиболее значимых проблем в области автоматизированного тестирования программного обеспечения. Их нестабильное поведение, проявляющееся в случайных успехах и падениях при идентичных условиях выполнения, существенно снижает эффективность процессов непрерывной интеграции и доставки (CI/CD). Особенно остро эта проблема проявляется при использовании Selenium-фреймворков для тестирования веб-приложений, где множество внешних факторов может влиять на стабильность тестов. В данной статье подробно рассматриваются современные методы борьбы с флакки-тестами, включая усовершенствованные подходы к работе с локаторами, интеллектуальные системы ожидания, передовые практики обработки асинхронных операций и инновационные стратегии повторного выполнения тестов. Особое внимание уделяется практическим аспектам внедрения этих методов в реальные проекты, а также анализу их эффективности на различных типах веб-приложений.

Ключевые слова: Флакки-тесты, Selenium WebDriver, автоматизированное тестирование веб-приложений, ложные срабатывания, стабильность тестов, непрерывная интеграция.

## OPTIMIZATION OF FLAK TESTS: METHODS FOR REDUCING FALSE CRASHES IN SELENIUM FRAMEWORKS

**Sulimov P.V.**

ST. PETERSBURG STATE UNIVERSITY OF TELECOMMUNICATIONS NAMED AFTER  
PROFESSOR M. A. BONCH-BRUEVICH, St. Petersburg, Russia (193232, St. Petersburg, ave.  
Bolshevikov, 22, bldg. 1), e-mail: [wrk.pa.su@gmail.com](mailto:wrk.pa.su@gmail.com)

Flaky tests constitute one of the most significant challenges in software automated testing. Their unstable behavior, manifested in random successes and failures under identical execution conditions, significantly reduces the efficiency of continuous integration and delivery (CI/CD) processes. This problem is particularly acute when using Selenium frameworks for web application testing, where numerous external factors can affect test stability. This article provides a comprehensive examination of modern methods for combating flaky tests, including advanced approaches to locator handling, intelligent waiting systems, best practices for asynchronous operations processing, and innovative test retry strategies. Special attention is paid to practical aspects of implementing these methods in real projects, as well as analyzing their effectiveness across different types of web applications.

Keywords: Flaky tests, Selenium WebDriver, web application automated testing, false positives, test stability, continuous integration.

### Введение

В современной практике разработки программного обеспечения автоматизированное тестирование стало неотъемлемой частью жизненного цикла продукта. Среди множества инструментов для автоматизации тестирования веб-приложений Selenium WebDriver занимает

лидирующие позиции благодаря своей универсальности, открытости и широким возможностям интеграции с различными языками программирования и фреймворками. Однако вместе с преимуществами Selenium приносит и характерные проблемы, среди которых флакки-тесты представляют особую сложность.

Флакки-тесты - это тесты, которые демонстрируют недетерминированное поведение, периодически завершаясь то успешно, то с ошибкой при выполнении на идентичном коде без каких-либо изменений. Согласно исследованиям крупных IT-компаний, доля таких тестов в общем наборе может достигать 15-20%, что приводит к значительным временным затратам на анализ ложных падений и повторные запуски. В условиях CI/CD, где скорость обратной связи критически важна, наличие флакки-тестов может серьезно замедлить весь процесс разработки и снизить доверие команды к системе автоматизированного тестирования в целом.

Проблема усугубляется тем, что причины нестабильности тестов в Selenium могут быть чрезвычайно разнообразны: от временных задержек при загрузке страниц и динамического изменения DOM до особенностей работы JavaScript в разных браузерах и проблем с синхронизацией в распределенных системах. Все это делает поиск эффективных методов борьбы с флакки-тестами актуальной задачей для сообщества автоматизаторов тестирования.

В данной статье мы проведем глубокий анализ природы флакки-тестов в контексте S-фреймворков, систематизируем основные причины их возникновения и предложим комплекс практических методов для повышения стабильности тестового набора. Особое внимание будет уделено не только техническим аспектам реализации, но и методологическим подходам к организации процесса тестирования, позволяющим минимизировать появление новых нестабильных тестов в проекте.

### **Оптимизация флакки-тестов: методы снижения ложных падений в Selenium-фреймворках**

Первым и наиболее важным шагом в борьбе с флакки-тестами является понимание их природы и классификация по основным типам. В контексте Selenium-тестирования можно выделить несколько категорий нестабильных тестов: тесты, чувствительные к времени выполнения; тесты, зависящие от порядка выполнения; тесты с неявными зависимостями от состояния системы; тесты, подверженные проблемам синхронизации; и тесты, зависящие от внешних сервисов. Каждая из этих категорий требует своего подхода к оптимизации и стабилизации [1].

Одним из фундаментальных аспектов создания стабильных Selenium-тестов является правильная работа с локаторами элементов. Традиционно многие автоматизаторы используют XPath-выражения, которые, будучи чрезмерно детализированными, часто ломаются при малейших изменениях в структуре страницы. Более надежным подходом является применение CSS-селекторов, основанных на стабильных атрибутах элементов, таких как data-test-id или другие специально добавленные для тестирования идентификаторы. Современные практики рекомендуют реализовывать стратегию "теговых атрибутов", когда разработчики фронтенда специально помечают ключевые элементы атрибутами, предназначенными исключительно для автоматизированного тестирования. Это создает четкий контракт между разработчиками и автоматизаторами, значительно повышая стабильность тестов [2].

Проблема временных задержек и синхронизации заслуживает отдельного рассмотрения. Классический подход с использованием Thread.sleep() давно признан антипаттерном в

автоматизированном тестировании, так как приводит либо к избыточному времени выполнения тестов, либо к ложным падениям при недостаточной длительности паузы. Вместо этого следует использовать систему "умных ожиданий", предоставляемую Selenium WebDriver через класс WebDriverWait. Особенно эффективна комбинация явных ожиданий с пользовательскими условиями, позволяющая точно определять момент готовности страницы или элемента к взаимодействию. Например, ожидание можно считать успешным не просто при наличии элемента в DOM, а при достижении им определенного состояния (видимость, кликабельность, наличие конкретного значения и т.д.).

Асинхронная природа современных веб-приложений добавляет дополнительные сложности в процесс тестирования. AJAX-запросы, динамическая подгрузка контента, WebSocket-соединения - все эти технологии могут стать источниками нестабильности тестов. Для надежной работы с такими приложениями необходимо внедрять продвинутые стратегии ожидания, включая: мониторинг активности сетевых запросов через прокси-серверы (например, BrowserMob), отслеживание состояния JavaScript-переменных через executeScript, и анализ логов браузера. Особенно эффективным может быть подход, при котором тест перед выполнением ключевых действий явно дожидается завершения всех фоновых процессов приложения [3].

Одной из современных тенденций в борьбе с флакки-тестами стало применение стратегий повторного выполнения (retry mechanisms). Однако важно понимать, что простое повторение упавшего теста - это лишь симптоматическое лечение, а не решение основной проблемы. Более прогрессивный подход заключается в реализации интеллектуальной системы повторных попыток, которая: анализирует тип ошибки (например, различает проблемы синхронизации от реальных дефектов приложения); использует экспоненциальное увеличение задержек между попытками; ведет подробную статистику по частоте падений; и автоматически помечает для углубленного анализа тесты, требующие слишком много повторных запусков. Такой подход позволяет одновременно снизить влияние флакки-тестов и выявлять те, которые требуют серьезной доработки [4].

Важнейшим, но часто недооцениваемым аспектом стабильности тестов является их изолированность и воспроизводимость. Многие флакки-тесты проявляют нестабильность именно из-за скрытых зависимостей между тестами или от состояния системы. Для решения этой проблемы необходимо: тщательно проектировать систему setup/teardown для каждого теста; использовать транзакционные механизмы для отката изменений в БД; реализовывать механизмы очистки кешей и локального хранилища браузера; и, возможно, даже перезапускать браузер между критически важными тестами. Особое внимание следует уделять тестам, работающим с авторизацией и сессиями пользователей, так как они особенно подвержены проблемам из-за сохранения состояния [5].

## **Заключение**

Проблема флакки-тестов в Selenium-фреймворках требует комплексного подхода, сочетающего технические решения с методологическими практиками. Как показано в статье, ключом к стабильности тестового набора является не какое-то одно "серебряное решение", а система взаимосвязанных мер: от грамотного выбора локаторов и реализации продвинутых стратегий ожидания до построения интеллектуальной системы повторных выполнений и обеспечения полной изолированности тестов.

Особенно важно отметить, что борьба с флакки-тестами - это не разовая акция, а постоянный процесс, требующий внимания на всех этапах жизненного цикла тестирования. Регулярный анализ причин падений, постоянная оптимизация тестового набора, тесное взаимодействие между разработчиками фронтенда и автоматизаторами - все это необходимые компоненты успешной стратегии по минимизации нестабильных тестов.

Внедрение описанных в статье методов позволяет не просто уменьшить количество ложных падений, но и в целом повысить качество автоматизированных тестов, сделать их более надежными, поддерживаемыми и эффективными. В результате команды получают возможность в полной мере использовать преимущества автоматизированного тестирования в процессах CI/CD, ускоряя разработку без потери качества продукта.

### Список литературы

1. Гельфанд А. М. Способы выбора стегоконтейнеров для передачи данных //Региональная информатика и информационная безопасность. – 2020. – С. 260-262
2. Кушнир Д. В. Исследование и разработка методов распределения конфиденциальных данных по квантовым каналам : дис. – Санкт-Петербург. гос. ун-т телекоммуникаций им. МА Бонч-Бруевича, 1996.
3. Леснова Е. М., Пестов И. Е. Разработка метода обнаружения и коррекции ошибок для распределенной информационной сети на основе больших данных //Региональная информатика и информационная безопасность. – 2018. – С. 236-240.
4. Горбань С. А., Красов А. В., Цветков А. Ю. Оценка эффективности механизмов контроля правами доступа в ОС Linux //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2023). – 2023. – С. 345-348
5. Петрова Т. В. и др. Подходы обнаружения беспроводной точки доступа злоумышленника в локальной вычислительной сети //Региональная информатика (РИ-2022). – 2022. – С. 572-573.

### References

1. Gelfand A.M. Ways of choosing stegocontainers for data transmission //Regional informatics and information security. - 2020. – pp. 260-262
  2. Kushnir D. V. Research and development of methods for distributing confidential data over quantum channels : St. Petersburg State University of Telecommunications named after MA Bonch–Bruevich, 1996.
  3. Lesnova E. M., Pestov I. E. Development of an error detection and correction method for a distributed information network based on big data //Regional informatics and information security. - 2018. – pp. 236-240.
  4. Gorban S. A., Krasov A.V., Tsvetkov A. Yu. Assessment of the effectiveness of access rights control mechanisms in Linux OS //Actual problems of infotelec communications in science and education (APINO 2023). – 2023. – pp. 345-348
  5. Petrova T. V. and others. Approaches to detecting an attacker's wireless access point on a local computer network //Regional Informatics (RI-2022). – 2022. – pp. 572-573.
-



Международный журнал информационных технологий и  
энергоэффективности

Сайт журнала:

<http://www.openaccessscience.ru/index.php/ijcse/>



УДК 004.056.53

## МЕТОД И АНАЛИЗ ВРЕДОНОСНЫХ ПРОГРАММ

**Вдовченко Г.П.**

*ФГБОУ ВО САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФЕССОРА М. А. БОНЧ-БРУЕВИЧА, Санкт-Петербург, Россия (193232, г. Санкт-Петербург, просп. Большевиков, 22, корп. 1), e-mail: vdovchenko2003@gmail.com*

Статья посвящена методам анализа вредоносных программ — статическому и динамическому — и их практическому применению с использованием инструментов Ghidra, IDA Pro и x64dbg. Рассмотрены ключевые особенности каждого подхода: статический анализ позволяет изучать код без его выполнения, выявляя алгоритмы шифрования, сетевые взаимодействия и обфускацию, тогда как динамический анализ фиксирует поведение малвера в реальном времени, включая манипуляции с файловой системой, реестром и сетевыми соединениями. Подробно разобраны возможности Ghidra (декомпиляция в C-подобный код, скриптовая автоматизация), IDA Pro (точный псевдокод с Hex-Rays, анализ сложных структур) и x64dbg (отладка, трассировка вызовов API). Приведены примеры рабочих процессов для анализа ransomware и банковских троянов, а также методы противодействия анти-анализ техникам (детекту виртуальных машин, обфускации). Статья подчёркивает важность комбинированного подхода и интеграции инструментов для эффективного исследования современных киберугроз. Рекомендации включают использование песочниц, эмуляторов и открытых баз данных. Материал адресован специалистам по кибербезопасности, исследователям малвера и IT-энтузиастам.

Ключевые слова: Статический анализ, динамический анализ, вредоносные программы, Ghidra, IDA Pro, x64dbg, реверс-инжиниринг, кибербезопасность, анти-анализ техники, обфускация кода, декомпиляция, отладка, ransomware, песочница, C&C-серверы.

## METHOD AND ANALYSIS OF MALWARE

**Vdovchenko G.P.**

*ST. PETERSBURG STATE UNIVERSITY OF TELECOMMUNICATIONS NAMED AFTER PROFESSOR M. A. BONCH-BRUEVICH, St. Petersburg, Russia (193232, St. Petersburg, ave. Bolshevnikov, 22, bldg. 1), e-mail: vdovchenko2003@gmail.com*

This article explores methods for analyzing malicious software—specifically static and dynamic analysis—and their practical application using tools such as Ghidra, IDA Pro, and x64dbg. It outlines the key features of each approach: static analysis enables code inspection without execution, helping to identify encryption algorithms, network communication, and obfuscation techniques, while dynamic analysis captures real-time malware behavior, including file system changes, registry modifications, and network activity. The article details Ghidra's capabilities (decompilation into C-like code, scripting automation), IDA Pro's strengths (accurate pseudocode with Hex-Rays, complex structure analysis), and x64dbg's functionality (debugging, API call tracing). Practical workflows are provided for investigating ransomware and banking trojans, along with strategies to bypass anti-analysis techniques such as virtual machine detection and code obfuscation. The article emphasizes the importance of combining both analysis methods and integrating tools for effective investigation of modern cyber threats. Recommendations include the use of sandboxes, emulators, and open-source threat intelligence databases. The material is intended for cybersecurity professionals, malware researchers, and IT enthusiasts.

Keywords: Static analysis, dynamic analysis, malware, Ghidra, IDA Pro, x64dbg, reverse engineering, cybersecurity, anti-analysis techniques, code obfuscation, decompilation, debugging, ransomware, sandbox, C&C servers.



## **Введение**

Анализ вредоносных программ стал ключевым направлением в кибербезопасности. Современные угрозы эволюционируют благодаря методам шифрования, полиморфизму и технологиям обхода защиты. По данным SonicWall, в 2023 году было обнаружено более 700 миллионов новых образцов вредоносного ПО. Такая активность требует точных и эффективных методик анализа.

Основой работы специалистов остаются два подхода — статический и динамический анализ. Статический анализ позволяет изучать код без его исполнения, а динамический раскрывает поведение в процессе выполнения.

Практическое применение этих методов возможно с использованием таких инструментов, как Ghidra, IDA Pro и x64dbg. Эти платформы формируют основу арсенала исследователя вредоносного ПО.

## **Статический анализ**

Данный анализ даёт возможность безопасно исследовать структуру вредоносной программы. В инструменте Ghidra это достигается через декомпиляцию бинарного кода в псевдоязык C, что значительно упрощает понимание логики работы. Используя граф вызовов, можно проследить взаимосвязи между функциями, определить точки входа и выявить критические участки кода. Через поиск строк и сигнатур с применением регулярных выражений можно обнаружить встроенные адреса, команды и индикаторы компрометации.

Автоматизация анализа реализуется с помощью скриптов, которые позволяют быстро находить повторяющиеся паттерны. При работе с обфусцированным кодом Ghidra предоставляет возможность выявлять шаблоны шифрования и нестандартные инструкции. Однако у инструмента есть ограничения: декомпилятор не всегда корректно интерпретирует сложные конструкции, а отсутствие встроенного отладчика ограничивает взаимодействие с исполняемым кодом[1].

IDA Pro предлагает более глубокий уровень анализа за счёт встроенного декомпилятора Hex-Rays, способного восстанавливать сложные логические структуры, включая классы и виртуальные таблицы. Распознавание библиотек с помощью сигнатур FLIRT позволяет ускорить разбор кода, особенно при наличии известных компонентов. Плагины расширяют функциональность — например, FindCrypt помогает идентифицировать криптографические алгоритмы, а Keupatch позволяет вносить изменения в код на лету. В IDA Pro удобно анализировать вредонос, взаимодействующий с сетью. Через просмотр вызовов API можно определить наличие функций socket или connect, что может указывать на бэкдор или C&C-коммуникацию. Сценарии на IDA Python позволяют извлекать строки, адреса и другие полезные артефакты. Главными недостатками остаются высокая стоимость лицензии и слабая поддержка альтернативных операционных систем[2].

## **Динамический анализ**

Этим способом мы можем наблюдать за поведением вредоносной программы в контролируемой среде. x64dbg, как один из самых популярных бесплатных отладчиков под Windows, предоставляет широкий функционал. С помощью брейкпоинтов можно перехватывать критические вызовы API, включая работу с файлами, памятью или реестром. Условные и аппаратные точки останова помогают обходить антиотладочные проверки.

Отладчик поддерживает трассировку всех действий, позволяет вести логирование, анализировать память и обнаруживать распакованный код. При исследовании шифровальщика можно установить брейкпоинт на функцию WriteFile, чтобы отследить процесс записи зашифрованных данных. Использование плагинов, таких как ScyllaHide, помогает скрыть наличие отладчика от вредоносного ПО. После выполнения определённого этапа работы, например шифрования, можно сделать дамп памяти и передать его на дальнейший статический анализ. Среди ограничений x64dbg — отсутствие поддержки macOS и Linux, а также невозможность декомпиляции[3].

### **Комбинированный подход**

На практике наибольшую ценность представляет эта практика. Статический анализ позволяет получить общее представление о структуре вредоносной программы, определить точки интереса и выстроить гипотезы. Динамический анализ уточняет поведение, проверяет предположения и помогает зафиксировать данные, недоступные при обычном просмотре кода. Например, при анализе банковского трояна можно в Ghidra найти функции, использующие VirtualAllocEx или WriteProcessMemory, что указывает на внедрение кода. В IDA Pro можно изучить, как реализован перехват ввода или обращение к окнам браузера. После чего в x64dbg наблюдаются попытки установления соединения с внешними IP-адресами, осуществляется дамп памяти, в котором может находиться декодированная конфигурация.

Большинство современных образцов вредоносного ПО используют методы противодействия анализу. Проверки наличия виртуальной среды, например через инструкции CPUID, могут блокировать выполнение. Некоторые программы используют таймеры для определения задержек, вызванных отладкой. Часто встречаются вызовы функций IsDebuggerPresent или CheckRemoteDebuggerPresent. Чтобы обойти эти проверки, используют модифицированные конфигурации гипервизора, физические устройства, а также плагины, скрывающие отладчик. Малверы также часто упакованы средствами вроде UPX, Themida или кастомными упаковщиками, что требует предварительной распаковки. Запуск такого файла в x64dbg и отслеживание вызова функций виртуального выделения памяти позволяет захватить распакованный участок кода. После этого осуществляется дамп памяти, который передаётся на анализ в Ghidra или IDA Pro[4].

### **Примеры декомпиляции на реальном опыте**

Опыт анализа шифровальщика начинается с декомпиляции в Ghidra, где можно найти использование функций CryptGenKey и CryptExportKey. В IDA Pro проводится поиск строк с расширениями файлов или сообщениями выкупа. Затем в x64dbg отслеживаются вызовы FindFirstFileW, что позволяет фиксировать каталоги, в которых осуществляется шифрование. Дополнительно используются инструменты мониторинга вроде Process Monitor для отслеживания изменений в реестре, например, в ветке HKCU\Software\Locked. В завершение анализа из дампа памяти извлекается ключ шифрования или информация о расшифровке.

Развитие технологий постепенно привносит автоматизацию в процесс анализа. Использование нейросетей и моделей машинного обучения ускоряет классификацию угроз и распознавание паттернов. Однако в условиях работы с уникальными, целевыми или нестандартными вредоносными программами только глубокий анализ позволяет понять суть угрозы.

Комбинация инструментов, знание архитектуры операционных систем и умение интерпретировать поведение программ остаются основными навыками аналитика[5].

### **Заключение**

В условиях стремительного роста киберугроз и постоянного появления новых разновидностей вредоносных программ анализ малвера становится неотъемлемой частью работы специалистов в области информационной безопасности. Статья подчёркивает значимость сочетания статических и динамических методов анализа, поскольку только такой подход позволяет максимально полно изучить как структуру вредоносного кода, так и его поведение в реальной среде.

Каждый из рассмотренных инструментов — Ghidra, IDA Pro и x64dbg — имеет свои сильные стороны и ограничения, однако при совместном применении они образуют мощный арсенал аналитика. Ghidra обеспечивает высокую скорость предварительного анализа, IDA Pro раскрывает сложные логические взаимосвязи и упрощает работу с сетевыми функциями, а x64dbg даёт возможность в реальном времени отслеживать вредоносную активность и делать дампы памяти на лету.

Кроме того, анализ противодействующих техник со стороны вредоносного ПО — таких как антиотладка, проверка виртуализации, обфускация и упаковка — остаётся важнейшим направлением исследований, требующим глубоких знаний архитектуры ОС и навыков низкоуровневой отладки.

Таким образом, успешный анализ вредоносных программ требует не только владения современными инструментами, но и системного подхода, постоянного повышения квалификации, обмена опытом и использования открытых источников информации. Только при таком подходе возможно эффективно выявлять, классифицировать и нейтрализовывать угрозы, обеспечивая надёжную защиту информационных систем.

### **Список литературы**

1. Штеренберг С. И. Анализ работы алгоритмов защиты информации на основе самомодифицирующегося кода с применением стеговложения //Научные технологии в космических исследованиях Земли. – 2016. – Т. 8. – №. 2. – С. 86-90.
2. Шемякин С. Н., Ахметшина М. Э., Катасонов А. И. Поиск функций, обладающих наилучшими характеристиками в классе от 4 переменных //Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. – 2020. – №. 4. – С. 61-65.
3. Радынская В. Е., Поляничева А. В., Ахрамева К. А. Разработка метода защиты ядра программных приложений с применением самомодифицирующегося кода //Региональная информатика и информационная безопасность. – 2019. – С. 136-141.
4. Волкогонов В. Н., Гельфанд А. М., Деревянко В. С. Актуальность автоматизированных систем управления //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019). – 2019. – С. 262-266.
5. Гельфанд А. М. и др. Оценка рисков и угроз безопасности в среде «УМНЫЙ ДОМ» //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2020). – 2020. – С. 316-321.

## References

1. Shterenberg S. I. Analysis of the work of information protection algorithms based on a self-modifying code with the use of stegonesting. – 2016. – Т. 8. – №. 2. – pp. 86-90.
  2. Shemyakin S. N., Akhmetshina M. E., Katasonov A. I. Search for functions possessing the best characteristics in a class of 4 variables. Series 1: Natural and Technical Sciences. – 2020. – №. 4. – pp. 61-65.
  3. Radynskaya V. E., Polyanicheva A. V., Akhrameeva K. A. Development of a method for protecting the core of software applications with the use of a self-modifying code. – 2019. – pp. 136-141.
  4. Volkogonov V. N., Gelfand A. M., Derevyanko V. S. Relevance of automated control systems // Actual problems of infotelecommunications in science and education (APINO 2019). – 2019. – pp. 262-266.
  5. Gelfand A. M. et al. Assessment of risks and threats to security in the environment of "SMART HOUSE" // Actual problems of infotelecommunications in science and education (APINO, 2020). – 2020. – pp. 316-321.
-



Международный журнал информационных технологий и  
энергоэффективности

Сайт журнала:

<http://www.openaccessscience.ru/index.php/ijcse/>



УДК 004.056.53

## **ПРИНЦИПЫ HARDENING'А ОС: WINDOWS, LINUX И MACOS МИНИМИЗАЦИЯ ПОВЕРХНОСТИ АТАКИ ЧЕРЕЗ ОТКЛЮЧЕНИЕ СЕРВИСОВ, АУДИТ СОБЫТИЙ И КОНТРОЛЬ ПРАВ ПОЛЬЗОВАТЕЛЕЙ**

**Вдовченко Г.П.**

*ФГБОУ ВО САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ  
ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФЕССОРА М. А. БОНЧ-БРУЕВИЧА, Санкт-Петербург,  
Россия (193232, г. Санкт-Петербург, просп. Большевиков, 22, корп. 1), e-mail:  
vdovchenko2003@gmail.com*

Статья посвящена методам повышения защищённости операционных систем Windows, Linux и macOS посредством применения техник жёсткой настройки (hardening). Особое внимание уделяется практическим шагам по снижению поверхности атаки и укреплению критических компонентов систем. Рассматриваются рекомендации по отключению неиспользуемых служб и протоколов, настройке системного журнала и аудита событий, а также ограничению полномочий пользователей и приложений. Приводятся примеры применения таких инструментов, как Group Policy для Windows, systemd и auditd для Linux, а также System Integrity Protection (SIP) для macOS. Отдельный акцент сделан на важности принципа минимально необходимых привилегий и изоляции процессов. Статья также описывает влияние политики обновлений, контроля доступа и систем мониторинга на общее снижение рисков кибератак. Материал ориентирован на системных администраторов, специалистов по ИБ и IT-архитекторов, стремящихся к созданию устойчивой к угрозам вычислительной среды.

Ключевые слова: Hardening, операционная система, информационная безопасность, Windows, Linux, macOS, аудит, права доступа, systemd, PowerShell, SELinux, SIP, защита системы, поверхность атаки.

## **PRINCIPLES OF OPERATING SYSTEM HARDENING: WINDOWS, LINUX, AND MACOS MINIMIZING THE ATTACK SURFACE THROUGH SERVICE DISABLING, EVENT AUDITING, AND USER RIGHTS MANAGEMENT**

**Vdovchenko G.P.**

*ST. PETERSBURG STATE UNIVERSITY OF TELECOMMUNICATIONS NAMED AFTER  
PROFESSOR M. A. BONCH-BRUEVICH, St. Petersburg, Russia (193232, St. Petersburg, ave.  
Bolshevikov, 22, bldg. 1), e-mail: vdovchenko2003@gmail.com*

The article is devoted to methods for increasing the security of Windows, Linux, and macOS operating systems by using hardening techniques. Particular attention is paid to practical steps to reduce the attack surface and strengthen critical system components. Recommendations for disabling unused services and protocols, configuring the system log and event audit, and limiting the privileges of users and applications are considered. Examples of using tools such as Group Policy for Windows, systemd and auditd for Linux, and System Integrity Protection (SIP) for macOS are given. Particular emphasis is placed on the importance of the principle of least necessary privileges and process isolation. The article also describes the impact of update policies, access control, and monitoring systems on the overall reduction of cyberattack risks. The material is aimed at system administrators, information security specialists, and IT architects seeking to create a threat-resistant computing environment

Keywords: Hardening, operating system, cybersecurity, Windows, Linux, macOS, auditing, access control, systemd, PowerShell, SELinux, SIP, system protection, attack surface.

## **Введение**

Операционные системы по умолчанию поставляются с широким набором функций и служб, предназначенных для обеспечения совместимости, удобства и гибкости. Однако многие из этих компонентов в реальной эксплуатации остаются неиспользуемыми, что превращает их в потенциальные точки уязвимости. Каждый активный сервис, открытый порт или доступная функция — это потенциальная лазейка, которую злоумышленник может использовать для проникновения в систему или повышения своих привилегий.

Hardening, или усиление защиты операционной системы, представляет собой систематический процесс настройки, цель которого — минимизация поверхности атаки. Под этим термином понимается совокупность всех мест, взаимодействие с которыми может привести к компрометации системы: сетевые службы, учетные записи, политики доступа, компоненты ядра, механизмы обновлений и т. д. В условиях увеличивающегося числа атак на инфраструктуру организаций и пользователей особую важность приобретает проактивный подход к безопасности, предполагающий не только реагирование на инциденты, но и предупреждение потенциальных угроз за счёт жёсткой настройки систем.

Настоящая статья фокусируется на практических аспектах hardening'a для трёх наиболее распространённых операционных систем — Windows, Linux и macOS. Рассматриваются конкретные шаги по отключению ненужных служб и компонентов, настройке системы аудита и журналирования, управлению правами пользователей и изоляции процессов. Для каждой платформы приведены соответствующие инструменты и механизмы: Group Policy и Security Templates для Windows, systemd и auditd для Linux, SIP и конфигурации через csrutil для macOS. Дополнительно освещаются методы контроля доступа к критически важным системным файлам, реализация принципа наименьших привилегий и обеспечение защищённого процесса обновления.

Цель статьи — предоставить читателю структурированный обзор подходов к снижению уязвимостей систем и дать практические рекомендации по построению более устойчивой и контролируемой среды эксплуатации. Материал ориентирован на системных администраторов, инженеров по безопасности, DevOps-специалистов и всех, кто отвечает за защиту ИТ-инфраструктуры.

## **Основы Hardening'a**

Hardening — это системный подход к защите операционной системы, основанный на минимизации потенциальных точек входа для злоумышленника. Основу этого процесса составляют три ключевых принципа.

Во-первых, удаление избыточного функционала, включающее отключение неиспользуемых сервисов, портов и протоколов. Это позволяет значительно сократить поверхность атаки.

Во-вторых, необходим мониторинг активности системы с помощью средств аудита, что позволяет своевременно выявлять подозрительные события. И, наконец, важнейшим компонентом является строгое соблюдение принципа наименьших привилегий (POLP), согласно которому каждый пользователь и процесс получают только минимально

необходимые для своей работы права. Соблюдение этих принципов значительно снижает вероятность успешной атаки на систему.

### **Hardening Windows**

В среде Windows практическая реализация hardening начинается с отключения уязвимых и неиспользуемых служб. Для этого применяются такие инструменты, как PowerShell, Group Policy и Services.msc. Например, служба Telnet, известная своей уязвимостью, может быть отключена командой Stop-Service -Name "Telnet" с последующим запретом её автозапуска. Среди других сервисов, подлежащих отключению, — Remote Registry и Windows Remote Management, если они не используются.

Для настройки аудита безопасности используется Local Security Policy (secpol.msc). Настраивается аудит успешных и неудачных попыток входа, а также доступ к системным файлам, включая директорию SAM. Полученные данные анализируются через Event Viewer, где особое внимание уделяется событиям с кодами 4625 (неудачный вход) и 4672 (привилегированный доступ).

Управление правами пользователей осуществляется за счёт создания ограниченных учётных записей и применения списков контроля доступа (ACL), позволяющих, например, запретить доступ к конфиденциальным директориям. Кроме того, рекомендуется внедрение Microsoft LAPS — системы управления паролями локальных администраторов с автоматической ротацией.

### **Hardening Linux**

Безопасность Linux-систем также начинается с минимизации запущенных служб и удаления лишних пакетов. Через systemd можно получить список активных сервисов, а ненужные, такие как FTP-сервер vsftpd, отключить и исключить из автозагрузки. Пакеты, не предназначенные для используемой архитектуры, такие как telnetd и rpcbind, подлежат удалению.

Для аудита используется подсистема auditd, которая позволяет настраивать правила логирования операций. Например, можно отслеживать любые изменения в файле /etc/passwd или фиксировать все действия суперпользователя. Это обеспечивает прозрачность и позволяет выявлять подозрительные сценарии поведения.

В целях ограничения привилегий рекомендуется использовать механизмы SELinux или AppArmor. Эти системы задают политику безопасности, ограничивая выполнение операций вне допустимых рамок. Одной из важных мер является запрет входа под root по SSH, что реализуется через изменение конфигурационного файла sshd\_config.

### **Hardening macOS**

Операционная система macOS также требует мер по усилению защиты. Через launchctl можно управлять системными и пользовательскими службами, отключая, к примеру, AirPlay или SMB, если они не используются. Это снижает возможность удалённого вмешательства и атак по локальной сети.

Аудит системы реализуется с помощью утилиты osquery, которая предоставляет широкие возможности мониторинга сетевых соединений, процессов и системных настроек.



Пример запроса — `SELECT * FROM socket_events WHERE remote_port != 0;` — позволяет получить сведения о текущей сетевой активности.

Фундаментальной защитной технологией в macOS является SIP (System Integrity Protection), ограничивающая возможность изменения системных файлов даже пользователями с root-доступом. Для управления административными правами применяется ограничение на использование `sudo` — только для доверенных групп пользователей. Рекомендуется также включение FileVault для шифрования данных.

### **Универсальные рекомендации**

Независимо от платформы, существуют общие меры повышения устойчивости систем:

- Включение автоматических обновлений безопасности для своевременного устранения уязвимостей;
- Использование встроенных или сторонних брандмауэров:
  - Windows: встроенный Windows Firewall;
  - Linux: `ufw` (Uncomplicated Firewall);
  - macOS: `pfctl`;
- Организация регулярного резервного копирования на изолированные физические носители.

### **Дополнительные аспекты реализации hardening**

Одним из ключевых факторов, усиливающих актуальность hardening-практик, является рост количества целевых атак, направленных на эксплуатацию неправильно настроенных или унаследованных системных компонентов. Согласно отчету IBM X-Force, в 2023 году более 30% инцидентов безопасности были связаны с использованием известных, но не закрытых уязвимостей в системных службах. Это подтверждает необходимость регулярного пересмотра и жёсткой настройки конфигураций.

Кроме технических настроек, важным направлением является интеграция hardening в общую архитектуру защиты. В частности, он должен дополняться использованием антивирусных решений, систем обнаружения вторжений (IDS/IPS), а также систем управления событиями безопасности (SIEM). Например, внедрение hardening на уровне ОС позволяет сократить количество ложных срабатываний в SIEM-системах за счёт уменьшения «шума» от нестандартизированной активности.

В корпоративной среде hardening требует централизованного управления. В Windows широко применяются групповые политики (Group Policy Objects), с помощью которых администратор может внедрять единые настройки безопасности на уровне домена. В Linux возможно использование систем управления конфигурацией, таких как Ansible или Puppet, что позволяет автоматизировать настройку прав, сервисов и политик SELinux на сотнях хостов. В macOS компании всё чаще внедряют решения MDM (Mobile Device Management), такие как Jamf, позволяющие централизованно управлять безопасностью устройств Apple.

Автоматизация играет ключевую роль в поддержании актуальности настроек безопасности. Так, с помощью OpenSCAP можно регулярно проверять соответствие систем установленным политикам, а такие инструменты, как Auditbeat от Elastic, позволяют интегрировать данные аудита в централизованное хранилище событий

### **Заключение**

Hardening Windows, Linux и macOS требует индивидуального подхода, учитывающего архитектурные особенности каждой системы, но при этом базируется на универсальных принципах: минимизация компонентов, контроль доступа и настройка аудита. Важно удалять или отключать все неиспользуемые службы, ограничивать права пользователей и активно применять встроенные средства управления безопасностью.

Для Windows ключевыми инструментами выступают PowerShell, Group Policy и AppLocker, позволяющие реализовать централизованную и гибкую защиту. В Linux основное внимание уделяется systemd, auditd и SELinux, обеспечивающим контроль над процессами и журналированием. В macOS важную роль играют SIP, osquery и контроль расширений ядра.

Независимо от платформы, регулярное обновление программного обеспечения, применение политики минимальных привилегий и системный мониторинг позволяют снизить вероятность успешной атаки. Комплексный подход к hardening-процедурам способствует созданию устойчивой к угрозам среды и повышает общий уровень безопасности информационной инфраструктуры.

### **Список литературы**

1. Волкогонов В. Н., Гельфанд А. М., Карамова М. Р. Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019). – 2019. – С. 266-270.
2. Волкогонов В. Н., Гельфанд А. М., Деревянко В. С. Актуальность автоматизированных систем управления //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019). – 2019. – С. 262-266.
3. Кирилова К. С. и др. Проблема обезвреживания руткитов уровня ядер в системах специального назначения //I-methods. – 2020. – Т. 12. – №. 3. – С. 2.
4. Катасонов А. И., Цветков А. Ю. Анализ механизмов разграничения доступа в системах специального назначения //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2020). – 2020. – С. 563-568.
5. Штеренберг С. И., Москальчук А. И., Красов А. В. Разработка сценариев безопасности для создания уязвимых виртуальных машин и изучения методов тестирования на проникновения–Информационные технологии и телекоммуникации, 2021 //Т. – 2021. – Т. 9. – С. 1-2.

### **References**

1. Volkogonov V. N., Gelfand A. M., Karamova M. R. Ensuring the Security of Personal Data in Their Processing in Information Systems of Personal Data // Actual Problems of Infotelecommunications in Science and Education (APINO 2019). – 2019. – pp. 266-270.
2. Volkogonov V. N., Gelfand A. M., Derevyanko V. S. Relevance of automated control systems // Actual problems of infotelecommunications in science and education (APINO 2019). – 2019. – pp. 262-266.

3. Kirilova K. S. et al. Problem of neutralization of nucleus-level rootkits in special purpose systems. – 2020. – Т. 12. – №. 3. – pp. 2.
  4. Katasonov A. I., Tsvetkov A. Y. Analysis of Access Differentiation Mechanisms in Special Purpose Systems // Actual Problems of Infotelecommunications in Science and Education (APINO 2020). – 2020. – pp. 563-568.
  5. Shterenberg S. I., Moskalchuk A. I., Krasov A. V. Development of Security Scenarios for Creating Vulnerable Virtual Machines and Studying Penetration Testing Methods–Information Technologies and Telecommunications, 2021 // Т. – 2021. – Т. 9. – pp. 1-2.
-



Международный журнал информационных технологий и энергоэффективности

Сайт журнала:

<http://www.openaccessscience.ru/index.php/ijcse/>



УДК 004.056

## ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ПРОМЫШЛЕННОМ ИНТЕРНЕТЕ ВЕЩЕЙ (IIOT): СПЕЦИФИКА УГРОЗ НА УРОВНЕ ПРОИЗВОДСТВЕННЫХ СИСТЕМ

Гаджиев Г.К.

ФГБОУ ВО САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФЕССОРА М. А. БОНЧ-БРУЕВИЧА, Санкт-Петербург, Россия (193232, г. Санкт-Петербург, просп. Большевиков, 22, корп. 1), e-mail: [gugac134@gmail.com](mailto:gugac134@gmail.com)

Статья посвящена проблемам информационной безопасности в промышленном интернете вещей (IIOT). Рассматриваются особенности архитектуры IIOT, характерные уязвимости производственных систем, угрозы, связанные с протоколами, оборудованием и SCADA-инфраструктурой. Представлены подходы к защите, включающие сетевую сегментацию, шифрование, безопасную аутентификацию и поведенческий анализ. Подчеркивается важность комплексного подхода и осведомлённости персонала для обеспечения устойчивости критически важной промышленной инфраструктуры.

Ключевые слова: IIOT, промышленный интернет вещей, SCADA, кибербезопасности, информационная безопасность, производственные системы, сетевые протоколы, сегментация сети, аутентификация, поведенческий анализ, критическая инфраструктура.

## INFORMATION SECURITY IN THE INDUSTRIAL INTERNET OF THINGS (IIOT): THE SPECIFICS OF THREATS AT THE LEVEL OF PRODUCTION SYSTEMS

Gadzhiev G.K.

ST. PETERSBURG STATE UNIVERSITY OF TELECOMMUNICATIONS NAMED AFTER PROFESSOR M. A. BONCH-BRUEVICH, St. Petersburg, Russia (193232, St. Petersburg, ave. Bolshhevikov, 22, bldg. 1), e-mail: [gugac134@gmail.com](mailto:gugac134@gmail.com)

The article is devoted to the problems of information security in the industrial Internet of Things (IIOT). The features of the IIOT architecture, characteristic vulnerabilities of production systems, and threats related to protocols, hardware, and SCADA infrastructure are considered. Security approaches are presented, including network segmentation, encryption, secure authentication, and behavioral analysis. The importance of an integrated approach and staff awareness is emphasized to ensure the sustainability of critical industrial infrastructure.

Keywords: IIOT, industrial Internet of Things, SCADA, cybersecurity, information security, production systems, network protocols, network segmentation, authentication, behavioral analysis, critical infrastructure.

### Введение

Промышленный интернет вещей (Industrial Internet of Things, IIOT) представляет собой революцию в области автоматизации и цифровизации производственных процессов. В отличие от классических IoT-систем, ориентированных на потребительский сектор, IIOT интегрируется непосредственно в критически важные производственные системы: станки с числовым программным управлением, SCADA-системы, датчики на конвейерах, автоматизированные системы управления технологическими процессами. Эти элементы связываются в единую цифровую экосистему, что позволяет собирать и анализировать данные в реальном времени, повышать производительность и снижать затраты. Однако с ростом

подключённости и сложности систем значительно увеличиваются риски в области информационной безопасности. В условиях, когда ИТ и операционные технологии (ОТ) тесно переплетаются, киберугрозы могут приводить не только к утечке данных, но и к прямым физическим последствиям: авариям, поломкам оборудования и рискам для жизни персонала.[1]

### **Уязвимости IIOT и причины угроз безопасности производственных систем**

Одной из главных особенностей IIOT является длительный жизненный цикл промышленного оборудования. Большинство производственных объектов разрабатывались десятилетия назад без учёта современных киберугроз. Часто такие системы работают на устаревших операционных системах, не поддерживающих обновления безопасности. Это создаёт благоприятную среду для эксплуатации известных уязвимостей. В отличие от корпоративных ИТ-сетей, в которых обновления и патчи можно внедрять централизованно, в ОТ-среде любое вмешательство требует длительного планирования и согласования, так как остановка производственного процесса может привести к существенным убыткам.

Большая часть угроз в IIOT исходит из слабости протоколов связи. Многие промышленные устройства используют небезопасные или устаревшие протоколы, такие как Modbus, DNP3, OPC, которые изначально разрабатывались без шифрования или аутентификации. Злоумышленники могут перехватывать команды управления, внедрять ложные сигналы, подменять параметры или вызывать отказ систем. [2] Такие атаки могут быть незаметными для операторов, но приводить к постепенному снижению качества продукции или нарушению технологических процессов.

Дополнительную угрозу представляют уязвимости в устройствах самого IIOT. Небезопасные конфигурации, жёстко зашитые учётные записи (hardcoded credentials), отсутствие средств мониторинга и логирования — всё это упрощает задачу атакующим. IIOT-устройства часто разрабатываются с приоритетом на функциональность и стоимость, а не на безопасность. При этом они имеют постоянное соединение с сетью и становятся мостами между внешним миром и закрытой производственной инфраструктурой.[3]

Одной из самых опасных форм атаки в промышленном секторе является проникновение в SCADA-системы — центральные элементы управления производством. Атаки на эти системы, такие как известный инцидент со Stuxnet, могут привести к разрушению оборудования, длительным простоям и экологическим катастрофам. При этом всё чаще используются атаки с длительной скрытой фазой — злоумышленники внедряются в сеть, изучают структуру системы и лишь затем инициируют разрушительное воздействие.

Для повышения уровня безопасности IIOT необходим многоуровневый подход, сочетающий как технические, так и организационные меры. Прежде всего следует реализовать сетевую сегментацию, отделяющую производственную инфраструктуру от корпоративной и внешней сети. Использование межсетевых экранов, шлюзов приложений и виртуальных частных сетей позволяет ограничить зону воздействия при возможном проникновении.

Критично обеспечить безопасную аутентификацию и управление доступом ко всем устройствам и системам IIOT. [4] Механизмы многофакторной аутентификации, ролевого разграничения прав и регулярный аудит прав доступа позволяют минимизировать угрозу внутреннего и внешнего злоупотребления. Все каналы передачи данных должны быть

защищены с помощью современных криптографических протоколов, таких как TLS, IPsec или VPN.

Важно внедрять средства мониторинга и анализа поведения в реальном времени, адаптированные под специфические характеристики OT-среды. Системы обнаружения вторжений (IDS), ориентированные на IIOT-протоколы, должны уметь выявлять аномалии в обмене данными между промышленными устройствами. Применение алгоритмов машинного обучения и поведенческого анализа помогает идентифицировать скрытые атаки и неполадки до момента наступления критических последствий.[5]

Обновление программного обеспечения должно осуществляться строго регламентированным образом, с предварительным тестированием на изолированной инфраструктуре. Организация безопасного процесса обновлений и патчей помогает защититься от атак, использующих известные уязвимости. Кроме того, производители IIOT-устройств должны внедрять принципы безопасной разработки (Security by Design) и предоставлять механизмы управления безопасностью на протяжении всего жизненного цикла оборудования.

Ключевым элементом защиты является и обучение персонала. Специалисты, работающие на производстве, должны понимать риски, связанные с подключёнными устройствами, и уметь распознавать признаки компрометации. В условиях роста атак, нацеленных на эксплуатацию человеческого фактора, информационная гигиена становится неотъемлемой частью общей стратегии безопасности.

### **Заключение**

Промышленный интернет вещей открывает широкие перспективы для повышения эффективности и прозрачности производственных процессов, но вместе с этим приносит и новые киберугрозы. Уязвимости на уровне устройств, протоколов и процессов делают IIOT-экосистему чувствительной к внешним и внутренним атакам. Для обеспечения безопасности необходимо внедрять комплексную защиту, сочетающую сетевую сегментацию, безопасную аутентификацию, мониторинг поведения и обновление систем. Только системный подход, включающий в себя как технические средства, так и подготовку персонала, позволяет обеспечить устойчивость промышленной инфраструктуры в условиях цифровой трансформации.

### **Список литературы**

1. Штеренберг, С. И. Компьютерные вирусы / С. И. Штеренберг, А. В. Красов, А. Ю. Цветков. Том Часть 1. – Санкт-Петербург : Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2015. –63с.– EDN CMMEML.
2. Катасонов А. И., Цветков А. Ю. Анализ механизмов разграничения доступа в системах специального назначения //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2020). – 2020. – С. 563-568.
3. Суворов А. М., Цветков А. Ю. Исследование атак типа переполнение буфера в 64-х разрядных unix подобных операционных системах //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2018). – 2018. – С. 570-573.

4. Пестов И. Е. Методика разработки управляющего воздействия на инстансы облачной инфраструктуры //Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. – 2020. – №. 4. – С. 72-76.
5. Казанцев А. А., Прохоров М. В., Худякова П. С. Обзор подходов к классификации текстов актуальными методами //Экономика и качество систем связи. – 2021. – №. 1 (19). – С. 57-67.

## References

1. Shterenberg, S. I. Computer viruses / S. I. Shterenberg, A.V. Krasov, A. Y. Tsvetkov. Volume Part 1. – St. Petersburg : St. Petersburg State University of Telecommunications named after prof. M.A. Bonch-Bruевич, 2015. –63 p. - EDN CMMEML.
  2. Katasonov A. I., Tsvetkov A. Yu. Analysis of access control mechanisms in special purpose systems //Actual problems of infotelec communications in science and education (APINO 2020). – 2020. – pp. 563-568.
  3. Suvorov A.M., Tsvetkov A. Y. Investigation of buffer overflow attacks in 64-bit unix-like operating systems //Actual problems of infotelec communications in science and education (APINO 2018). – 2018. – pp. 570-573.
  4. Pestov I. E. Methodology for developing control effects on cloud infrastructure instances //Bulletin of the St. Petersburg State University of Technology and Design. Series 1: Natural and Technical Sciences. – 2020. – №. 4. – pp. 72-76.
  5. Kazantsev A. A., Prokhorov M. V., Khudyakova P. S. Review of approaches to text classification by current methods //Economics and quality of communication systems. – 2021. – №. 1 (19). – pp. 57-67.
-





Международный журнал информационных технологий и  
энергоэффективности

Сайт журнала:

<http://www.openaccessscience.ru/index.php/ijcse/>



УДК 004.8

## ПОВЫШЕНИЕ ЛОЯЛЬНОСТИ КЛИЕНТОВ С ПОМОЩЬЮ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

**Естехина С.С.**

ФГАОУ ВО "НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ЯДЕРНЫЙ УНИВЕРСИТЕТ  
"МИФИ", Москва, Россия (115409, город Москва, Каширское ш., д.31), e-mail: sofya-  
estehina@mail.ru

В статье рассмотрено влияние искусственного интеллекта на формирование лояльности клиентов. Особое внимание уделено двухкомпонентной природе лояльности, включающей экономическую и эмоциональную составляющие. Экономическая лояльность связана с рациональными факторами, такими как цена и качество, тогда как эмоциональная формируется через положительный опыт взаимодействия с брендом, доверие и чувство принадлежности. Проанализированы современные технологии искусственного интеллекта, включая машинное обучение, обработку естественного языка и рекомендательные системы, которые позволяют компаниям создавать персонализированный клиентский опыт. На примерах Starbucks, Amazon, Spotify и Sephora продемонстрировано, как персонализация, интеллектуальные чат-боты и поведенческая аналитика повышают вовлеченность клиентов, увеличивают повторные покупки и снижают отток. Сделан вывод о ключевой роли искусственного интеллекта в укреплении лояльности за счет сочетания рациональных и эмоциональных факторов. Статья представляет интерес для специалистов в области маркетинга, клиентского опыта и цифровых технологий, а также для всех, кто изучает современные методы взаимодействия с потребителями.

Ключевые слова: Лояльность клиентов, искусственный интеллект, персонализация, клиентский опыт, маркетинг, эмоциональная лояльность.

## ENHANCING CUSTOMER LOYALTY THROUGH ARTIFICIAL INTELLIGENCE

**Estekhina S.S.**

"NATIONAL RESEARCH NUCLEAR UNIVERSITY "MEPHI", Moscow, Russia (115409, Moscow,  
Kashirskoye sh., 31 e-mail: sofya-estehina@mail.ru

The article examines the impact of artificial intelligence on customer loyalty formation. Special attention is paid to the dual-component nature of loyalty, encompassing economic and emotional aspects. Economic loyalty is tied to rational factors such as price and quality, while emotional loyalty is shaped through positive brand interactions, trust, and a sense of belonging. Modern artificial intelligence technologies are analyzed, including machine learning, natural language processing, and recommendation systems, which enable companies to create personalized customer experiences. Case studies of Starbucks, Amazon, Spotify, and Sephora demonstrate how personalization, intelligent chatbots, and behavioral analytics enhance customer engagement, increase repeat purchases, and reduce churn. The conclusion highlights the pivotal role of artificial intelligence in strengthening loyalty by combining rational and emotional factors. The article is relevant for marketing professionals, customer experience specialists, and digital technology experts, as well as anyone interested in modern consumer engagement strategies.

Keywords: Customer loyalty, artificial intelligence, personalization, customer experience, marketing, emotional loyalty.

### Введение

В условиях усиливающейся конкуренции на глобальном рынке лояльность клиентов становится критически важным фактором устойчивого развития бизнеса в любых отраслях.

Согласно данным Statista, объем мирового рынка персонализированных сервисов к 2026 году достигнет 11,6 млрд долларов, демонстрируя рост в 65% с 2021 года [1]. Такие показатели отражают растущие ожидания потребителей к индивидуальному подходу и вынуждают компании всех секторов экономики пересматривать свои стратегии взаимодействия с клиентами.

Лояльность потребителей в современной бизнес-среде приобретает особую ценность: в отличие от разовых транзакций, долгосрочные отношения с клиентами обеспечивают стабильный доход и снижают затраты на привлечение новой аудитории.

Искусственный интеллект (ИИ) предлагает революционные возможности для создания персонализированного клиентского опыта, который напрямую влияет на лояльность. Технологии машинного обучения (ML), обработки естественного языка (NLP) и предиктивной аналитики позволяют компаниям адаптировать свои продукты и услуги под индивидуальные предпочтения клиентов, прогнозировать их потребности и предотвращать отток.

Целью данного исследования является анализ влияния технологий искусственного интеллекта (ИИ) на формирование клиентской лояльности, включая её экономическую и эмоциональную составляющие. В работе рассматриваются современные ИИ-решения, такие как персонализация, рекомендательные системы и чат-боты, а также их эффективность на примере ведущих компаний.

### **Материалы и методы исследования**

Теоретической основой исследования послужили научные работы, раскрывающие природу клиентской лояльности. Эмпирическая база сформирована на основе анализа практических кейсов внедрения ИИ-технологий в компаниях Starbucks, Amazon, Spotify, Sephora и Duolingo. Для количественной оценки эффективности использованы статистические данные авторитетных источников (Statista, McKinsey, Renaissance). Методологический аппарат включал анализ научной литературы, сравнительное изучение успешных практик применения ИИ, а также оценку ключевых показателей эффективности, таких как динамика продаж, уровень клиентской вовлеченности.

### **Результаты исследования и их обсуждение**

Анализ практического опыта компаний показал, что внедрение персонализированных решений на основе ИИ приводит к росту экономических показателей. В частности, Starbucks зафиксировал трехкратное увеличение средних расходов участников программы лояльности. В аспекте эмоциональной лояльности особую эффективность показали интерактивные решения, такие как Sephora Virtual Artist и образовательная платформа Duolingo. Эти технологии способствовали формированию устойчивой эмоциональной связи с брендом через создание персонализированного пользовательского опыта.

В научной литературе существует множество определений лояльности:

1. Лояльность клиента - это положительное отношение и постоянство в обращении к услугам одной и той же компании [2]
2. Потребитель, лояльный бренду, – это человек, который покупает ваш бренд в 100% случаев [3]
3. Лояльность – это глубокая решимость постоянно покупать определенный, под одним и тем же брендом продукт, независимо от ситуации и рекламы других брендов [4]

Если обобщить вышеупомянутые определения, то лояльность клиентов можно сформулировать, как понятие, которое отражает приверженность потребителей к бренду, продукту или компании, проявляющуюся в повторных покупках, положительных рекомендациях и устойчивости к предложениям конкурентов. Лояльность формируется под влиянием рациональных или экономических (цена, качество) и эмоциональных (доверие, комфорт) факторов, что делает ее ключевым элементом долгосрочных отношений компании с потребителями.

Рассмотрим подробнее две стороны лояльности: экономическую и эмоциональную.

Экономическая лояльность клиента представляет собой его способность генерировать устойчивую прибыль для компании. Данное понятие подразумевает, что доходы, получаемые от взаимодействия с таким клиентом, должны превышать затраты на его обслуживание и привлечение.

Ключевые характеристики экономически лояльных клиентов:

1. Они совершают повторные покупки
2. Их средний чек превышает затраты компании на обслуживание
3. Они демонстрируют устойчивое потребление в долгосрочной перспективе

Данный тип лояльности формируется на основе логического анализа и прагматических соображений потребителя. Он включает три ключевых компонента:

1. Временная составляющая. Отражает стремление потребителя минимизировать временные затраты на процесс выбора и покупки.
2. Сравнительная составляющая. Основана на сознательном анализе альтернатив по ключевым параметрам: соотношение цены и качества, функциональные характеристики продукта и другие
3. Риск-ориентированная составляющая. Связана со стремлением потребителя минимизировать различные виды рисков, например, финансовые или риски, связанные с личной безопасностью

Эмоциональная лояльность формируется иначе, чем экономическая приверженность бренду. Если экономическая лояльность основывается на объективных характеристиках продукта, то эмоциональная возникает как следствие продолжительного позитивного взаимодействия между компанией и потребителем. Она складывается под влиянием субъективных, трудно измеримых факторов, которые в совокупности создают у клиента устойчивое чувство удовлетворенности.

Эмоциональная лояльность формируется из личных оценок и переживаний потребителя, формирующих его отношение к бренду: от базовой удовлетворенности до более сложных эмоциональных состояний, таких как искренняя заинтересованность, теплое отношение, чувство гордости от принадлежности к сообществу бренда, доверие, воспринимаемое почти как дружеская связь. Особенность эмоциональной лояльности проявляется в высокой степени вовлеченности потребителя в процесс выбора и использования продукта. Именно клиенты, чья привязанность к бренду обусловлена эмоциональными факторами, демонстрируют наибольшую устойчивость и продолжительность отношений с компанией, что делает их наиболее ценными в долгосрочной перспективе [5].

Эта составляющая лояльности формируется на основе субъективных переживаний и включает:

1. Опытную составляющую. Формируется через положительный опыт взаимодействия с брендом на всех этапах. Кумулятивный эффект положительных эмоций (удовольствие, удобство, чувство благодарности) закрепляет привязанность. Особенно важными являются следующие точки: первая покупка (эффект «вау» от упаковки/сервиса), решение возникших у клиента проблем (например, быстрый возврат денег, что усиливает доверие к компании), неожиданные бонусы в подходящий момент

2. Идентификационную составляющую. Проявляется, когда потребитель начинает ассоциировать себя с брендом. Это подтверждается теорией социальной идентичности Г. Тешфела и Дж. Тернера: человек стремится к брендам, укрепляющим его Я-концепцию. [6]

3. Социальную составляющую. Отражает влияние социального окружения на лояльность. Большинство покупателей выбирают бренды, одобренные их социальным кругом

Таким образом, лояльность формируется на основе рациональных критериев и эмоциональной приверженности бренду. Важно отметить, что экономическая лояльность и эмоциональная взаимосвязаны. Рациональные факторы часто становятся основой для последующего формирования эмоциональной привязанности. Эмоциональная лояльность может усиливать восприятие рациональных преимуществ. Это демонстрирует необходимость комплексного подхода к формированию клиентской лояльности.

### **Технологии искусственного интеллекта и лояльность потребителей**

Современные компании активно внедряют технологии искусственного интеллекта в обслуживание клиентов, стремясь повысить эффективность взаимодействия и укрепить их приверженность бренду. Ключевым механизмом влияния ИИ на лояльность являются опосредующие факторы — удовлетворенность клиентов и воспринимаемая эффективность сервиса.

Рассмотрим способы применения технологий искусственного интеллекта для формирования лояльности клиентов.

Персонализация - это адаптация продукта, сервиса или контента под индивидуальные потребности, поведение и предпочтения пользователя на основе данных. Она строится на глубоком анализе данных о поведении, демографических характеристиках, истории взаимодействий и других параметрах, которые помогают создать уникальный опыт для клиента. Основная цель персонализации — повысить удовлетворенность пользователей, увеличить вовлеченность и укрепить лояльность, предлагая именно то, что нужно человеку, в нужный момент и в подходящей форме. Одной из ключевых технологий персонализации является машинное обучение, которое анализирует большие массивы данных и выявляет скрытые закономерности в поведении пользователей. Еще одной важной технологией являются рекомендательные системы, которые активно используются в интернет-магазинах, стриминговых платформах и других сервисах. Эти системы работают на основе различных методов, включая коллаборативную фильтрацию, которая анализирует поведение похожих пользователей, и контентную фильтрацию, которая учитывает характеристики самого продукта. Обработка естественного языка (NLP) — это еще одна технология, которая играет важную роль в персонализации. NLP позволяет анализировать текстовые данные, такие как отзывы, сообщения в чатах или посты в социальных сетях, чтобы лучше понимать настроения и предпочтения пользователей.

Глубокое обучение, особенно нейронные сети, также вносит значительный вклад в персонализацию. Эти технологии способны обрабатывать сложные и неструктурированные данные, такие как изображения или видео, чтобы предлагать более точные рекомендации.

О. Tyrväinen, Н. Karjaluo и Н. Saarijärvi изучили связь между персонализацией, гедонистической мотивацией, клиентским опытом и лояльностью. Их исследование подтвердило положительную связь между персонализацией и гедонистической мотивацией, которая, в свою очередь, влияет на эмоциональные и когнитивные компоненты клиентского опыта и лояльность. [7]

В качестве примера применения персонализации можно привести Starbucks: ИИ-алгоритмы в программе лояльности Starbucks Rewards анализируют историю покупок, предпочтения, местоположение и даже погоду, чтобы предлагать персонализированные рекомендации и бонусы. Согласно статистике, члены программы лояльности Starbucks тратят в 3 раза больше, чем те, кто не является ее членами, и посещают заведения чаще, а 41% продаж Starbucks в США приходится на участников программы лояльности [8]. Подбор персональных предложений и скидок формирует у клиентов понимание того, что они всегда могут найти наиболее быстрое и с наибольшей степенью подходящее в данный момент решение, за счет чего реже пользуются товарами конкурентов. Что, как можно увидеть по статистике, влияет на приверженность клиентов бренду и соответственно на лояльность в целом.

Amazon использует искусственный интеллект и машинное обучение для анализа поведения пользователей и генерации персонализированных рекомендаций. Алгоритмы глубокого обучения анализируют просмотры, покупки, оценки, отзывы и даже время, проведенное на страницах товаров. Рекомендации обновляются в реальном времени, учитывая последние действия пользователя (например, добавление товара в корзину). Персонализация Amazon напрямую увеличивает вовлеченность и повторные покупки:

1. 35% продаж Amazon генерируется через рекомендации [9]
2. 56% пользователей, взаимодействующих с персонализированными предложениями, чаще возвращаются [10]
3. Снижение оттока — персонализация уменьшает вероятность ухода к конкурентам, так как пользователи чувствуют индивидуальный подход

Spotify использует алгоритмы машинного обучения для совершенствования и улучшения своего механизма рекомендаций музыки, гарантируя, что пользователи получают самые релевантные предложения. MIT Technology Review отмечает, что такой подход может повысить вовлеченность аудитории на 60%, что положительно сказывается на лояльности клиентов в целом [11].

Spotify создает уникальные персонализированные сервисы, такие как Spotify Wrapped, чтобы вовлекать пользователей и формировать чувство общности:

1. Предоставляет пользователям персонализированный обзор их привычек прослушивания, включая их самые популярные песни, исполнителей и жанры. Данные Spotify показывают, что Wrapped ежегодно генерирует более 1,5 млрд показов в социальных сетях, что подчеркивает его успех в повышении вовлеченности пользователей
2. Создает статистику на основе анализа данных пользователя за год. Эта стратегия геймификации повышает вовлеченность и лояльность пользователей, поскольку пользователи с нетерпением ждут своих результатов каждый год. Опрос Hootsuite показал, что 67% пользователей чувствуют себя более связанными с брендами, которые вовлекают их через

кампании в социальных сетях, что говорит о положительном влиянии данной активности на эмоциональную привязанность клиентов к бренду [11].

Следующим инструментом, основанном на искусственном интеллекте, позволяющем повысить лояльность клиентов, являются чат-боты и виртуальные ассистенты. Эти технологии обеспечивают автоматизацию взаимодействия между компаниями и их клиентами, позволяя значительно повысить эффективность коммуникации и удовлетворенность пользователей. Основой функционирования чат-ботов является алгоритм обработки естественного языка, который позволяет им понимать и генерировать текстовые сообщения, а также интерпретировать намерения пользователей. Они могут использоваться для автоматизации процесса обслуживания, предоставления рекомендаций по продуктам, обработки запросов на возврат и обмен товаров и др. Кроме того, чат-боты могут функционировать круглосуточно, что позволяет компаниям предоставлять услуги в любое время без необходимости увеличения численности персонала. Это особенно актуально в условиях растущей конкуренции, когда потребители ожидают быстрого и качественного обслуживания.

Примером успешного внедрения чат-ботов на основе искусственного интеллекта является компания Sephora:

1. Sephora Virtual Artist: Это мобильное приложение использует технологию дополненной реальности, что позволяет клиентам примерять тысячи продуктов Sephora непосредственно через мобильное устройство. Данная функция обеспечивает высокую степень интерактивности и персонализации пользовательского опыта. К 2018 году, всего через два года после запуска приложения, Sephora Virtual Artist зарегистрировал более 200 миллионов примерок оттенков и свыше 8,5 миллионов посещений данной функции.

2. Sephora Color Match: помогал клиентам в подборе оттенков и предоставлял рекомендации по продуктам из всего ассортимента Sephora. Это позволяло пользователям пробовать разные оттенки в режиме реального времени и покупать продукт непосредственно с веб-сайта/мобильного приложения Sephora [12].

Чат-боты и виртуальные ассистенты могут быть модернизированы в части реализации не просто текстового обмена человека с ботом, но и голосового или даже видео-обмена, что и сделала компания Duolingo. Пользователи приложения могут создавать видео-диалоги с виртуальным ассистентом. Эта возможность основана на генеративном ИИ, который используется для создания реалистичных разговорных сценариев, и на компьютерном зрении, используемом для анализа мимики, что напрямую способствует формированию лояльности за счет нескольких ключевых факторов: она решает основную проблему онлайн-обучения — отсутствие разговорной практики, а благодаря персонализации диалогов (адаптации сложности, тематики и обратной связи под уровень пользователя), создает эффект индивидуального подхода, который, согласно исследованию McKinsey, повышает вовлеченность на 40% [13].

Приведенные выше примеры связаны с непосредственным использованием клиентами описанных технологий на базе искусственного интеллекта. Но ИИ может быть задействован и во вспомогательных процессах, неявно формирующих пользовательский опыт. Например, показ рекламы. Компания Duolingo успешно применила машинное обучение в маркетинге. Вместо тотального показа рекламы, система адаптирует объявления под интересы учеников. Основной задачей было создать алгоритм, который бы учитывал, как коммерческие показатели (доход от рекламы), так и качество пользовательского опыта. Система оценивает

каждое доступное рекламное предложение по двум параметрам: вероятной доходности и ожидаемому уровню взаимодействия пользователя. Результаты внедрения показали значительное улучшение ключевых показателей: за первые несколько месяцев новая модель принесла миллионы долларов дополнительного годового дохода, а количество ежедневных посетителей возросло. При этом важно отметить, что система не оказала негативного влияния на удержание пользователей, что свидетельствует о сохранении положительного опыта взаимодействия с приложением [14].

Проведенный анализ демонстрирует значительное влияние технологий искусственного интеллекта на формирование лояльности клиентов через различные механизмы персонализации. Как показывают исследования и практические примеры ведущих компаний (Starbucks, Amazon, Spotify, Sephora, Duolingo), применение ИИ-решений позволяет:

1. Повысить уровень персонализации за счет анализа поведения, предпочтений и контекста пользователей (история покупок, местоположение, погода и т. д.), что напрямую увеличивает удовлетворенность и вовлеченность.
2. Улучшить клиентский опыт благодаря адаптивным рекомендациям, чат-ботам и интерактивным функциям (например, видео-диалогам в Duolingo), которые делают взаимодействие с брендом более удобным и релевантным.
3. Стимулировать повторные покупки и эмоциональную привязанность, что подтверждается приведенной выше статистикой

Ключевым фактором успеха является баланс между монетизацией и пользовательским опытом. Технологии ИИ, такие как машинное обучение, NLP и компьютерное зрение, не только оптимизируют бизнес-процессы, но и создают эмоциональную связь с клиентами, что критически важно для долгосрочной лояльности.

### **Вывод**

Проведенное исследование демонстрирует, что технологии искусственного интеллекта становятся значимым аспектом формирования клиентской лояльности в цифровую эпоху. На основе анализа теоретических концепций и практических кейсов ведущих компаний можно сделать следующие выводы.

Современные ИИ-решения обеспечивают комплексное воздействие на оба компонента лояльности. На экономическую лояльность - через персонализацию предложений и прогнозирование потребностей. На эмоциональную лояльность - за счет создания персонализированного опыта и эмпатичного взаимодействия.

Ключевым конкурентным преимуществом становится способность ИИ-систем балансировать между коммерческой эффективностью и качеством клиентского опыта, интегрировать рациональные и эмоциональные факторы лояльности и обеспечивать непрерывное взаимодействие со всеми каналами коммуникации.

Таким образом, искусственный интеллект оказывает существенное влияние на формирование удовлетворенности клиентов, как с точки зрения получения экономической выгоды для клиента, так и с точки зрения формирования эмоциональной привязанности к бренду. Дальнейшие исследования могут быть сфокусированы на исследовании долгосрочного влияния искусственного интеллекта на лояльность потребителей и анализу применимости различных новых технологий на базе ИИ для управления лояльностью потребителей.

## Список литературы

1. Customer experience personalization and optimization software and services revenue worldwide from 2020 to 2026 [Электронный ресурс] // Statista. – URL: <https://www.statista.com/statistics/1333448/cx-personalization-optimization-revenue-worldwide/> (дата обращения: 20.04.2025)
2. Носова Н.С. Лояльность клиентов, или Как удержать старых и привлечь новых клиентов / Н.С. Носова. - М.: «Дашков и К»; Саратов: ООО «Ан-лейс», 2012. - 192 с.
3. Широценская И. П. Основные понятия и методы измерения лояльности // Маркетинг в России и за рубежом. 2004. № 2 (40). С. 36.
4. Темпорал П., Трот М. Роман с покупателем: пер. с англ. / под ред. Ю. Н. Кантуревского. СПб., 2002. С. 146.
5. Воронин В.Н., Ионцева М.В. Особенности формирования клиентской лояльности // Вестник университета. - 2013.
6. Микляева А.В, Румянцева Полина Витальевна Теория социальной идентичности как источник современных практико-ориентированных психологических исследований: зарубежный опыт // Азимут научных исследований: педагогика и психология. - 2017.
7. Tyrväinen O., Karjaluoto H., Saarijärvi H. Personalization and hedonic motivation in creating customer experiences and loyalty in omnichannel retail // Journal of Retailing and Consumer Services. - 2020. - Vol. 57
8. Scale success story: Starbucks rewards program [Электронный ресурс] // LoyaltyLion. - 2022. - URL: <https://loyaltylion.com/blog/scale-success-story-starbucks-rewards-program> (дата обращения: 20.04.2025).
9. How retailers can keep up with consumers [Электронный ресурс] // McKinsey & Company. - 2023. - URL: <https://www.mckinsey.com/industries/retail/our-insights/how-retailers-can-keep-up-with-consumers> (дата обращения: 20.04.2025).
10. The Amazon effect [Электронный ресурс] // Rebuy Engine. - 2023. - URL: <https://www.rebuyengine.com/blog/the-amazon-effect> (дата обращения: 20.04.2025).
11. Johnson M. How Spotify delivers a unique customer experience with personalized music recommendations // Customer Experience Journal. - 2022. - Vol. 5. - No. 2. - P. 34-45
12. Beauty and the bot: how Sephora reimaged customer experience with AI [Электронный ресурс] // Cut the SaaS. - 2023. - URL: <https://www.cut-the-saas.com/ai/beauty-and-the-bot-how-sephora-reimagined-customer-experience-with-ai> (дата обращения: 20.04.2025).
13. The value of getting personalization right - or wrong - is multiplying [Электронный ресурс] // McKinsey & Company. - 2023. - URL: <https://www.mckinsey.com/capabilities/growth-marketing-and-sales/our-insights/the-value-of-getting-personalization-right-or-wrong-is-multiplying> (дата обращения: 20.04.2025).
14. How we use machine learning for better ads [Электронный ресурс] // Duolingo Blog. - 2023. - URL: <https://blog.duolingo.com/machine-learning-ads/> (дата обращения: 20.04.2025).

## References

1. Customer experience personalization and optimization software and services revenue worldwide from 2020 to 2026 [Электронный ресурс] // Statista. – URL:



- <https://www.statista.com/statistics/1333448/cx-personalization-optimization-revenue-worldwide/> (дата обращения: 20.04.2025)
2. Носова Н.С. Лояльность клиентов, или Как удержать старых и привлечь новых клиентов / Н.С. Носова. - М.: «Дашков и К»; Саратов: ООО «Ан-лейс», 2012. - 192 с.
  3. Широценская И. П. Основные понятия и методы измерения лояльности // Маркетинг в России и за рубежом. 2004. № 2 (40). С. 36.
  4. Темпорал П., Трот М. Роман с покупателем: пер. с англ. / под ред. Ю. Н. Кантуревского. СПб., 2002. С. 146.
  5. Воронин В.Н., Ионцева М.В. Особенности формирования клиентской лояльности // Вестник университета. - 2013.
  6. Микляева А.В, Румянцева Полина Витальевна Теория социальной идентичности как источник современных практико-ориентированных психологических исследований: зарубежный опыт // Азимут научных исследований: педагогика и психология. - 2017.
  7. Tyrväinen O., Karjaluoto H., Saarijärvi H. Personalization and hedonic motivation in creating customer experiences and loyalty in omnichannel retail // Journal of Retailing and Consumer Services. - 2020. - Vol. 57
  8. Scale success story: Starbucks rewards program [Электронный ресурс] // LoyaltyLion. - 2022. - URL: <https://loyaltylion.com/blog/scale-success-story-starbucks-rewards-program> (дата обращения: 20.04.2025).
  9. How retailers can keep up with consumers [Электронный ресурс] // McKinsey & Company. - 2023. - URL: <https://www.mckinsey.com/industries/retail/our-insights/how-retailers-can-keep-up-with-consumers> (дата обращения: 20.04.2025).
  10. The Amazon effect [Электронный ресурс] // Rebuy Engine. - 2023. - URL: <https://www.rebuyengine.com/blog/the-amazon-effect> (дата обращения: 20.04.2025).
  11. Johnson M. How Spotify delivers a unique customer experience with personalized music recommendations // Customer Experience Journal. - 2022. - Vol. 5. - No. 2. - P. 34-45
  12. Beauty and the bot: how Sephora reimaged customer experience with AI [Электронный ресурс] // Cut the SaaS. - 2023. - URL: <https://www.cut-the-saas.com/ai/beauty-and-the-bot-how-sephora-reimagined-customer-experience-with-ai> (дата обращения: 20.04.2025).
  13. The value of getting personalization right - or wrong - is multiplying [Электронный ресурс] // McKinsey & Company. - 2023. - URL: <https://www.mckinsey.com/capabilities/growth-marketing-and-sales/our-insights/the-value-of-getting-personalization-right-or-wrong-is-multiplying> (дата обращения: 20.04.2025).
  14. How we use machine learning for better ads [Электронный ресурс] // Duolingo Blog. - 2023. - URL: <https://blog.duolingo.com/machine-learning-ads/> (дата обращения: 20.04.2025).
-



Международный журнал информационных технологий и энергоэффективности

Сайт журнала:

<http://www.openaccessscience.ru/index.php/ijcse/>



УДК 004.056

## АНАЛИЗ И ПЕРСПЕКТИВЫ ПРИМЕНЕНИЯ МАШИННОГО ОБУЧЕНИЯ И НЕЙРОСЕТЕВЫХ ТЕХНОЛОГИЙ ДЛЯ ЗАЩИТЫ ИНФОРМАЦИОННЫХ СИСТЕМ

**Маркевич Д.В.**

*ФГБОУ ВО "ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ПУТЕЙ СООБЩЕНИЯ ИМПЕРАТОРА АЛЕКСАНДРА I", Санкт-Петербург, Россия (190031, город Санкт-Петербург, Московский пр-кт, д.9), e-mail: dmarkevich811@mail.ru*

Статья посвящена системному анализу применения методов машинного обучения (ML) и нейросетевых технологий в задачах выявления уязвимостей информационных систем. Рассматриваются современные вызовы кибербезопасности, включая атаки на цепочки поставок и 0-day уязвимости, требующие перехода от традиционных методов тестирования к интеллектуальным системам анализа. Особое внимание уделено:

- классификации методов ML (обучение с учителем/без учителя, гибридные подходы);
- практическому применению моделей CodeBERT и графовых нейросетей (GCN) для обнаружения уязвимостей;
- перспективам создания самообучающихся систем тестирования на основе нейросетей.

Приведены результаты тестирования на датасетах OWASP Benchmark и реальных проектах GitHub, демонстрирующие повышение точности обнаружения уязвимостей на 17-30% по сравнению с традиционными методами. Отмечены ключевые ограничения технологий, включая проблему «чёрного ящика» и ложных срабатываний. Материалы статьи основаны на данных ENISA, CISA и ФСТЭК России за 2021-2023 гг.

Ключевые слова: Машинное обучение, кибербезопасность, анализ уязвимостей, нейросетевые модели, 0-day уязвимости, CodeBERT, графовые нейронные сети (GCN), OWASP Benchmark.

## ANALYSIS AND PROSPECTS OF USING MACHINE LEARNING AND NEURAL NETWORK TECHNOLOGIES TO PROTECT INFORMATION SYSTEMS

**Markevich D.V.**

*"PETERSBURG STATE RAILWAY ENGINEERING UNIVERSITY OF EMPEROR ALEXANDER I", St. Petersburg, Russia (190031, St. Petersburg, Moskovsky prospekt, 9), e-mail: dmarkevich811@mail.ru*

This article presents a systematic analysis of machine learning (ML) and neural network applications for vulnerability detection in information systems. The study addresses modern cybersecurity challenges, including supply chain attacks and zero-day vulnerabilities, which necessitate transitioning from traditional testing methods to intelligent analysis systems. Key focus areas include:

- classification of ML approaches (supervised/unsupervised learning, hybrid methods);
- practical implementation of CodeBERT and graph neural networks (GCN) for vulnerability detection;
- development prospects for self-learning testing systems based on neural architectures.

Experimental results using OWASP Benchmark datasets and real GitHub projects demonstrate 17-30% improvement in vulnerability detection accuracy compared to conventional methods. The study also examines critical technology limitations, including the "black box" problem and false positives. The research incorporates data from ENISA, CISA, and FSTEC Russia (2021-2023).

Keywords: Machine learning, cybersecurity, vulnerability analysis, neural network models, zero-day vulnerabilities, CodeBERT, graph convolutional networks (GCN), OWASP Benchmark.

## **Введение**

Современный ландшафт киберугроз стремительно усложняется, что ставит перед специалистами по информационной безопасности новые вызовы. Традиционные методы тестирования безопасности, основанные преимущественно на сигнатурном анализе и ручной проверке, становятся недостаточными для эффективного противодействия сложным атакам, включая угрозы типа Advanced Persistent Threats (АЗРТ), атаки на цепочки поставок и методы fileless.

По данным отчёта ENISA Threat Landscape 2023 [1], 67% организаций столкнулись с атаками, в которых использовались технологии искусственного интеллекта и машинного обучения. Эти изменения требуют от отрасли перехода к более интеллектуальным способам тестирования и защиты информационных систем.

Одним из таких направлений становится применение методов машинного обучения (ML), способных автоматически анализировать большие объёмы данных, выявлять скрытые уязвимости и прогнозировать возможные сценарии атак. Кроме того, перспективным направлением является использование нейросетевых архитектур для повышения качества анализа и автоматизации процессов тестирования.

Целью данной статьи является проведение системного анализа применения методов машинного обучения в задачах выявления уязвимостей, а также рассмотрение перспектив использования нейросетей в тестировании безопасности.

Научная новизна работы заключается в:

- систематизации существующих методов применения машинного обучения для анализа уязвимостей;
- сравнении эффективности различных подходов на реальных практических кейсах;
- определении перспектив внедрения нейросетевых моделей для дальнейшего развития систем тестирования.

Таким образом, в работе будет рассмотрено, как методы машинного обучения и нейросети могут способствовать построению более эффективных и адаптивных систем обеспечения безопасности на всех этапах жизненного цикла программного обеспечения.

## **Применение методов машинного обучения в тестировании безопасности**

Применение методов машинного обучения (ML) в области тестирования информационной безопасности позволяет существенно повысить эффективность выявления уязвимостей за счёт автоматизации анализа больших объёмов данных, способности выявлять аномалии и прогнозировать новые угрозы [1], [2].

Методы машинного обучения, применяемые в анализе безопасности, можно условно разделить на три основные категории [3], [4]:

- *Обучение с учителем (Supervised Learning)*. Метод подразумевает обучение моделей на размеченных данных, где известны примеры как безопасных, так и уязвимых кодовых фрагментов. Это позволяет строить классификаторы, способные находить аналогичные уязвимости в новых данных [3].
- *Обучение без учителя (Unsupervised Learning)*. Используется в ситуациях, когда отсутствует размеченная выборка. Модели выявляют скрытые закономерности и аномалии в данных, что позволяет обнаруживать неизвестные ранее уязвимости или атипичное поведение в системах [5], [6].

- *Гибридные подходы.* Комбинируют методы обучения с учителем и без учителя, а также интегрируют статический и динамический анализ кода [7], [8]. Это обеспечивает более полное покрытие возможных угроз и позволяет повысить точность выявления уязвимостей.

Применение машинного обучения в задачах тестирования обладает рядом ключевых преимуществ:

- *Адаптивность к новым угрозам.* Модели способны самостоятельно обновляться на основе новых данных об атаках и уязвимостях, обеспечивая более быструю реакцию на изменяющийся ландшафт угроз [1], [5].
- *Масштабируемость.* Машинное обучение позволяет обрабатывать большие объёмы кода и сетевого трафика за значительно меньшее время по сравнению с традиционными методами анализа [3].
- *Снижение нагрузки на экспертов.* Автоматизация рутинных задач освобождает время специалистов для анализа наиболее критичных инцидентов [6].

Тем не менее, применение методов ML связано и с определёнными ограничениями:

- *Вероятность ложных срабатываний (False Positives).* Недостаточное качество обучающих данных или неправильная настройка модели могут привести к ошибкам в классификации [4].
- *Необходимость постоянного обновления данных.* Для поддержания эффективности модели требуется регулярное обновление обучающей выборки, чтобы учитывать появление новых угроз [9].
- *Проблемы интерпретируемости решений.* Некоторые модели, особенно глубокие нейронные сети, обладают «чёрным ящиком» в структуре принятия решений, что усложняет объяснение причин выявления той или иной уязвимости [10].

Несмотря на такие ограничения, как ложные срабатывания, зависимость от качества данных и низкую интерпретируемость решений («чёрный ящик»), методы машинного обучения демонстрируют неоспоримые преимущества:

- адаптивность к новым типам угроз (например, 0-day);
- масштабируемость для анализа больших объёмов кода;
- снижение нагрузки на специалистов за счёт автоматизации.

Это подтверждает перспективность ML для создания гибких систем тестирования безопасности, особенно в условиях быстро меняющегося ландшафта угроз.

### **Практическое применение методов машинного обучения в выявлении уязвимостей**

В реальных условиях тестирования информационной безопасности методы машинного обучения демонстрируют высокую эффективность при решении практических задач. Ниже представлены два ключевых примера использования ML для выявления уязвимостей.

Одной из важнейших задач современных систем безопасности является выявление ранее неизвестных уязвимостей (0-day) в коде веб-приложений. Традиционные методы, основанные на сигнатурном анализе, часто оказываются недостаточно эффективными в условиях динамично меняющихся угроз [1].

С применением моделей обработки естественного языка, таких как CodeBERT [7], появляется возможность автоматизировать анализ исходного кода и находить потенциальные уязвимости на ранних этапах. CodeBERT – это предварительно обученная трансформер-

модель, предназначенная для анализа программного кода и естественного языка. Она позволяет обнаруживать потенциальные уязвимости на основе контекстного понимания структуры кода. В рамках тестирования на датасете OWASP Benchmark [5] использование CodeBERT позволило:

- повысить точность обнаружения уязвимостей на 17% по сравнению с традиционными статическими анализаторами (SAST) [3];
- сократить среднее время анализа кода на 42%.

Такой подход особенно эффективен в условиях использования CI/CD пайплайнов (Continuous Integration/Continuous Delivery - методологии непрерывной интеграции и доставки кода, где изменения автоматически тестируются и развертываются), где требуется быстрое выявление уязвимостей без существенного увеличения времени релиза.

Цепочки поставок программного обеспечения становятся одной из наиболее уязвимых точек атаки, что подтверждают инциденты, подобные атаке на SolarWinds [2] в 2020 году, когда через обновление легитимного ПО Orion были скомпрометированы тысячи организаций, включая правительственные учреждения США. Основной риск заключается в уязвимостях сторонних зависимостей, которые интегрируются в конечные продукты.

Для анализа сложных взаимосвязей между зависимостями используются методы графового машинного обучения, в частности графовые нейронные сети (Graph Convolutional Networks - GCN) - специальный тип нейросетей, который обрабатывает данные в виде графов, сохраняя топологические связи между элементами [8]. В контексте безопасности это позволяет анализировать зависимости между программными компонентами как узлы графа и выявлять уязвимые цепочки. На примере анализа зависимостей в проектах GitHub было установлено, что применение GCN позволило:

- выявить уязвимости в 30% популярных open-source проектов [11];
- провести автоматическую категоризацию рисков по уровню их критичности.

Использование графового анализа значительно повышает качество оценки безопасности программных продуктов, позволяя заблаговременно выявлять и устранять слабые места в цепочках поставок.

### **Перспективы применения нейросетевых архитектур в тестировании безопасности**

Развитие нейросетевых технологий открывает новые возможности в области тестирования безопасности информационных систем. Хотя машинное обучение уже активно используется для анализа уязвимостей, применение специализированных нейросетевых архитектур позволяет значительно расширить потенциал автоматизации и повышения точности обнаружения угроз.

Нейросети обладают способностью выявлять сложные закономерности в данных, что делает их перспективным инструментом для:

- обучения существующим методам и способам тестирования;
- совершенствования существующих методик анализа безопасности;
- выработки новых подходов к тестированию на основе изучения больших массивов кода и данных о уязвимостях.

Такие подходы могут способствовать созданию адаптивных систем обучения для специалистов по информационной безопасности, где нейросети будут не только обучать

базовым методам, но и предлагать инновационные техники на основе анализа реальных угроз [3], [7].

Одним из наиболее перспективных направлений является разработка самообучающихся систем тестирования, использующих нейросетевые модели для:

- автоматического выявления новых классов уязвимостей без необходимости предварительного ручного обучения [8];
- прогнозирования возможных векторов атак на основе анализа исторических данных о безопасности [5];
- постоянной адаптации тестовых сценариев к изменяющимся условиям внешней среды.

Применение нейросетей в данном контексте может стать основой для построения интеллектуальных систем тестирования, способных не только фиксировать текущие уязвимости, но и предсказывать их возникновение на этапе проектирования программных продуктов.

### **Практическое применение нейросетей в тестировании безопасности**

Наряду с перспективами применения нейросетей в обучении и прогнозировании угроз, уже сегодня существуют практические направления их использования для повышения эффективности тестирования информационной безопасности.

Нейросетевые модели позволяют автоматизировать ряд ключевых этапов тестирования безопасности, включая:

- автоматическую генерацию отчётов об обнаруженных уязвимостях на основе анализа исходного кода и сетевого трафика [7];
- систематизацию результатов тестирования с выделением приоритетных угроз в зависимости от уровня их критичности [8];
- построение ранжированных списков рекомендаций по устранению уязвимостей.

Такой подход снижает нагрузку на специалистов и позволяет сократить общее время реакции на выявленные угрозы.

На базе нейросетевых систем возможно развитие интеллектуальных инструментов, способных:

- выявлять слабые места в существующих методах тестирования на основе анализа данных о пропущенных уязвимостях;
- предлагать усовершенствования тестовых сценариев с учётом новых типов атак [5];
- оптимизировать процессы тестирования с учётом динамики развития угроз и изменения инфраструктуры информационных систем.

Внедрение таких инструментов в существующие процессы DevSecOps способно обеспечить не только повышение качества тестирования, но и его адаптацию к быстро меняющимся условиям киберугроз.

### **Интеграция методов машинного обучения и нейросетей в адаптивные системы безопасности**

Адаптивные системы безопасности представляют собой важное направление развития средств защиты информации, основанное на возможности автоматической подстройки под

изменяющийся ландшафт угроз. Применение методов машинного обучения и нейросетей позволяет значительно расширить функциональные возможности таких систем.

Методы машинного обучения обеспечивают:

- автоматизацию анализа данных о событиях безопасности;
- выявление аномалий в сетевом трафике и коде программных продуктов [1], [5];
- прогнозирование вероятности появления новых уязвимостей.

Благодаря этим возможностям системы тестирования безопасности становятся более гибкими и способны быстрее реагировать на появление новых угроз. Кроме того, нейросетевые модели дополняют машинное обучение за счёт: более эффективного выявления сложных и ранее неизвестных аномалий [7], возможности построения самообучающихся механизмов анализа и систематизации данных для формирования стратегий защиты [8]. Таким образом, развитие нейросетевых технологий открывает перспективы построения интеллектуальных адаптивных систем, где процессы тестирования и анализа безопасности будут осуществляться с минимальным участием человека.

### Список литературы

1. ENISA Threat Landscape Report 2023 [Электронный ресурс]. – European Union Agency for Cybersecurity, 2023. – URL: <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023> (дата обращения: 01.07.2024).
2. Supply Chain Compromise of SolarWinds Orion Products [Электронный ресурс] // Cybersecurity & Infrastructure Security Agency. – 2021. – URL: <https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-008a> (дата обращения: 01.07.2024).
3. Li Z., Zou D., Xu S., Jin H., Zhu Y., Chen Z. VulDeePecker: A Deep Learning-Based System for Vulnerability Detection [Электронный ресурс] // arXiv. – 2018. – URL: <https://arxiv.org/abs/1801.01681> (дата обращения: 05.07.2024).
4. Hin D., Kan A., Chen H., Babar M. A. LineVD: Statement-level Vulnerability Detection using Graph Neural Networks [Электронный ресурс] // arXiv. – 2022. – URL: <https://arxiv.org/abs/2203.05181> (дата обращения: 05.07.2024).
5. OWASP Benchmark Project [Электронный ресурс] // OWASP Foundation. – 2024. – URL: <https://owasp.org/www-project-benchmark/> (дата обращения: 15.07.2024).
6. Zhou Y., Liu S., Siow J., Du X., Liu Y. Devign: Effective Vulnerability Identification by Learning Comprehensive Program Semantics via Graph Neural Networks [Электронный ресурс] // Proceedings of the 33rd Conference on Neural Information Processing Systems (NeurIPS 2019). – Vancouver, Canada: NeurIPS Foundation, 2019. – С. 3147-3157. – URL: <https://proceedings.neurips.cc/paper/2019/file/49265d2447bc3bbfe9e76306ce40a31f-Paper.pdf> (дата обращения: 18.07.2024).
7. Feng Z., Guo D., Tang D. et al. CodeBERT: A Pre-Trained Model for Programming and Natural Language Processing [Электронный ресурс] // arXiv. – 2020. – arXiv:2002.08155. – URL: <https://arxiv.org/abs/2002.08155> (дата обращения: 06.05.2025).
8. Chen Z., Komrusch S., Tufano M., et al. SequenceR: Sequence-to-Sequence Learning for End-to-End Program Repair [Electronic resource] // *IEEE Transactions on Software Engineering*. – 2021. – Vol. 47, no. 9. – P. 1943–1959. – DOI: 10.1109/TSE.2019.2940179. – Date of access: 06.05.2025.

9. Cho D.X. A new approach to software vulnerability detection based on CPG and deep learning graph networks // *Cogent Engineering*. – 2023. – Vol. 10, No. 1. – P. 2221962. – DOI: 10.1080/23311916.2023.2221962. – [Electronic resource]. – Available at: <https://doi.org/10.1080/23311916.2023.2221962> (accessed: 05.05.2025).
10. McLaughlin C., Lu Y. Multi-class vulnerability prediction using value flow and graph neural networks // *Neural Computing and Applications*. – 2024. – Vol. 36, No. 25. – P. 15843–15868. – DOI: 10.1007/s00521-024-09819-3. – [Электронный ресурс]. – Режим доступа: <https://link.springer.com/article/10.1007/s00521-024-09819-3> (дата обращения: 05.05.2025).
11. World Economic Forum. Global Cybersecurity Outlook 2023. – [Электронный ресурс]. – Режим доступа: [https://www3.weforum.org/docs/WEF\\_Global\\_Security\\_Outlook\\_Report\\_2023.pdf](https://www3.weforum.org/docs/WEF_Global_Security_Outlook_Report_2023.pdf) (дата обращения: 05.05.2025). 01.07.2024).

## References

1. European Union Agency for Cybersecurity (ENISA). ENISA Threat Landscape Report 2023 [Electronic resource]. – 2023. – Available at: <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023> (accessed: 01.07.2024).
2. Cybersecurity & Infrastructure Security Agency (CISA). Supply Chain Compromise of SolarWinds Orion Products [Electronic resource]. – 2021. – Available at: <https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-008a> (accessed: 01.07.2024).
3. Li Z., Zou D., Xu S., Jin H., Zhu Y., Chen Z. *VulDeePecker: A Deep Learning-Based System for Vulnerability Detection* [Electronic resource] // *arXiv*. — 2018. — Available at: <https://arxiv.org/abs/1801.01681> (accessed: 05.07.2024).
4. Hin D., Kan A., Chen H., Babar M.A. LineVD: Statement-level Vulnerability Detection using Graph Neural Networks [Electronic resource] // *arXiv*. – 2022. – Available at: <https://arxiv.org/abs/2203.05181> (accessed: 05.07.2024).
5. OWASP Foundation. OWASP Benchmark Project [Electronic resource]. – 2024. – Available at: <https://owasp.org/www-project-benchmark/> (accessed: 15.07.2024).
6. Zhou Y., Liu S., Siow J., Du X., Liu Y. Devign: Effective Vulnerability Identification by Learning Comprehensive Program Semantics via Graph Neural Networks [Electronic resource] // In: *Proceedings of the 33rd Conference on Neural Information Processing Systems (NeurIPS 2019)*. – Vancouver, Canada: NeurIPS Foundation, 2019. – pp. 3147–3157. – Available at: <https://proceedings.neurips.cc/paper/2019/file/49265d2447bc3bbfe9e76306ce40a31f-Paper.pdf> (accessed: 18.07.2024).
7. Feng Z., Guo D., Tang D., Duan N., Feng X., Gong M., Shou L., Qin B., Liu T., Jiang D. CodeBERT: A Pre-Trained Model for Programming and Natural Language Processing [Electronic resource] // *arXiv*. – 2020. – arXiv:2002.08155. – Available at: <https://arxiv.org/abs/2002.08155> (accessed: 06.05.2025).
8. Chen Z., Kommrusch S., Tufano M., Watson C., Pouchet L.-N., Poshyvanyk D. SequenceR: Sequence-to-Sequence Learning for End-to-End Program Repair [Electronic resource] // *IEEE Transactions on Software Engineering*. – 2021. – Vol. 47, no. 9. – pp. 1943–1959. – DOI: 10.1109/TSE.2019.2940179. – Available at: <https://doi.org/10.1109/TSE.2019.2940179> (accessed: 06.05.2025).
9. Cho D.X. A new approach to software vulnerability detection based on CPG and deep learning graph networks [Electronic resource] // *Cogent Engineering*. – 2023. – Vol. 10, No. 1. – pp.



Маркевич Д.В. Анализ и перспективы применения машинного обучения и нейросетевых технологий для защиты информационных систем // Международный журнал информационных технологий и энергоэффективности. – 2025. – Т. 10 № 7(57) Ч.1. с. 42–49

---

2221962. – DOI: 10.1080/23311916.2023.2221962. – Available at: <https://doi.org/10.1080/23311916.2023.2221962> (accessed: 05.05.2025).

10. McLaughlin C., Lu Y. Multi-class vulnerability prediction using value flow and graph neural networks [Electronic resource] // Neural Computing and Applications. – 2024. – Vol. 36, No. 25. – pp. 15843–15868. – DOI: 10.1007/s00521-024-09819-3. – Available at: <https://link.springer.com/article/10.1007/s00521-024-09819-3> (accessed: 05.05.2025).
  11. World Economic Forum. Global Cybersecurity Outlook 2023 [Electronic resource]. – Available at: [https://www3.weforum.org/docs/WEF\\_Global\\_Security\\_Outlook\\_Report\\_2023.pdf](https://www3.weforum.org/docs/WEF_Global_Security_Outlook_Report_2023.pdf) (accessed: 05.05.2025).
-



Международный журнал информационных технологий и  
энергоэффективности

Сайт журнала:

<http://www.openaccessscience.ru/index.php/ijcse/>



УДК 004.056:004.7

## ИНТЕГРАЦИЯ DLP И CASB ДЛЯ ЗАЩИТЫ КРИТИЧЕСКИ ВАЖНЫХ ДАННЫХ В ОБЛАКЕ

**Заозерский А.А.**

ФГБОУ ВО САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ  
ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФЕССОРА М. А. БОНЧ-БРУЕВИЧА, Санкт-Петербург,  
Россия (193232, г. Санкт-Петербург, просп. Большевиков, 22, корп. 1), e-mail:  
[spbtown1703@gmail.com](mailto:spbtown1703@gmail.com)

Статья рассматривает интеграцию Data Loss Prevention (DLP) и Cloud Access Security Broker (CASB) для защиты данных в облаке. Описаны уязвимости облачных сред, принципы совместного использования DLP и CASB, методы предотвращения утечек, примеры успешного внедрения и рекомендации по повышению эффективности защиты критически важных данных.

Ключевые слова: DLP, CASB, безопасность облака, защита данных, утечки, контроль доступа.

## INTEGRATION OF DLP AND CASB FOR THE PROTECTION OF CRITICAL DATA IN THE CLOUD

**Zaozersky A.A.**

ST. PETERSBURG STATE UNIVERSITY OF TELECOMMUNICATIONS NAMED AFTER  
PROFESSOR M. A. BONCH-BRUEVICH, St. Petersburg, Russia (193232, St. Petersburg, ave.  
Bolshevikov, 22, bldg. 1), e-mail: [spbtown1703@gmail.com](mailto:spbtown1703@gmail.com)

This article explores the integration of Data Loss Prevention (DLP) and Cloud Access Security Broker (CASB) technologies for securing data in cloud environments. It outlines the vulnerabilities of cloud platforms, the principles of combining DLP and CASB, methods for preventing data leaks, examples of successful implementation, and recommendations for enhancing the protection of critical information.

Keywords: DLP, CASB, cloud security, data protection, data leaks, access control.

### Введение

В условиях цифровой трансформации всё больше компаний переходят на облачные сервисы для хранения и обработки данных. Однако использование публичных и гибридных облаков несёт значительные риски утечки конфиденциальной информации. Для предотвращения подобных угроз применяются решения Data Loss Prevention (DLP) и Cloud Access Security Broker (CASB), которые обеспечивают контроль над данными и доступом к облачным сервисам. DLP-системы позволяют обнаруживать, отслеживать и предотвращать несанкционированную передачу критически важных данных. CASB, в свою очередь, действует как посредник между пользователем и облачными сервисами, обеспечивая контроль доступа, мониторинг активности и защиту от утечек информации. Интеграция этих двух технологий позволяет создать комплексную систему защиты информации в облаке, минимизируя риски несанкционированного доступа и потери данных. В корпоративной среде это особенно актуально, поскольку организации сталкиваются с множеством угроз.

### **Интеграция DLP и CASB для защиты критически важных данных в облаке**

Одной из наиболее распространённых проблем является отсутствие чёткого контроля доступа к облачным хранилищам, что может привести к утечке данных. Пользователи нередко загружают конфиденциальную информацию в небезопасные сервисы, нарушая политики хранения. Иногда данные сохраняются без шифрования, делая их уязвимыми для атак. Использование слабых паролей и отсутствие многофакторной аутентификации также увеличивает риск взлома учётных записей. Кроме того, недостаточная защита API-интерфейсов может привести к утечке данных и атакам на облачную инфраструктуру. Контроль над данными усложняется тем, что информация может находиться за пределами периметра традиционной корпоративной сети, из-за чего мониторинг становится затруднённым. Сотрудники используют личные устройства и сторонние приложения для работы с корпоративной информацией. Механизмы шифрования и маскирования требуют глубокой интеграции с существующей IT-инфраструктурой, что не всегда легко реализовать[1].

Совместное использование DLP и CASB помогает выстроить многоуровневую защиту. CASB анализирует сетевой трафик между пользователем и облачными сервисами, выявляя потенциальные угрозы, в то время как DLP проверяет содержание передаваемых данных, оценивая их чувствительность и соответствие политикам безопасности. Если сотрудник пытается загрузить файл с конфиденциальной информацией в публичный облачный сервис, CASB может заблокировать или ограничить передачу, а DLP зафиксирует инцидент и уведомит службу безопасности[2]. Сотрудники нередко используют несанкционированные облачные платформы для передачи рабочих файлов. CASB выявляет такие приложения и может ограничить их использование, а DLP блокирует попытку передачи критичных данных в ненадёжный сервис. Это предотвращает несанкционированный обмен корпоративной информацией. Интеграция с системами управления доступом позволяет CASB реализовывать политику многофакторной аутентификации, а DLP — задавать уровни конфиденциальности информации. В случаях, когда пользователь пытается загрузить клиентскую базу через незащищённое соединение, CASB может потребовать дополнительную проверку, а DLP зашифрует данные перед отправкой. Обе технологии формируют подробные журналы событий. Это позволяет организациям отслеживать аномалии, проводить регулярный аудит и соответствовать требованиям регуляторов, таких как GDPR, ISO 27001 и HIPAA. Повторяющееся копирование конфиденциальных данных одним пользователем может быть воспринято как возможная инсайдерская угроза и стать предметом расследования[3].

Практика показывает, что такие меры успешно реализуются в различных отраслях. В банковском секторе DLP и CASB позволяют выявлять несанкционированные загрузки клиентских данных в облако и предотвращать их утечку за счёт автоматического шифрования. В здравоохранении CASB помогает обнаруживать подозрительные API-запросы к базам пациентов, а DLP блокирует попытки передачи медицинских данных по незащищённым каналам. В сфере информационных технологий компании успешно ограничивают использование неавторизованных хранилищ для передачи исходного кода и интегрируют решения с SIEM-системами для улучшенного анализа событий. Для эффективного внедрения подобных решений необходимо сначала определить критичные данные, классифицировать их и задать соответствующие политики безопасности. Политики CASB должны быть гибкими, не

только запрещать, но и предлагать альтернативные действия, такие как шифрование. Совместный анализ событий с использованием SIEM позволяет быстрее реагировать на инциденты. Обучение сотрудников безопасной работе с облачными сервисами также является важным фактором снижения рисков[5].

### **Заключение**

Интеграция DLP и CASB позволяет организациям эффективно защищать критически важные данные в облаке, предотвращая утечки информации и обеспечивая соответствие нормативным требованиям, таким как GDPR, HIPAA и ISO 27001. Совместное использование этих решений даёт комплексный контроль над данными, доступом и пользовательской активностью, что особенно важно в условиях активного перехода на облачные технологии и увеличения числа удалённых сотрудников[4]. Правильная реализация DLP и CASB способствует не только защите данных, но и повышению прозрачности облачных сервисов, позволяя компаниям лучше понимать, какие данные обрабатываются и передаются внутри их инфраструктуры. Это снижает вероятность инцидентов, связанных с человеческими ошибками или инсайдерскими угрозами, а также помогает в обнаружении теневых ИТ-ресурсов, которые могут быть источником потенциальных утечек. Несмотря на сложность внедрения и необходимость постоянного управления, DLP и CASB обеспечивают надёжную защиту корпоративных данных, минимизируют риски киберугроз и создают безопасную цифровую экосистему для бизнеса. В будущем ожидается дальнейшее развитие этих технологий, включая автоматизацию обнаружения угроз на основе искусственного интеллекта и машинного обучения, что позволит компаниям ещё более эффективно управлять безопасностью облачных данных.

### **Список литературы**

1. Гельфанд А. М. и др. Организация концептуальной модели критической информационной инфраструктуры //Методы и технические средства обеспечения безопасности информации. – 2020. – №. 29. – С. 39-40.
2. Пешков А. И., Тихонова Э. Н. Информационная безопасность открытых данных //Региональная информатика и информационная безопасность. – 2017. – С. 317-320.
3. Голубов Н. А., Косов Н. А. Внутренние угрозы: Разнообразие и профилактика инсайдеров в организациях. – 2023.
4. Гельфанд А. М. и др. ОЦЕНКА РИСКОВ И УГРОЗ БЕЗОПАСНОСТИ В СРЕДЕ «УМНЫЙ ДОМ» //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2020). – 2020. – С. 316-321.
5. Пестов И. Е. Методика разработки управляющего воздействия на инстансы облачной инфраструктуры //Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. – 2020. – №. 4. – С. 72-76.

### **References**

1. Gelfand A.M. et al. Organization of a conceptual model of critical information infrastructure //Methods and technical means of ensuring information security. 2020. No. 29. pp. 39-40.
2. Peshkov A. I., Tikhonova E. N. Information security of open data //Regional Informatics and information security. 2017. pp. 317-320.

3. Golubev N. A., Kosov N. A. Internal threats: Diversity and prevention of insiders in organizations. – 2023.
  4. Gelfand A.M. et al. ASSESSMENT OF RISKS AND SECURITY THREATS IN THE SMART HOME ENVIRONMENT //Actual problems of infotelec communications in science and education (APINO 2020). 2020. pp. 316-321.
  5. Pestov I. E. Methodology for developing control effects on cloud infrastructure instances //Bulletin of the St. Petersburg State University of Technology and Design. Series 1: Natural and Technical Sciences. - 2020. – No. 4. – pp. 72-76.
-



Международный журнал информационных технологий и энергоэффективности

Сайт журнала:

<http://www.openaccessscience.ru/index.php/ijcse/>



УДК 004.056

## НЕЙРОСЕТИ В ЗАДАЧАХ ПРОГНОЗИРОВАНИЯ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

**Заозерский А.А.**

ФГБОУ ВО САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФЕССОРА М. А. БОНЧ-БРУЕВИЧА, Санкт-Петербург, Россия (193232, г. Санкт-Петербург, просп. Большевиков, 22, корп. 1), e-mail: [spbtown1703@gmail.com](mailto:spbtown1703@gmail.com)

Статья рассматривает использование нейросетевых технологий для прогнозирования угроз информационной безопасности. Описаны типы нейросетей (RNN, LSTM, GRU, CNN) и их применение для анализа логов, сетевого трафика и выявления вредоносного ПО. Подчеркиваются преимущества нейросетей, такие как способность выявлять аномалии и обрабатывать новые угрозы, а также вызовы, связанные с обучением, интерпретируемостью и устойчивостью моделей. Также рассматривается важность комплексного подхода к киберзащите с применением искусственного интеллекта.

Ключевые слова: Информационная безопасность, нейросети, прогнозирование угроз, искусственный интеллект, аномалия, кибератаки, RNN, машинное обучение.

## NEURAL NETWORKS IN THREAT PREDICTION FOR INFORMATION SECURITY

**Zaozersky A.A.**

ST. PETERSBURG STATE UNIVERSITY OF TELECOMMUNICATIONS NAMED AFTER PROFESSOR M. A. BONCH-BRUEVICH, St. Petersburg, Russia (193232, St. Petersburg, ave. Bolshevnikov, 22, bldg. 1), e-mail: [spbtown1703@gmail.com](mailto:spbtown1703@gmail.com)

This article explores the application of machine learning for anomaly detection in network traffic as a key tool in cybersecurity. It describes the stages of data processing, model building and training, as well as the use of algorithms in real-time analysis. The advantages of this approach in identifying new threats are highlighted, along with its limitations, including the need for model updates and managing false positives.

Keywords: Machine learning, anomalies, network traffic, cybersecurity, autoencoder, unsupervised learning, intrusion detection, traffic analysis.

### Введение

Современное информационное пространство развивается стремительными темпами, и вместе с его расширением растёт и количество угроз, связанных с кибербезопасностью. Угрозы становятся всё более изощрёнными, атаки — масштабнее, а последствия — разрушительнее. В таких условиях традиционные методы защиты информации уже не способны обеспечивать надёжную и своевременную реакцию. Это привело к активному внедрению методов искусственного интеллекта, в частности, нейросетей, в задачи прогнозирования и выявления угроз информационной безопасности. Благодаря способности к самообучению, анализу больших объёмов данных и выявлению скрытых закономерностей, нейросети становятся мощным инструментом для предсказания потенциальных инцидентов безопасности и минимизации рисков.

Прогнозирование угроз — это проактивный подход к обеспечению безопасности, когда цель не просто реагировать на уже произошедшие события, а предугадывать и предотвращать атаки до их реализации. В этом контексте нейросети позволяют анализировать аномалии поведения пользователей, сетевой трафик, логи систем, а также взаимодействие различных компонентов цифровой инфраструктуры. Ключевая особенность нейросетей — способность адаптироваться к изменяющимся условиям и обнаруживать нетривиальные взаимосвязи, которые не всегда доступны аналитикам с помощью классических методов.

Одним из самых применимых видов нейросетей в задачах кибербезопасности являются рекуррентные нейронные сети (RNN), особенно их модификации — LSTM и GRU. Эти архитектуры хорошо подходят для анализа временных последовательностей, таких как логи активности, сетевые запросы, сигналы датчиков. На основе прошлых данных они способны выявлять закономерности и предсказывать возможные отклонения от нормального поведения. Например, система может заметить, что определённый пользователь начал в необычное время обращаться к конфиденциальной информации или что объем передаваемых данных резко увеличился — и выдать предупреждение о возможной утечке данных[1].

Кроме того, нейросети могут применяться для построения моделей поведения внутренних и внешних субъектов. Такие модели обучаются на основе исторических данных и используются для определения отклонений, которые могут указывать на вредоносную активность. Это особенно актуально в условиях сложных атак, таких как APT (Advanced Persistent Threat), когда злоумышленник действует скрытно и в течение длительного времени. Выявление таких угроз вручную требует колоссальных ресурсов, в то время как обученная нейросеть может оперативно сигнализировать о подозрительной активности.

Не менее важное направление — обнаружение вредоносного программного обеспечения. Здесь используются сверточные нейросети (CNN), способные классифицировать исполняемые файлы по признакам вредоносности. Суть подхода заключается в том, что бинарный код файла преобразуется в изображение, на котором нейросеть распознаёт характерные «паттерны» вредоносного поведения. Это позволяет выявлять даже ранее неизвестные образцы вредоносных программ, которые еще не занесены в антивирусные базы[2].

Важным преимуществом нейросетей в этих задачах является их способность к обобщению. В отличие от систем, основанных на чётких правилах (rule-based systems), нейросети не ограничиваются заранее заданными сценариями. Это особенно ценно при защите от нулевых угроз (zero-day attacks), для которых отсутствуют сигнатуры или точные описания. Правильно обученная модель может по косвенным признакам распознать аномалию и предупредить о потенциальной атаке, даже если она ранее не встречалась.

Однако внедрение нейросетей в системы информационной безопасности связано с рядом трудностей. Во-первых, требуется большое количество качественных данных для обучения. Причём эти данные должны быть разнородными, репрезентативными и помеченными с высокой точностью. Во-вторых, есть проблема интерпретируемости моделей: нейросети, особенно глубокие, работают как «чёрные ящики», и объяснить, почему именно система сочла ту или иную активность подозрительной, бывает сложно. Это может вызывать затруднения при расследовании инцидентов или принятии решений о блокировке действий пользователя[3].

Ещё одна проблема — устойчивость моделей к манипуляциям. Злоумышленники могут использовать техники атак на искусственный интеллект (adversarial attacks), чтобы вводить нейросети в заблуждение. Например, сгенерировать запрос или поведение, которое будет выглядеть безопасным для модели, но в реальности приведёт к компрометации системы. Поэтому всё больше внимания уделяется разработке устойчивых архитектур и методов повышения доверия к результатам нейросетевых решений.

Немаловажен и вопрос этики: автоматизация принятия решений в области информационной безопасности должна учитывать возможность ложных срабатываний, особенно если речь идёт об ограничении прав пользователей. Например, автоматическая блокировка доступа к ресурсам на основании решения нейросети может вызвать недовольство или привести к срыву бизнес-процессов. Поэтому в ряде случаев решения нейросетей должны использоваться как вспомогательный элемент для аналитика, а не как автономный исполнитель[4].

Нейросети также применяются для анализа социальных медиа и внешней информационной среды, что позволяет выявлять информационные атаки, фишинговые кампании и попытки дискредитации компаний или государственных структур. Обученные модели отслеживают изменение тональности публикаций, рост обсуждений конкретных тем и могут предупреждать о начале организованной кампании ещё до её активной фазы.

Кроме технологического аспекта, значительное внимание уделяется построению комплексных систем, интегрирующих нейросетевые модули с другими механизмами анализа и принятия решений. Такие системы сочетают преимущества машинного обучения, экспертных правил, анализа поведения и визуализации данных. Это позволяет добиться баланса между точностью, скоростью реакции и интерпретируемостью результатов[5].

Развитие облачных технологий и распределённых вычислений также способствует применению нейросетей в задачах кибербезопасности. Обработка больших массивов данных и обучение моделей в облаке позволяет организациям быстро внедрять интеллектуальные инструменты без необходимости в собственных суперкомпьютерных мощностях. Кроме того, появляются решения, использующие федеративное обучение — подход, при котором модели обучаются на распределённых данных без их централизованного сбора, что снижает риски утечек и соответствует требованиям конфиденциальности.

### **Заключение**

Использование нейросетей в задачах прогнозирования угроз информационной безопасности становится неотъемлемой частью современных стратегий киберзащиты. Эти технологии позволяют перейти от реактивной модели к проактивной, что существенно повышает уровень устойчивости к атакам. Несмотря на ряд ограничений и вызовов, таких как необходимость большого количества данных, сложность интерпретации и уязвимость к целенаправленным атакам, нейросети демонстрируют высокую эффективность в обнаружении сложных и скрытых угроз. Будущее информационной безопасности неразрывно связано с развитием искусственного интеллекта, и роль нейросетей в этом контексте будет только возрастать. Важно не только совершенствовать технологии, но и обеспечивать их этичное, надёжное и безопасное применение в условиях постоянно меняющейся среды.

### **Список литературы**



1. Скорых М. А., Израйлов К. Е., Башмаков А. В. Задачаориентированное сравнение средств анализа сетевого трафика //ТЕОРИЯ И ПРАКТИКА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. – 2021. – С. 103-107.
2. Кибирев М. П., Миняев А. А., Скорых М. А. СРАВНИТЕЛЬНЫЙ АНАЛИЗ УТИЛИТ ДЛЯ ПРОВЕДЕНИЯ АТАКИ РТН //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2023). – 2023. – С. 710-715.
3. Волкогонов В. Н., Гельфанд А. М., Деревянко В. С. Актуальность автоматизированных систем управления //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019). – 2019. – С. 262-266.
4. Алехин Р. В. и др. Исследование критической уязвимости сервиса аутентификации и последствий для медицинских учреждений, относящихся к субъектам критической информационной инфраструктуры //Офтальмохирургия. – 2022. – №. 4s. – С. 115-122.
5. Бударный Г. С. и др. Разновидности нарушений безопасности и типовые атаки на операционную систему //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2022). – 2022. – С. 406-411.

#### References

1. . Skorykh M. A., Izrailov K. E., Bashmakov A.V. Task-oriented comparison of network traffic analysis tools //THEORY AND PRACTICE OF INFORMATION SECURITY. – 2021. – PP. 103-107.
  2. Kibirev M. P., Minyaev A. A., Skorykh M. A. COMPARATIVE ANALYSIS OF UTILITIES FOR CONDUCTING A PTH ATTACK //Actual problems of infotelec communications in science and education (APINO 2023). – 2023. – pp. 710-715.
  3. Volkogonov V. N., Gelfand A.M., Derevyanko V. S. Relevance of automated control systems //Actual problems of infotelec communications in science and education (APINO 2019). – 2019. – pp. 262-266.
  4. Alyokhin R. V. et al. Investigation of the critical vulnerability of the authentication service and the consequences for medical institutions related to the subjects of the critical information infrastructure //Ophthalmosurgery. – 2022. – No. 4s. – pp. 115-122.
  5. Budarny G. S. and others. Types of security breaches and typical attacks on the operating system //Actual problems of infotelec communications in science and education (APINO 2022). – 2022. – pp. 406-411.
-



Международный журнал информационных технологий и энергоэффективности

Сайт журнала:

<http://www.openaccessscience.ru/index.php/ijcse/>



УДК 004.056

## МЕТОДЫ ПРОТИВОДЕЙСТВИЯ ФИШИНГУ И СОЦИАЛЬНОЙ ИНЖЕНЕРИИ В КОРПОРАТИВНОЙ СРЕДЕ

**Заозерский А.А.**

ФГБОУ ВО САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФЕССОРА М. А. БОНЧ-БРУЕВИЧА, Санкт-Петербург, Россия (193232, г. Санкт-Петербург, просп. Большевиков, 22, корп. 1), e-mail: [spbtown1703@gmail.com](mailto:spbtown1703@gmail.com)

Статья посвящена методам противодействия фишингу и социальной инженерии в корпоративной среде. Рассматриваются ключевые угрозы, связанные с обманом сотрудников и попытками получить несанкционированный доступ к корпоративной информации. Особое внимание уделено необходимости обучения персонала, внедрению многофакторной аутентификации, использованию технических средств защиты, а также развитию культуры информационной безопасности. Подчеркивается важность комплексного подхода, сочетающего технические, организационные и поведенческие меры.

Ключевые слова: Фишинг, социальная инженерия, корпоративная безопасность, информационная безопасность, обучение сотрудников, многофакторная аутентификация, защита данных, киберугрозы.

## METHODS OF COUNTERING PHISHING AND SOCIAL ENGINEERING IN THE CORPORATE ENVIRONMENT

**Zaozersky A.A.**

ST. PETERSBURG STATE UNIVERSITY OF TELECOMMUNICATIONS NAMED AFTER PROFESSOR M. A. BONCH-BRUEVICH, St. Petersburg, Russia (193232, St. Petersburg, ave. Bolshevikov, 22, bldg. 1), e-mail: [spbtown1703@gmail.com](mailto:spbtown1703@gmail.com)

This article is dedicated to methods of countering phishing and social engineering in the corporate environment. It examines key threats related to employee deception and attempts to gain unauthorized access to corporate information. Special attention is given to the necessity of employee training, the implementation of multi-factor authentication, the use of technical protection tools, and the development of a culture of information security. The importance of a comprehensive approach that combines technical, organizational, and behavioral measures is emphasized.

Keywords: Phishing, social engineering, corporate security, information security, employee training, multi-factor authentication, data protection, cyber threats.

### Введение

Фишинг и социальная инженерия представляют собой одни из наиболее распространенных и опасных угроз в современной корпоративной среде. Эти методы направлены на манипуляцию людьми с целью получения конфиденциальной информации или доступа к корпоративным ресурсам, что может привести к утечке данных, финансовым потерям или повреждению репутации компании. С развитием технологий и увеличением числа кибератак эти угрозы становятся всё более изощрёнными, а значит, важно принимать комплексные меры для защиты сотрудников и корпоративных данных.

Фишинг — это способ обмана, при котором злоумышленники пытаются заставить жертву раскрыть личные данные, например, логины и пароли, через фальшивые электронные письма, веб-сайты или сообщения. Этот метод часто использует элементы доверия, подстраиваясь под привычные действия пользователя, такие как запросы о подтверждении данных, изменение настроек аккаунтов или запросы на перевод средств. Социальная инженерия, в свою очередь, ориентирована на манипулирование людьми с целью получения информации или доступа через личные контакты, звонки, сообщения и другие способы взаимодействия.

Для борьбы с фишингом и социальной инженерией необходимо развивать у сотрудников корпоративной культуры информационной безопасности, что включает в себя как технические, так и организационные меры. Важным элементом защиты является обучение персонала, которое должно стать регулярным процессом, а не единичной акцией. Обучение должно охватывать не только технические аспекты, такие как признаки фишинговых атак, но и психологические аспекты взаимодействия с киберпреступниками, чтобы сотрудники могли адекватно реагировать в ситуациях, когда на них оказывают давление[1].

Одним из важнейших шагов в противодействии фишингу является внедрение многоуровневой аутентификации. Многофакторная аутентификация значительно усложняет задачу злоумышленникам, поскольку даже если они получают логин и пароль, доступ к системе будет ограничен без второго уровня проверки, например, с использованием SMS-кода, биометрии или токена.

Кроме того, важно внедрение систем защиты электронной почты, которые помогают фильтровать подозрительные письма и блокировать фальшивые сообщения. Использование фильтров, которые анализируют содержание сообщений, позволяет уменьшить вероятность того, что фишинговое письмо попадет в почтовый ящик сотрудника. Важно, чтобы эти фильтры регулярно обновлялись и адаптировались к новым методам атак[2].

Технические средства защиты должны быть дополнены регулярными проверками и тестированием сотрудников. Например, проведение фишинговых тренировок в виде моделирования реальных атак позволяет проверять, насколько хорошо сотрудники готовы к выявлению угроз. Эти тренировки не только помогают повысить осведомленность, но и дают возможность оперативно выявить слабые места в процессе безопасности и оперативно их устранить.

Социальная инженерия представляет собой более сложную угрозу, поскольку она воздействует не только на технические, но и на психологические аспекты поведения сотрудников. В отличие от фишинга, который обычно требует от пользователя выполнения конкретных действий (например, перехода по ссылке или ввода личных данных), социальная инженерия использует человеческие слабости и часто требует меньших усилий со стороны злоумышленников.

Чтобы снизить риски социальной инженерии, организациям необходимо разработать строгие внутренние правила по обработке конфиденциальной информации. Например, сотрудники должны быть обучены не раскрывать личные данные по телефону или через электронную почту, если не удостоверились, что собеседник является надежным. Важным шагом является внедрение системы проверки личности сотрудников и партнёров компании, что может помочь предотвратить попытки манипуляции[3].

Не менее важным аспектом защиты является регулярный аудит безопасности. Он позволяет выявлять уязвимости в текущих процессах и методах защиты, а также помогает создавать более эффективные политики безопасности. В дополнение к этому, важно наладить чёткую процедуру уведомления о возможных инцидентах. Сотрудники должны понимать, как и кому сообщать о подозрительных действиях и что делать в случае сомнений.

Еще одной мерой защиты является использование системы защиты от утечек данных (DLP). Эти системы отслеживают движение информации в сети и блокируют попытки несанкционированного доступа или утечек данных. Такие системы могут предотвратить, например, отправку конфиденциальных документов на внешние ресурсы или попытки копирования данных на внешний носитель[4].

Ключевым элементом в обеспечении безопасности является создание культуры ответственности за данные и безопасность на всех уровнях компании. Важно, чтобы защита данных не ограничивалась только IT-отделом. Все сотрудники должны понимать свою роль в поддержке безопасности, начиная от руководителей и заканчивая техническими специалистами. В связи с этим следует активно развивать культуру внимательности и осведомленности о рисках, что будет способствовать выработке правильных реакций и действий в случае угроз[5].

### **Заключение**

Проблемы фишинга и социальной инженерии остаются актуальными для большинства организаций, и только комплексный подход, включающий технические средства защиты, организационные меры и постоянное обучение персонала, может эффективно снизить риски. Важно, чтобы компания осознавала важность не только внедрения технологических решений, но и формирования правильного отношения к безопасности среди сотрудников. Чем более осведомленными будут сотрудники, тем труднее станет злоумышленникам манипулировать их действиями и использовать их в своих целях.

### **Список литературы**

1. Виткова Л. А. и др. Конвергенция информационных технологий для повышения эффективности управления информационным пространством Санкт-Петербурга //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2018). – 2018. – С. 140-142.
2. Гельфанд А. М. и др. Организация концептуальной модели критической информационной инфраструктуры //Методы и технические средства обеспечения безопасности информации. – 2020. – №. 29. – С. 39-40.
3. Бударный Г. С. и др. Разновидности нарушений безопасности и типовые атаки на операционную систему //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2022). – 2022. – С. 406-411.
4. Гельфанд А. М. и др. ОЦЕНКА РИСКОВ И УГРОЗ БЕЗОПАСНОСТИ В СРЕДЕ «УМНЫЙ ДОМ» //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2020). – 2020. – С. 316-321.
5. Алехин Р. В. и др. Исследование критической уязвимости сервиса аутентификации и последствий для медицинских учреждений, относящихся к субъектам критической информационной инфраструктуры //Офтальмохирургия. – 2022. – №. 4s. – С. 115-122.

## References

1. Vitkova L. A. and others. Convergence of information technologies to improve the management efficiency of the St. Petersburg information space //Actual problems of infotelec communications in science and education (APINO 2018). 2018. pp. 140-142.
  2. Gelfand A.M. et al. Organization of a conceptual model of critical information infrastructure //Methods and technical means of ensuring information security. - 2020. – No. 29. – pp. 39-40.
  3. Budarny G. S. and others. Types of security breaches and typical attacks on the operating system //Actual problems of infotelec communications in science and education (APINO 2022). – 2022. – pp. 406-411.
  4. Gelfand A.M. et al. ASSESSMENT OF RISKS AND THREATS TO SECURITY IN THE SMART HOME ENVIRONMENT //Actual problems of infotelec communications in science and education (APINO 2020), 2020, pp. 316-321.
  5. Alekhine R. V. and others. Investigation of the critical vulnerability of the authentication service and the consequences for medical institutions related to the subjects of the critical information infrastructure //Ophthalmosurgery. – 2022. – No. 4s. – pp. 115-122.
-



Международный журнал информационных технологий и  
энергоэффективности

Сайт журнала:

<http://www.openaccessscience.ru/index.php/ijcse/>



004.8

## ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В МОДЕ: ВЛИЯНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА НА ИНДУСТРИЮ МОДЫ

<sup>1</sup>Голубкова И.Л., Зеленина Л.И. (научный руководитель)

ФГБОУ ВО "РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА И  
ГОСУДАРСТВЕННОЙ СЛУЖБЫ ПРИ ПРЕЗИДЕНТЕ РФ" СЕВЕРО-ЗАПАДНЫЙ  
ИНСТИТУТ УПРАВЛЕНИЯ (ФИЛИАЛ), Санкт-Петербург, Россия (199178, город Санкт-  
Петербург, пр-кт Средний В.О., д. 57/43), e-mail: <sup>1</sup>golubkova irinal23@mail.ru

Искусственный интеллект всё активнее проникает в индустрию моды. В этой статье мы рассмотрим, как именно искусственный интеллект проникает в модный бизнес, какие системы созданы на его основе. А также сделаем обзор ведущих сервисов и платформ, использующих искусственный интеллект для анализа трендов, поиска вещей, виртуальной примерки и даже генерации новых моделей.

Ключевые слова: Искусственный интеллект, fashion-индустрия, модная индустрия, инструменты искусственного интеллекта, ИИ, мода, инновации в моде, виртуальные модели, компьютерное зрение и мода.

## ARTIFICIAL INTELLIGENCE IS IN FASHION: THE INFLUENCE OF ARTIFICIAL INTELLIGENCE ON THE FASHION INDUSTRY

<sup>1</sup>Golubkova I.L., Zelenina L.I. (scientific supervisor)

RUSSIAN PRESIDENTIAL ACADEMY OF NATIONAL ECONOMY AND PUBLIC  
ADMINISTRATION NORTH-WEST INSTITUTE OF MANAGEMENT (BRANCH), St. Petersburg,  
Russia (57/43 Sredniy V.O., pr-kt St. Petersburg, St. Petersburg, 199178), e-mail:  
<sup>1</sup>golubkova irinal23@mail.ru

Artificial intelligence is increasingly penetrating the fashion industry. In this article, we will look at exactly how artificial intelligence penetrates the fashion business, and what systems are created based on it. We will also review the leading services and platforms that use artificial intelligence to analyze trends, find things, try on virtual models, and even generate new models.

Keywords: Artificial intelligence, fashion industry, fashion industry, artificial intelligence tools, AI, fashion, innovations in fashion, virtual models, computer vision and fashion.

В эпоху стремительного развития искусственного интеллекта (ИИ) его внедрение затронуло все сферы жизни, включая индустрию моды. ИИ проник в каждый уголок мира, почти каждый второй человек использует искусственный интеллект, например, чтобы узнать рецепт пирога или для написания плана развития социальной сети. Сейчас нейронные сети можно использовать для бизнеса, учебы или просто для развлечений. Около 55% компаний на данный момент используют искусственный интеллект.[7] По данным Statista каждый год рынок искусственного интеллекта увеличивается на 20%. По данным Forbes самый частый запрос ИИ – ответить на сообщения, они составляют 45%, потом идет помощь с финансовыми вопросами – 43%, планирование маршрута – 38%, создание электронных писем – 31%,

подготовка к собеседованию – 30%, и еще огромное количество запросов. [6] Индустрия моды не стала исключением.

ИИ стремительно меняет индустрию моды, открывая новые горизонты для всех потребителей. Дизайнеры, бренды, стилисты, да и просто люди, каждый день используют нейросети. От автоматизированного создания уникальных дизайнов до персонализированных рекомендаций в стиле. Технологии на основе нейросетей трансформируют привычные процессы и делают моду более инновационной и доступной.

Этот технологический прорыв открывает перед модной индустрией беспрецедентные возможности. Искусственный интеллект уже сейчас помогает брендам оптимизировать производство, снижать издержки и предлагать клиентам более точные и удобные решения. Он не только анализирует тренды, но и предсказывает, какие стили и модели будут востребованы в будущем. Согласно данным, компании, которые используют ИИ для персонализации предложений, отмечают увеличение продаж на 50%. [4] Более того, примерно 59% организаций внедряют нейросети для увеличения прибыли. [5]

В 2023 году прошла первая в мире неделя моды ИИ — AI Fashion Week.[10] В ней захотели поучаствовать около 400 дизайнеров, которые захотели показать миру свои коллекции. На данном показе все люди и элементы одежды и аксессуар – всё было создано ИИ. Многие популярные журналы поддержали такую идею. Но также была и другая сторона, в социальных сетях пошла волна, которая просила остановить такие показы.



Рисунок 1 - Модели с Fashion Week AI. Источник Habr.



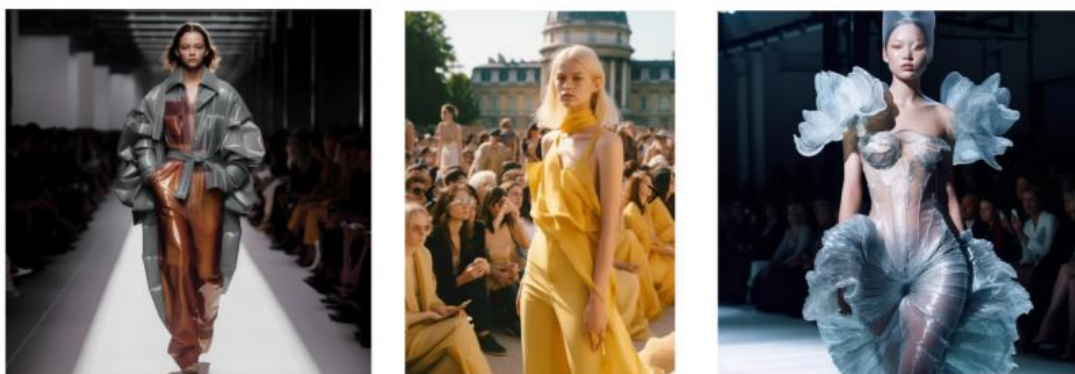


Рисунок 2 - Победители AI Fashion Week 2023:  
слева направо - Paatiff, Matilde Mariano, OPE (Фото: AIFW)

Ещё один пример работы с нейронными сетями показал цифровой художник Зак Кревитт, которого пригласил дизайнер одежды Вилли Норрис для своего бренда Outlier [11]. Зак с помощью нейросети заменил лица моделей на лица пришельцев, что вышло довольно эксцентрично и забавно. После этого дизайнер для показа напечатал такие маски. [8]

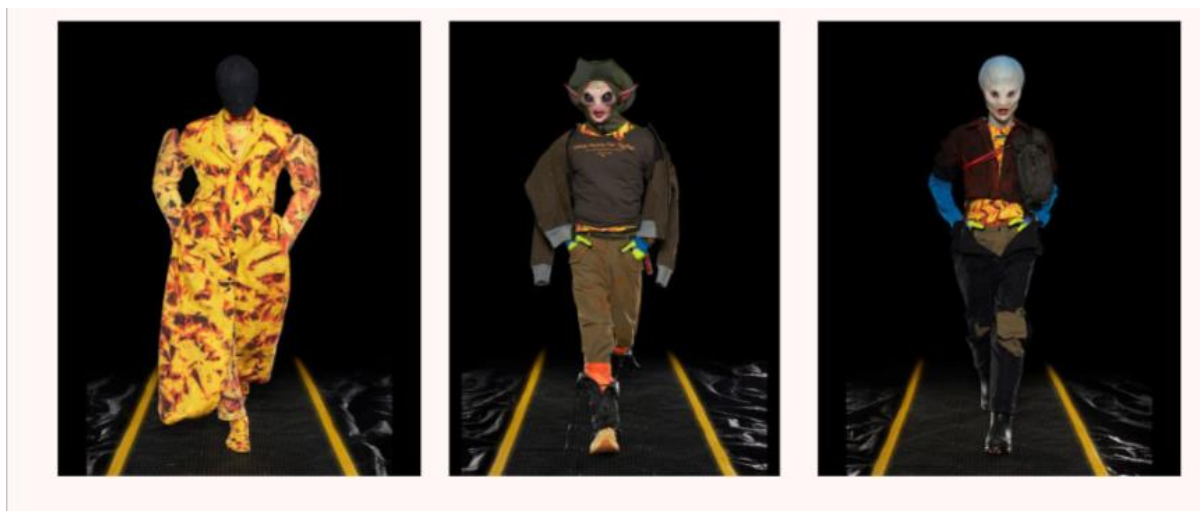


Рисунок 3 - Коллекция бренда Outlier (Фото:red.eyе)

ИИ может генерировать новые коллекции для модных домов, анализируя глобальные данные о моде, культурные тенденции, веяния моды и предлагать персонализированные рекомендации, которые могут быть адаптированы к конкретным рынкам или даже индивидуальным предпочтениям. Дизайнеры могли бы сотрудничать с ИИ, расширяя свои творческие границы и экспериментировать с новыми формами и материалами. [2] Существуют нейросети, позволяющие создавать уникальные принты и дизайны, например генеративные модели, такие как GANs, могут обучаться на огромных выборках изображений и после создавать собственные принты. Такие нейросети использовали компания H&M и модный дом Balenciaga для создания линейки одежды с принтами. [9].

ИИ используется в мире моды в разных его представлениях. Одной из главных тенденций по праву может считаться система распознавания. Сколько раз за день нам попадается целая подборка похожих товаров, после того как на Wildberries или Ozon



закончился товар или не подходит размер — это всё алгоритм нейросети. Чаще всего покупатели одежды и аксессуаров не знают, какой марки вещь они хотят, потому что просто увидели красивую сумку на улице или у какого-нибудь fashion-инфлюенсера на фотографии и захотели такую же. Сервисы, заточенные на поиск объекта по картинке, как раз основанные на ИИ-механизмах, используются повсеместно. На данный момент такие визуальные поисковики есть у Google, Pinterest, Lamoda, Яндексa и не только у них. [1]

В сфере розничной торговли товарами модной индустрии искусственный интеллект активно применяется для анализа данных для брендов, что позволяет лучше понимать потребности клиентов и предлагать более актуальных продуктов. Это способствует повышению удовлетворенности клиентов, и как следствию, росту продаж. По найденным данным, примерно 73% потребителей готовы использовать чат-боты на основе ИИ, а 60% уже их применяли.

На основе искусственного интеллекта создано достаточное количество платформ, начиная от помощников в выборе одежды и заканчивая платформами для подбора стиля. Некоторые представляют интерес для профессионалов, а некоторые понятны и для обычных пользователей. Так как в интернете размещено огромное количество сайтов и приложений, связывающих моду и искусственный интеллект, дальше будут рассмотрены самые интересные и практичные из них.

Существует, так называемый “Shazam для одежды” – сайт [Lykdat](#). Он существует для поиска вещи по фотографии, там можно сразу перейти по ссылке и приобрести понравившуюся вещь. Платформа использует алгоритмы компьютерного зрения и машинного обучения для анализа предоставленных изображений, для определения характеристик, например узора и цвета. На сайте удобный интерфейс, также можно отфильтровать по необходимым критериям, например по сегменту вещи и валюте. [3]

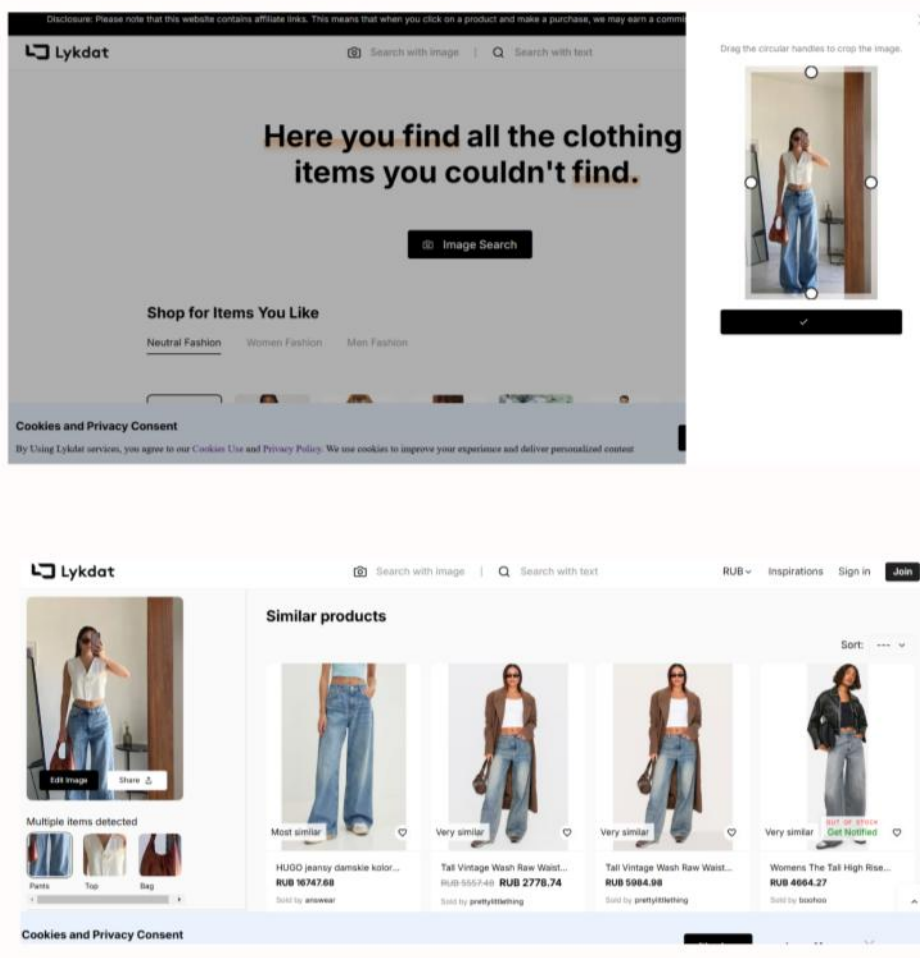


Рисунок 4 - Интерфейс сайта Lykdat

Похожий по своим свойствам визуальный поиск есть у интернет-магазина Lamoda. Пользователь загружает фотографию вещи, которую хочет найти и приложение само находит данную вещь и предлагает похожую. Но в сервисе Lamoda можно загрузить фотографию с целым образом и система, проанализировав картинку, выдаст результаты по категориям и сегментам. Например, можно найти из образа только юбку и добавить в корзину или добавить все товары для полноты образа. Визуальный поиск упрощает шопинг и позволяет сэкономить время на другие дела, потому что не надо часами сидеть и искать вещь, у которой помнишь только цвет.

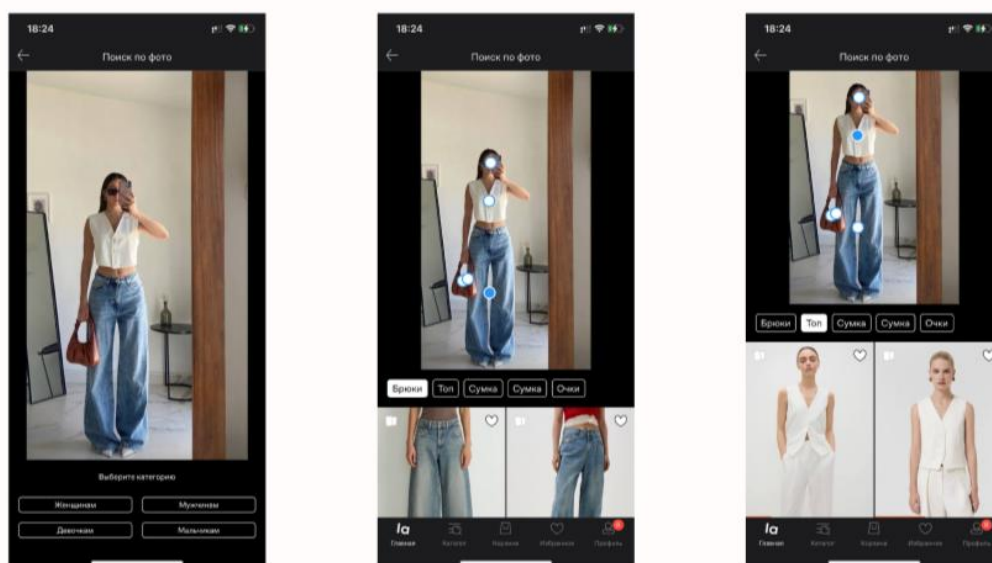


Рисунок 5 - Интерфейс визуального поиска Lamoda

Ещё одна интересная платформа на основе искусственного интеллекта [STYLERISER](#). Данная платформа предлагает виртуального помощника, который поможет подобрать одежду или аксессуары под ваши предпочтения по стилю на основе ваших черт лица, таких как оттенок кожи, цвета глаз и формы лица. Правильно подобранный, стиль необходим в нынешних условиях, а на самостоятельный разбор уходит очень много времени, такие платформы значительно сокращают время и минимизируют возможность ошибки. Данные на сайте хранятся 30 дней. (меньше выбор, развить тему)

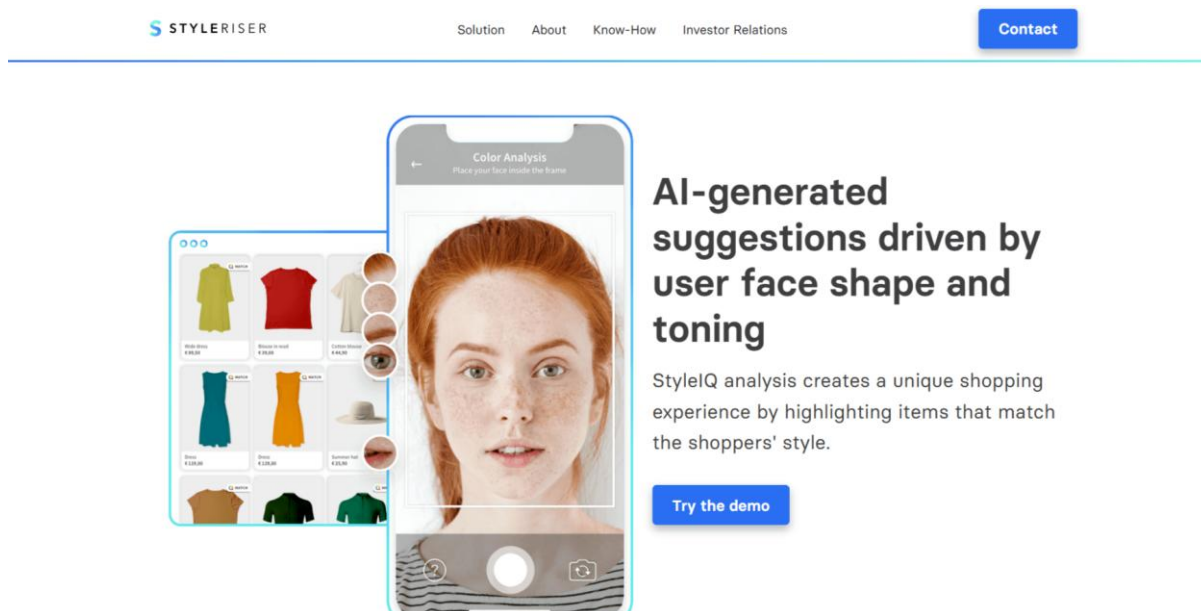


Рисунок 6 - Интерфейс платформы STYLERISER

Искусственный интеллект стремительно меняет жизнь, проникая во всех сферы. Он делает технологии более удобными, автоматизирует рутинные задачи и помогает находить инновационные решения. ИИ кардинально меняет модную индустрию, делая её более

инновационной, персонализированной и устойчивой. Благодаря ИИ бренды и стилисты могут прогнозировать тренды, создавать виртуальных моделей и улучшать пользовательский опыт через индивидуальные рекомендации. Эти технологии помогают компаниям не только повышать эффективность, но и делать моду более доступной и инклюзивной. Однако, несмотря на все преимущества, развитие искусственного интеллекта ставит перед обществом новые вызовы, такие как этика использования данных, замещение рабочих мест и необходимость регулирования технологий. В будущем нейросети продолжит совершенствоваться и открывать больше возможностей, но необходимо найти баланс между технологическим прогрессом и ответственным его применением.

### Список литературы

1. Смотрим в «Черное зеркало»: как нейросети уже используются в моде и что будет дальше. Правила жизни, 2023. URL: <https://www.pravilamag.ru/life-style/696515-smotrim-sya-v-chnoe-zerkalo-kak-neiroseti-uje-ispolzuyutsya-v-mode-i-chno-budet-dalshe/> (дата обращения: 18.03.2025).
2. AI в модной индустрии и ритейле: как технологии меняют фэшн-бизнес. Ultralytics, 2023. URL: <https://www.ultralytics.com/ru/blog/ai-in-fashion-retail> (дата обращения: 18.03.2025).
3. 10 лучших AI-инструментов для модной индустрии в 2023 году. Mpost.io, 2023. URL: <https://mpost.io/ru/10-best-ai-tools-for-fashion-in-2023/> (дата обращения: 18.03.2025).
4. Как искусственный интеллект увеличивает продажи: примеры и статистика // BotSeller.AI, 2024. URL: <https://botseller.ai/blog/ai-dlya-biznesa/sales-without-borders-with-an-ai-seller.html> (дата обращения: 18.03.2025).
5. Влияние искусственного интеллекта на производительность и прибыль бизнеса // IntellectDialog, 2024. URL: <https://intellectdialog.com/blog/iskusstvennyy-intellekt-vliyanie-na-proizvoditelnost> (дата обращения: 18.03.2025).
6. Статистика искусственного интеллекта // ИНКЛИЕНТ URL: <https://inclient.ru/ai-stats/> (дата обращения: 05.04.2025).
7. Искусственный интеллект в 2024 году: статистика и факты // VC.RU URL: <https://vc.ru/money/1335638-iskusstvennyi-intellekt-v-2024-godu-statistika-i-fakty> (дата обращения: 05.04.2025).
8. Конец эпохи fashion-дизайнеров? Как ИИ меняет мир моды // HABR URL: <https://habr.com/ru/articles/857038/> (дата обращения: 05.04.2025).
9. Как искусственный интеллект меняет модную индустрию // РБК Тренды URL: <https://trends.rbc.ru/trends/industry/6720bb5d9a7947638317dce6> (дата обращения: 05.04.2025).
10. AI FASHION WEEK SEASON 1 // AI FASHION WEEK URL: <https://fashionweek.ai/season-1/> (дата обращения: 06.04.2025).
11. Capturing the Futuristic Essence: Unveiling Outlier Fall 23 Collection with Zak Krevitt // red.eye URL: <https://red-eye.world/c/capturing-the-futuristic-essence-unveiling-outlier-fall-23-collection-with-zak-krevitt> (дата обращения: 06.04.2025).

### References

1. . We look into the "Black Mirror": how neural networks are already being used in fashion and what will happen next. Rules of Life, 2023. URL: <https://www.pravilamag.ru/life->

- style/696515-smotrimsy-a-v-chnoe-zerkalo-kak-neiroseti-uje-ispolzuyutsya-v-mode-i-chno-budet-dalshe / (accessed: 03/18/2025).
2. AI in the fashion industry and retail: how technology is changing the fashion business. Ultralytics, 2023. URL: <https://www.ultralytics.com/ru/blog/ai-in-fashion-retail> (date of request: 03/18/2025).
  3. The 10 best AI tools for the fashion industry in 2023. Mpost.io , 2023. URL: <https://mpost.io/ru/10-best-ai-tools-for-fashion-in-2023> / (accessed: 03/18/2025).
  4. How artificial intelligence increases sales: examples and statistics // BotSeller.AI, 2024. URL: <https://botseller.ai/blog/ai-dlya-biznesa/sales-without-borders-with-an-ai-seller.html> (date of request: 03/18/2025).
  5. The impact of artificial intelligence on business productivity and profit // IntellectDialog, 2024. URL: <https://intellectdialog.com/blog/iskusstvennyy-intellekt-vliyanie-na-proizvoditelnost> (date of access: 03/18/2025).
  6. Artificial intelligence statistics // INCLUSIVE URL: <https://inclient.ru/ai-stats> / (date of access: 04/05/2025).
  7. Artificial intelligence in 2024: statistics and facts // VC.RU URL: <https://vc.ru/money/1335638-iskusstvennyi-intellekt-v-2024-godu-statistika-i-fakty> (date of request: 04/05/2025).
  8. The end of the era of fashion designers? How AI is changing the fashion world // HABR URL: <https://habr.com/ru/articles/857038> / (date of access: 04/05/2025)
  9. How artificial intelligence is changing the fashion industry // RBC Trends URL: <https://trends.rbc.ru/trends/industry/6720bb5d9a7947638317dce6> (accessed: 04/05/2025).
  10. AI FASHION WEEK SEASON 1 // AI FASHION WEEK URL: <https://fashionweek.ai/season-1> / (date of request: 04/06/2025).
  11. Capturing the Futuristic Essence: Unveiling Outlier Fall 23 Collection with Zak Krevitt // red.eye URL: <https://red-eye.world/c/capturing-the-futuristic-essence-unveiling-outlier-fall-23-collection-with-zak-krevitt> (date of request: 04/06/2025).
-



Международный журнал информационных технологий и  
энергоэффективности

Сайт журнала:

<http://www.openaccessscience.ru/index.php/ijcse/>



УДК 004.056

## АРХИТЕКТУРА СИСТЕМЫ ВЫЯВЛЕНИЯ И ПРОТИВОДЕЙСТВИЯ ВРЕДОНОСНЫМ ДИПФЕЙКАМ

**Волков М.Д.**

ФГБОУ ВО САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ  
ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФЕССОРА М. А. БОНЧ-БРУЕВИЧА, Санкт-Петербург,  
Россия (193232, г. Санкт-Петербург, просп. Большевиков, 22, корп. 1), e-mail:  
[rexendrprorpror@gmail.com](mailto:rexendrprorpror@gmail.com)

С развитием технологий дипфейков возможности манипуляции аудио- и видеоконтентом стали угрозой для частной жизни, публичной репутации и информационной безопасности. Современные методы создания дипфейков, основанные на глубоких нейронных сетях, требуют внедрения новых систем защиты, способных обнаруживать поддельные материалы с высокой точностью. В данной статье рассматриваются ключевые подходы к детекции дипфейков, включая использование сверточных нейронных сетей и трансформеров, а также их комбинирование для повышения эффективности.

Ключевые слова: Дипфейк; детекция; безопасность данных; искусственные нейронные сети; трансформеры.

## ARCHITECTURE OF THE SYSTEM FOR DETECTING AND COUNTERING MALICIOUS DEEPFAKES

**Volkov M.D.**

ST. PETERSBURG STATE UNIVERSITY OF TELECOMMUNICATIONS NAMED AFTER  
PROFESSOR M. A. BONCH-BRUEVICH, St. Petersburg, Russia (193232, St. Petersburg, ave.  
Bolshevikov, 22, bldg. 1), e-mail: [rexendrprorpror@gmail.com](mailto:rexendrprorpror@gmail.com)

With the advancement of deepfake technology, the manipulation of audio and video content poses a serious threat to privacy, public reputation, and information security. Modern methods of deepfake creation, based on deep neural networks, necessitate the development of new detection systems capable of identifying fake materials with high precision. This article explores key approaches to deepfake detection, including the use of convolutional neural networks and transformers, as well as their combination to enhance effectiveness.

Keywords: Deepfake; detection; data security; artificial neural networks; transformers.

Современные технологии «deepfake» представляют серьезную угрозу информационной безопасности и личной приватности. Deepfake — это синтетический медиаконтент, созданный с использованием искусственного интеллекта, который способен имитировать визуальные и аудиоданные реальных людей с высокой степенью достоверности.

Примеры использования технологии дипфейков в мошеннических целях в России демонстрируют, насколько опасными могут быть такие методы в реальном мире. Вот несколько случаев:

*Хищение средств с использованием дипфейков:* Центральный банк России в 2024 году отметил рост случаев мошенничества с применением дипфейков. Злоумышленники создают реалистичные видеоролики, где изображают знакомых своих жертв, например, друзей или

родственников, прося деньги для "срочных нужд". Часто такие поддельные сообщения сопровождаются реалистичным голосом и мимикой, которые трудно отличить от реальных.

*Использование дипфейков в корпоративной среде:* [1] Зампред правления Сбербанка Станислав Кузнецов сообщил, что такие технологии уже применяются для атак на компании. Например, подделываются видео и аудио руководителей с целью получения доступа к корпоративным ресурсам или денежным средствам

*Политический контекст:* В 2023 году технология дипфейков использовалась для создания видеовопросов президенту России Владимиру Путину, которые вызвали значительный общественный интерес. Хотя это событие не имело мошеннических намерений, оно показало, как технологии могут быть использованы для манипуляции общественным мнением и информацией [2]

В условиях цифровизации общества и растущей доступности deepfake инструментов разработка систем их выявления и противодействия становится приоритетной задачей.

### **Цели и задачи**

Цель данного исследования заключается в систематизации и анализе ключевых компонентов архитектуры современных систем выявления дипфейков. [3] Основное внимание уделяется методам обработки медиафайлов, выявлению аномалий, а также использованию нейросетевых моделей для повышения точности и эффективности детекции. В рамках работы будут рассмотрены основные подходы к обработке видео и изображений для выявления подделок, такие как предварительная обработка данных, анализ аномалий в движении лиц и синхронизации речи, а также использование сверточных нейронных сетей и трансформеров для более глубокого анализа. Цель исследования — представить комплексное описание архитектуры таких систем и предложить пути улучшения их эффективности, принимая во внимание последние достижения в области искусственного интеллекта и машинного обучения.

### **Архитектура системы выявления и противодействия дипфейкам**

После определения цели система выстраивается в четкую последовательность этапов, каждая из которых решает свою задачу и направлена на максимальное повышение точности обнаружения поддельного контента. Все эти элементы вместе формируют гибкую архитектуру, способную адаптироваться к новым угрозам.

### **Часть 1. Определение вредоносного дипфейка**

Первым шагом в системе распознавания дипфейков является не только идентификация поддельного контента, но и определение его потенциальной вредоносности. Не все дипфейки создаются с намерением нанести вред: существует множество примеров использования этой технологии в развлечениях, рекламе и обучении. Однако распознавание зловредных дипфейков, таких как те, которые используются для дезинформации или мошенничества, требует более сложного подхода. [4]

#### *Основные критерии для оценки вредоносности дипфейка*

1. *Контекст и намерение:* Система должна учитывать, в каком контексте используется видео. Например, дипфейк, распространяемый с целью шутки в кругу друзей, отличается от подделки, нацеленной на дискредитацию политика. Анализ метаданных и

социальных факторов (например, каналы распространения и комментарии) может помочь системе определить возможное намерение автора. [5]

2. *Содержимое видео:* Некоторые признаки указывают на потенциальную вредоносность. Это могут быть видеоролики с явным нарушением репутации личности, содержащие ложные заявления или вводящие в заблуждение кадры. Например, поддельное видео с политиком, говорящим то, чего он никогда не произносил, почти наверняка будет классифицировано как вредоносное.

3. *Анализ аудио и речи:* Поддельные аудиотреки могут сопровождаться ложной интонацией, несоответствующей контексту сообщения, или неестественной скоростью речи. Такие особенности могут быть признаками манипуляции, особенно в случае пропаганды или мошеннических звонков, использующих дипфейковую речь для обмана. [6]

## **Часть 2. Этап подготовки данных**

Перед анализом все входящие данные требуют тщательной подготовки. Видео и изображения очищаются от визуального шума и приводятся к стандартному формату, чтобы алгоритмы могли корректно выделять ключевые признаки. Например, разрешение видео нормализуется, а чрезмерная яркость или затемненность изображения корректируется до приемлемых уровней. Эти шаги не только улучшают качество данных, но и устраняют внешние помехи, которые могут маскировать признаки подделки.

Интересное исследование в этом направлении было проведено с использованием датасета FaceForensics++. Команда ученых заметила, что даже минимальное улучшение качества входных данных, например, восстановление текстуры кожи, значительно повышает точность анализа. В их эксперименте этот подход обеспечил до 12% прироста точности в работе с поддельными видео.

## **Часть 3. Выявление скрытых аномалий**

На следующем этапе работы системы выявления дипфейков ключевым является обнаружение аномалий, которые нехарактерны для подлинных медиафайлов. Одним из таких параметров является синхронизация речи и движений губ. В реальных видео мимика и звуки речи всегда взаимосвязаны, что делает любые отклонения от этой синхронности очевидными. В дипфейках алгоритмы часто допускают ошибки, такие как опережение речи относительно движений рта или полное отсутствие синхронности. Например, в высококачественных дипфейках, где визуальные ошибки практически [7] незаметны, такие временные несоответствия остаются заметными и могут быть использованы для успешной детекции. [8] Исследования, использующие датасет **LipForensics**, продемонстрировали точность более 96% при выявлении подобных отклонений, даже когда визуальные элементы были практически безупречны.

Еще одним ярким примером аномалии являются ошибки в освещении и теняльных видео освещенность и тени всегда подчиняются законам физики, то есть тени должны логически следовать за источниками света и формировать ожидаемое распределение. В дипфейках же часто бывают нелогичные или искусственно исправленные тени, что может указывать на подделку. Например, исследование, проведенное на датасете *DFDC*, показало, что в 70% случаев использование алгоритмов для анализа несовпадений в тенях и освещении позволяет точно идентифицировать подделку. [9] Эти ошибки особенно заметны, когда



освещение на лице персонажа не совпадает с общими источниками света на фоне, что делает видео искусственным.

Кроме того, дипфейки часто страдают от нехватки естественных микродвижений, таких как моргание глаз или изменения выражений лица. В реальных видео эти микродвижения происходят автоматически и незаметно для зрителя, однако в подделках такие движения либо отсутствуют, либо происходят в несоответствующем ритме, что выдает искусственную природу изображения. Например, в дипфейках часто можно наблюдать лица, которые не моргают или моргают очень редко, что является явным признаком подделки. Такие аномалии также активно используются для разработки алгоритмов детекции, поскольку они легко выявляются при сравнении с реальными видеоматериалами. [2] Другой важной особенностью дипфейков является проблема текстурных ошибок, связанных с кожей и другими поверхностями. В процессе генерации изображений с помощью алгоритмов типа GAN (Generative Adversarial Networks) часто возникают странные текстурные дефекты, такие как повторяющиеся узоры, сглаженные участки или артефакты, которые не встречаются в реальных видео. Эти аномалии могут быть трудно заметны на фоне высокого качества изображения, но с помощью специализированных алгоритмов анализа текстур можно эффективно выявить такие ошибки.

Наконец, не менее важными являются аномалии в динамике движений головы и тела. В реальных видео движения человека подчиняются биомеханическим закономерностям, что делает их естественными и плавными. В дипфейках же часто наблюдаются странности в движении головы, такие как резкие повороты или непропорциональная скорость, что делает движение человека неестественным. Это также является характерной особенностью, по которой можно определить подделку.

В целом, все эти аномалии — это не просто случайные ошибки, а закономерные следствия ограничений алгоритмов, создающих дипфейки. Современные системы детекции направлены на использование этих аномалий для выявления подделок, анализируя как локальные особенности, так и более сложные временные и пространственные взаимосвязи. Технологии, учитывающие такие отклонения, становятся все более эффективными, позволяя достигать высокой точности в идентификации медиафайлов с измененной информацией. [10]

#### **Часть 4. Использование нейросетей**

Нейросетевые модели занимают центральное место в распознавании дипфейков благодаря своей способности анализировать как отдельные изображения, так и видеопоследовательности с учётом временных и пространственных зависимостей. Основными инструментами в этой области являются *сверточные нейронные сети (CNN)* и *трансформеры*. Эти модели успешно справляются с задачами выявления мельчайших аномалий, которые незаметны при обычном визуальном анализе. [11]

##### *Сверточные нейронные сети (CNN)*

Сверточные нейронные сети традиционно используются для обработки изображений. Они анализируют локальные особенности — текстуры, границы, контуры — что делает их особенно эффективными для выявления визуальных аномалий на лицах и других поверхностях.

##### *Принципы работы CNN в детекции дипфейков:*

1. *Анализ текстур*: CNN способны выявлять дефекты, возникающие из-за работы генеративных алгоритмов. Например, дипфейковые лица могут содержать сглаженные участки кожи или искажённые блики, что редко встречается в реальных изображениях.

2. *Детекция артефактов*: CNN хорошо справляются с нахождением повторяющихся узоров или мелких несовпадений, таких как искажения в области глаз, рта или носа.

### **Практические примеры:**

- В проекте FaceForensics++, исследователи использовали CNN для анализа текстурных особенностей видео, что позволило добиться точности до 95%. Модель могла легко идентифицировать ошибки, незаметные для человеческого глаза, такие как неестественные градиенты освещения или артефакты на границах лица.
- Проект DeepFake Detection Challenge (DFDC) применял CNN для анализа микродеталей, таких как частота моргания и микродвижения глаз. Это позволило эффективно выявлять несоответствия в поведении персонажей, особенно в видео с высоким разрешением [6] *Трансформеры*

Трансформеры, такие как *Vision Transformer (ViT)* и другие их вариации, более эффективны при анализе временных и пространственных зависимостей. В отличие от CNN, которые фокусируются на отдельных изображениях, трансформеры анализируют последовательности кадров, что особенно важно для видео.

### *Особенности применения трансформеров:*

1. *Анализ последовательностей*: Трансформеры анализируют временные закономерности, выявляя аномалии в движении губ, глаз или головы.
2. *Контекстуальный анализ*: Эти модели способны учитывать не только изображение, но и его окружение, что позволяет распознавать манипуляции в динамике видео.

### *Примеры успешного применения:*

- В DFDC трансформеры показали точность до 98% в детекции дипфейков, превосходя CNN при анализе сложных видеопоследовательностей. Модель выявляла рассинхронизацию между движением губ и речью, что часто встречается в дипфейках.
- Применение Vision Transformer в сочетании с моделями для анализа движений позволило обнаруживать несоответствия в микродвижениях лица, что существенно повышает точность распознавания.

### *Комбинированный подход: CNN + Трансформеры*

Совмещение CNN и трансформеров становится одним из наиболее перспективных направлений в детекции дипфейков. Этот подход позволяет использовать преимущества обеих технологий:

1. CNN анализируют локальные особенности изображения — текстуры, артефакты и детали. [10]
2. Трансформеры отслеживают временные изменения и анализируют последовательности кадров, что позволяет выявить динамические ошибки.

### *Преимущества комбинированного подхода:*

- Более высокая точность в сложных сценариях, когда отдельные кадры выглядят естественно, но временная последовательность содержит ошибки.

- Улучшенная устойчивость к новым методам создания дипфейков, где ошибки минимизированы на уровне отдельных изображений, но сохраняются на уровне динамики видео.

Примером эффективного применения этого подхода является XceptionNet с трансформерами. В данной архитектуре CNN обрабатывают изображение для выявления текстурных аномалий, а трансформеры анализируют синхронизацию движений и речи, что значительно повышает точность распознавания даже в сложных случаях.

## Результат

Таким образом, архитектура системы выявления дипфейков представляет собой многоуровневую структуру, направленную на анализ и выявление поддельного контента с использованием различных методов и технологий. Вся система состоит из следующих ключевых этапов:

### 1. *Определение вредоносности контента*

- Система анализирует контекст, в котором используется видео, включая метаданные и социальные факторы, чтобы оценить намерение его создания. Это позволяет различать безобидные дипфейки и зловердные, созданные для дезинформации или мошенничества.

### 2. *Предобработка данных*

- Входные медиафайлы очищаются от визуального шума и нормализуются по разрешению, контрасту и освещению. Этот этап улучшает качество данных и снижает влияние внешних факторов на процесс детекции.

### 3. *Выявление аномалий*

- *Синхронизация речи и движений губ*: проверяется согласованность между движением губ и речью, так как в дипфейках часто присутствует рассинхронизация.
- *Освещение и тени*: анализируется логика расположения теней и источников света. Нелогичное распределение теней указывает на подделку.
- *Микродвижения и моргание*: Отсутствие естественных микродвижений или неправильный ритм моргания — важные признаки подделки.
- *Текстурные ошибки*: используются алгоритмы для выявления дефектов кожи и поверхностей, таких как сглаженные участки или повторяющиеся узоры.
- *Анализ динамики движений*: Оцениваются движения головы и тела на предмет их естественности и биомеханической закономерности.

### 4. *Использование нейросетей*

- *Сверточные нейронные сети (CNN)*: обрабатывают изображения на уровне пикселей, выявляя локальные аномалии в текстурах и контурах лица.
- *Трансформеры*: анализируют временные зависимости и последовательности кадров, отслеживая несоответствия в движениях и синхронизации.
- *Комбинированный подход*: Сочетание CNN для локального анализа и трансформеров для временного анализа позволяет достичь высокой точности даже при минимальных визуальных ошибках.

### 5. *Вывод и интерпретация результатов*

- На основе выявленных признаков система выдает заключение о вероятности подделки.

Современные алгоритмы позволяют классифицировать контент с высокой степенью точности, что делает их эффективными инструментами в борьбе с дезинформацией и мошенничеством.

Ниже данная система представлена в виде блок-схемы:

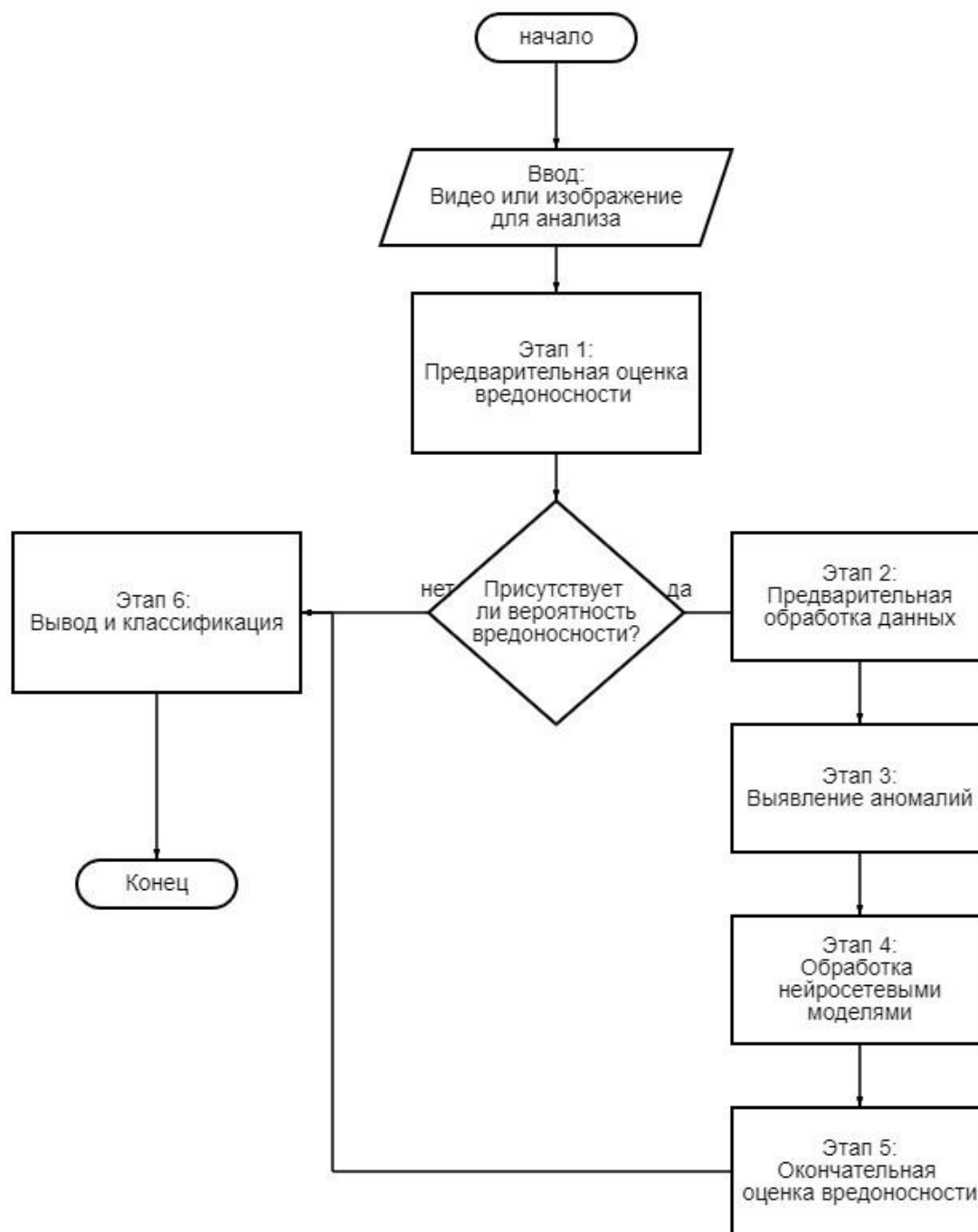


Рисунок 1 - Блок-схема архитектуры системы выявления дипфейков

### Список литературы

1. "Обзор методов выявления дипфейков" Юй Пэйпэн, 2021.
2. "Методы автоматического распознавания дипфейков" Дмитрий Веснин, 2024. (Работа проведена в Лаборатории проблем компьютерной безопасности СПб ФИЦ РАН).

3. "Программа для выявления поддельного видеоконтента" Александр Джуров, 2023. (Разработка специалистов Донского государственного технического университета).
4. Штеренберг С. И. Методика построения защищенных систем искусственного интеллекта для проведения электроретинографии в офтальмологии //Офтальмохирургия. – 2022. – №. 4s. – С. 51-57.
5. Бударный Г. С. и др. Исследование концепции ядра в различных операционных системах //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2022). – 2022. – С. 411-417.
6. Синельщиков В. С., Цветков А. Ю. Защита персональных данных на предприятии //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2021). – 2021. – С. 653-657.
7. Алехин Р.В., Красов А.В., Макарова А.Д., Орлов Г. А. Облачные сервисы. принцип работы, классификация и модели обслуживания // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2022). XI Международная научно-техническая и научно-методическая конференция. Санкт-Петербург, 2022. С. 70–74.
8. Красов А. В., Сахаров Д. В., Тасюк А. А. Проектирование системы обнаружения вторжений для информационной сети с использованием больших данных //Наукоемкие технологии в космических исследованиях Земли. – 2020. – Т. 12. – №. 1. – С. 70-76.
9. "Обзор алгоритмов глубокого обучения для анализа изображений". В. А. Лобанов, Е. С. Ильина, 2021.
10. "Мошенничество с использованием дипфейков: современные вызовы". М. Ю. Кравченко, 2020.
11. "Обнаружение дипфейков с использованием свёрточных трансформеров и нейронных сетей" - Ахмед Хатем Соуди и др., 2023.

## References

1. "Review of methods for detecting deepfakes" by Yu Peipeng, 2021.
2. "Methods for automatic recognition of deepfakes" by Dmitry Vesnin, 2024. (The work was carried out at the Laboratory of Computer Security Problems of St. Petersburg FIT RAS).
3. "A program for detecting fake video content" Alexander Dzhurov, 2023. (Developed by specialists of the Don State Technical University).
4. Shterenberg S. I. Methodology for building secure artificial intelligence systems for electroretinography in ophthalmology //Ophthalmosurgery. – 2022. – No. 4s. – pp. 51-57.
5. Budarny G. S. and others. Exploring the concept of the kernel in various operating systems //Actual problems of infotelec communications in science and education (APINO 2022). – 2022. – pp. 411-417.
6. Sinelshchikov V. S., Tsvetkov A. Yu. Protection of personal data at the enterprise //Actual problems of infotelec communications in science and education (APINO 2021). – 2021. – pp. 653-657.
7. Alyokhin R.V., Krasov A.V., Makarova A.D., Orlov G. A. Cloud services. operating principle, classification and service models // Actual problems of infotelec communications in science and education (APINO 2022). XI International Scientific, Technical, Scientific and Methodological Conference. Saint Petersburg, 2022. pp. 70-74.

8. Krasov A.V., Sakharov D. V., Tasyuk A. A. Designing an intrusion detection system for an information network using big data //High-tech technologies in space exploration of the Earth. 2020. – Vol. 12. – No. 1. – pp. 70-76.
  9. "Review of deep learning algorithms for image analysis." V. A. Lobanov, E. S. Ilyina, 2021.
  10. "Fraud using deepfakes: modern challenges." M. Y. Kravchenko, 2020.
  11. "Deepfake detection using convolutional transformers and neural networks" - Ahmed Hatem Soudi et al., 2023.
-



Международный журнал информационных технологий и энергоэффективности

Сайт журнала:

<http://www.openaccessscience.ru/index.php/ijcse/>



УДК 004.8:004.891.2

## АДАПТИВНАЯ ГЕНЕРАЦИЯ ПОЛЬЗОВАТЕЛЬСКОГО ИНТЕРФЕЙСА С ПОМОЩЬЮ ОБУЧЕНИЯ С ПОДКРЕПЛЕНИЕМ

<sup>1</sup>Кравцова Е.Ю., <sup>2</sup>Болбаков Р.Г.

ФГБОУ ВО «МИРЭА - РОССИЙСКИЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ», Москва, Россия (119454, г. Москва, пр-т Вернадского, д. 78, стр. 4), e-mail: <sup>1</sup>9067320378@mail.ru, <sup>2</sup>bolbakov@mirea.ru

В данном исследовании представлена технология создания адаптивного пользовательского интерфейса, демонстрирующая роль взаимодействия человека и компьютера в оптимизации пользовательского опыта. Сосредоточившись на улучшении взаимодействия между пользователями и интеллектуальными системами, этот подход направлен на автоматическую корректировку макетов и конфигураций интерфейса на основе обратной связи с пользователем, что упрощает процесс проектирования. Традиционное проектирование интерфейсов требует значительных ручных усилий и не позволяет удовлетворить развивающиеся индивидуальные потребности пользователей. Предлагаемая система объединяет адаптивную генерацию интерфейса с обучением с подкреплением Reinforcement Learning (RL) и интеллектуальными механизмами обратной связи для динамической настройки пользовательского интерфейса, что позволяет лучше учитывать индивидуальные особенности использования. В эксперименте для проверки адаптивности предложенного метода в качестве оценочных показателей использовались частота кликов и коэффициент удержания пользователей. Полученные результаты подчеркивают способность системы предоставлять гибкие и персонализированные интерфейсные решения, обеспечивая новый и эффективный подход к проектированию взаимодействия с пользователем и, в конечном счете, улучшая взаимодействие человека и компьютера за счет непрерывного обучения и адаптации.

Ключевые слова: Адаптивный пользовательский интерфейс, обучение с подкреплением, персонализация интерфейса, взаимодействие человека и компьютера (HCI), интеллектуальные агенты, функция вознаграждения, динамическая настройка интерфейса, коэффициент кликов (CTR), коэффициент удержания (RR), генеративные состязательные сети, сравнительный анализ моделей.

## ADAPTIVE USER INTERFACE GENERATION USING REINFORCEMENT LEARNING

Kravtsova E.Y., Bolbakov R.G.

MIREA - RUSSIAN TECHNOLOGICAL UNIVERSITY, Moscow, Russia (119454, Moscow, avenue Vernadsky, 78, b. 4), e-mail: <sup>1</sup>9067320378@mail.ru, <sup>2</sup>bolbakov@mirea.ru

This study presents an adaptive user interface design technique that demonstrates the role of human-computer interaction in optimizing user experience. Focusing on improving the interaction between users and intelligent systems, this approach aims to automatically adjust interface layouts and configurations based on user feedback to simplify the design process. Traditional interface design requires significant manual effort and fails to meet evolving individual user needs. The proposed system combines adaptive interface generation with Reinforcement Learning (RL) and intelligent feedback mechanisms to dynamically customize the user interface to better accommodate individual usage patterns. In the experiment, click rate and user retention rate were used as evaluation metrics to test the adaptability of the proposed method. The results highlight the system's ability to provide flexible and personalized interface solutions, providing a novel and effective approach to user interaction design and ultimately improving human-computer interaction through continuous learning and adaptation.

Keywords: Adaptive user interface, reinforcement learning, interface personalization, human-computer interaction (HCI), intelligent agents, reward function, dynamic interface customization, click-through rate (CTR), retention rate (RR), generative adversarial networks (GANs), comparative model analysis.

## **Введение**

В последние годы, с быстрым развитием технологий искусственного интеллекта, спрос на интеллектуальный дизайн пользовательского интерфейса (UI) постепенно растет [1]. Пользовательский интерфейс напрямую влияет на восприятие пользователя, а эффективный и интуитивно понятный дизайн интерфейса может значительно повысить эффективность и удовлетворенность пользователей. Однако традиционный дизайн интерфейса требует от профессиональных дизайнеров много времени и сил на ручную разработку и оптимизацию, что затрудняет удовлетворение индивидуальных потребностей пользователей. Исходя из этого, технология адаптивной генерации пользовательского интерфейса в сочетании с технологией обучения с подкреплением Reinforcement Learning (RL) постепенно привлекает широкое внимание [2]. Внедряя обучение с подкреплением, система может автоматически корректировать макет интерфейса под обратную связь пользователей в реальном времени, постепенно удовлетворять предпочтения пользователей и предоставлять новый автоматизированный и адаптивный метод для проектирования интерфейса [3].

Основное преимущество обучения с подкреплением заключается в том, что оно постоянно оптимизирует стратегии за счет взаимодействия с окружающей средой, что обеспечивает высокую степень гибкости при создании пользовательских интерфейсов. Генерация интерфейса на основе обучения с подкреплением может получать обратную связь о поведении пользователя с помощью интеллектуальных агентов и динамически настраиваться, чтобы адаптироваться к индивидуальным потребностям пользователей. Например, алгоритмы RL могут непрерывно изучать модели поведения пользователя и его привычки использования интерфейса, а также оптимизировать расположение, размер кнопок и другие конфигурации элементов интерфейса в режиме реального времени в соответствии с обратной связью с пользователем. По сравнению с традиционным способом проектирования интерфейсов, эта технология адаптивной генерации позволяет быстро реагировать на потребности пользователей и обеспечивать высоко персонализированный опыт работы.

## **Материалы и методы**

Метод данного исследования основан на основной идее обучения с подкреплением (RL) и реализует адаптивную генерацию пользовательских интерфейсов путем создания интеллектуальных агентов [4]. Обучение с подкреплением определяется как парадигма машинного обучения, в которой агент (обучаемая модель) взаимодействует с окружающей средой с целью выработки оптимальной стратегии поведения. Основная цель модели обучения с подкреплением – выработать оптимальную стратегию, чтобы интеллектуальный агент мог постоянно оптимизировать расположение интерфейса и конфигурацию элементов на основе обратной связи с пользователем, тем самым максимизируя пользовательский опыт.

Сначала состояние системы генерации интерфейса устанавливается в  $s$ , то есть состояние текущего макета интерфейса; действие  $a$  определяется как операцию настройки, выполняемую системой над интерфейсом, например изменение размера, расположения или цвета кнопок; функция вознаграждения  $r$  используется для измерения удовлетворенности пользователя текущим интерфейсом. Целью обучения с подкреплением является выработка



стратегии, обеспечивающей максимальную сумму вознаграждений  $R$ , которое формируется следующим образом:

$$R = \sum_{t=0}^T \gamma^t r_t$$

Кроме того, данное исследование гарантирует, что созданный интерфейс соответствует предпочтениям пользователя, путем разработки разумной функции вознаграждения. Функция вознаграждения задается как  $r = f(u)$ , где  $u$  представляет собой обратную связь с пользователем, такую как частота нажатий, время пребывания и другие конкретные данные о взаимодействии. Чем больше значение функции вознаграждения, тем ближе сгенерированный эффект текущего интерфейса к идеальному состоянию пользователя.

## Результаты

Чтобы всесторонне оценить технологию адаптивной генерации пользовательских интерфейсов на основе обучения с подкреплением, в данном исследовании было выбрано пять репрезентативных моделей сравнения. К ним относятся метод оптимизации интерфейса на основе алгоритма Multi-Armed Bandit (MAB), который постепенно оптимизирует пользовательский опыт, исследуя различные макеты интерфейса; модель байесовской оптимизации (Bayesian Optimization model), которая выбирает оптимальную конфигурацию параметров интерфейса с помощью распределения вероятностей; генерация интерфейса на основе марковского процесса принятия решений (MDP – Markov decision process), который используется для моделирования непрерывного принятия решений пользователями в интерфейсе; алгоритм Policy Gradient, который используется для генерации интерфейса на основе глубокого обучения; и Collaborative Filtering, который генерирует персонализированные интерфейсы на основе сходства предпочтений между пользователями. Эти модели охватывают различные идеи генерации - от классических методов до моделей глубокого обучения с подкреплением, обеспечивая многостороннее сравнение для оценки технологии адаптивной генерации [5].

Что касается показателей оценки, то в данной работе в качестве основных показателей оценки выбраны коэффициент кликов (CTR) и коэффициент удержания пользователей (RR). Коэффициент кликов используется для измерения привлекательности созданных элементов интерфейса для пользователей и отражает, насколько дизайн интерфейса соответствует потребностям пользователей.

Таблица 1 – Результаты показателей оценки алгоритмов

Модель	CTR	RR
MAB	0.65	0.72
Bayesian Optimization	0.68	0.74
MDP	0.70	0.76
Policy Gradient	0.72	0.78
Collaborative Filtering	0.69	0.75
Ours	0.78	0.83

Модель на основе обучения с подкреплением (Ours) достигает CTR 0,78 и RR 0,83, значительно превосходя другие модели в задачах адаптивной генерации пользовательского интерфейса, как показано в Таблице 1.

Способность обучения с подкреплением (RL) оптимизировать дизайн интерфейса за счет итеративного обучения, корректировок в реальном времени и механизмов вознаграждения делает его очень эффективным для создания дизайна, ориентированного на пользователя. Оно динамически согласовывает характеристики интерфейса с предпочтениями пользователей, превосходя ограничения других моделей.

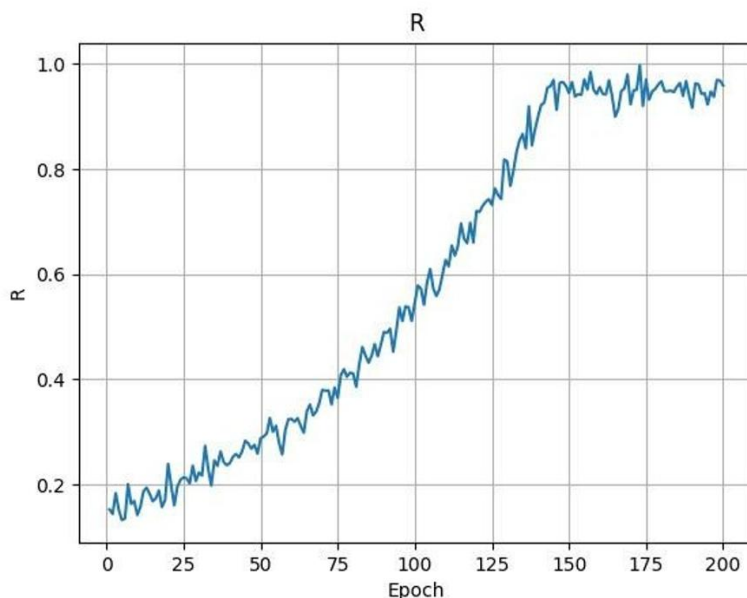


Рисунок 1 - Тенденция роста функции активации

На Рисунке 1 показан восходящий тренд функции активации в процессе обучения, демонстрирующий, что по мере обучения модель обучения с подкреплением сходится к более высокому уровню политики. В начале обучения модель демонстрирует значительные колебания, но с увеличением числа итераций значения вознаграждения стабилизируются, что отражает совершенствование стратегии модели по созданию пользовательских интерфейсов. Эта тенденция указывает на способность модели динамически оптимизировать расположение и конфигурацию интерфейса с помощью итеративных циклов обратной связи "состояние - действие".

Технология создания адаптивного пользовательского интерфейса, описанная в данном исследовании, демонстрирует значительные преимущества в улучшении взаимодействия человека и компьютера. Ориентируясь на поведение пользователей и модели взаимодействия, этот подход направлен на постоянное обучение и адаптацию к привычкам пользователей, что позволяет динамически настраивать макеты и конфигурации интерфейса. Предложенная система продемонстрировала превосходные показатели по количеству кликов и удержанию пользователей по сравнению с традиционными методами, такими как Multi-Armed Bandit и Bayesian Optimization, что выявляет ее сильные стороны в обеспечении персонализированного и увлекательного пользовательского опыта.

### Заключение

Исследование демонстрирует способность систем генерации интерфейсов к адаптации и масштабированию в процессе проектирования взаимодействия с пользователем. Система не только эффективно фиксирует модели поведения пользователей, но и обеспечивает поддержку

принятия решений на основе данных для повышения качества и персонализации интерфейсов. Кроме того, интеграция моделей глубокого обучения, таких как генеративные состязательные сети, может еще больше повысить персонализацию и качество дизайна интерфейсов. Будущее адаптивных пользовательских интерфейсов (UI) заключается в их более широком применении в различных сценариях, что позволит обеспечить более персонализированное взаимодействие человека и компьютера в режиме реального времени. Для решения ключевых задач будущие исследования будут направлены на разработку облегченных моделей и интеграция пограничных вычислений для снижения требований к ресурсам, а также улучшение задержки системы для обеспечения оперативности реагирования в реальном времени. Усилия будут направлены на адаптацию пользовательских интерфейсов для более широкого спектра устройств и сред, укрепление доверия пользователей за счет прозрачности данных и усиления контроля конфиденциальности.

### Список литературы

1. Глебов, Д. Д. Применение искусственного интеллекта в исследованиях пользовательского опыта / Д. Д. Глебов. — Текст: непосредственный // Молодой ученый. — 2024. — № 21 (520). — С. 65-68. — URL: <https://moluch.ru/archive/520/114563/> (дата обращения: 04.03.2025).
2. Жуков А. Д. Генеративный искусственный интеллект в образовательном процессе: вызовы и перспективы // Вестник МГУКИ. 2023. №5 (115). URL: <https://cyberleninka.ru/article/n/generativnyy-iskusstvennyy-intellekt-v-obrazovatelnom-protseesse-vyzovy-i-perspektivy> (дата обращения: 10.03.2025).
3. Т. М. Зубкова, Л. Ф. Тагирова, В. К. Тагиров Автоматизация проектирования адаптивных пользовательских интерфейсов с элементами искусственного интеллекта // Программные продукты и системы. 2020. №1. URL: <https://cyberleninka.ru/article/n/avtomatizatsiya-proektirovaniya-adaptivnyh-polzovatel'skih-interfeysov-s-elementami-iskusstvennogo-intellekta> (дата обращения: 12.03.2025).
4. Кравченко Ю. А. Интеграция свойств когнитивных стилей и интеллектуальных агентов как основа создания адаптивных информационных обучающих систем // Открытое образование. 2010. №4. URL: <https://cyberleninka.ru/article/n/integratsiya-svoystv-kognitivnyh-stiley-i-intellektualnyh-agentov-kak-osnova-sozdaniya-adaptivnyh-informatsionnyh-obuchayuschih> (дата обращения: 15.03.2025).
5. Пальмов С. В., Артюшкина Е. С. Глубокое обучение: определение и отличительные особенности // Форум молодых ученых. 2020. №3 (43). URL: <https://cyberleninka.ru/article/n/glubokoe-obuchenie-opredelenie-i-otlichitelnye-osobennosti> (дата обращения: 20.03.2025).

### References

1. Glebov, D. D. Application of artificial intelligence in user experience research / D. D. Glebov. — Text: direct // Young scientist. — 2024. — № 21 (520). — Pp. 65-68. — URL: <https://moluch.ru/archive/520/114563/> (date of access: 03/04/2025).
2. Zhukov A.D. Generative artificial intelligence in the educational process: challenges and prospects // Bulletin of MGUKI. 2023. No. 5 (115). URL:

- <https://cyberleninka.ru/article/n/generativnyy-iskusstvennyy-intellekt-v-obrazovatelnom-protseesse-vyzovy-i-perspektivy> (date of request: 03/10/2025).
3. T.M.Zubkova, L.F.Tagirova, V.K.Tagirov Automation of design of adaptive user interfaces with elements of artificial intelligence // Software products and systems. 2020. No. 1. URL: <https://cyberleninka.ru/article/n/avtomatizatsiya-proektirovaniya-adaptivnyh-polzovatelskih-interfeysov-s-elementami-iskusstvennogo-intellekta> (date of request: 03/12/2025).
  4. Kravchenko Yu. A. Integration of the properties of cognitive styles and intellectual agents as the basis for creating adaptive information learning systems // Open Education. 2010. No.4. URL: <https://cyberleninka.ru/article/n/integratsiya-svoystv-kognitivnyh-stiley-i-intellektualnyh-agentov-kak-osnova-sozdaniya-adaptivnyh-informatsionnyh-obuchayuschiy> (date of request: 03/15/2025).
  5. Palmov S. V., Artyushkina E. S. Deep learning: definition and distinctive features // Forum of Young Scientists. 2020. No. 3 (43). URL: <https://cyberleninka.ru/article/n/glubokoe-obuchenie-opredelenie-i-otlichitelnye-osobennosti> (date of request: 03/20/2025).
-



Международный журнал информационных технологий и энергоэффективности

Сайт журнала:

<http://www.openaccessscience.ru/index.php/ijcse/>



УДК 004.9

## АНАЛИЗ САНКЦИОННЫХ ДАННЫХ ДЛЯ КЛАССИФИКАЦИИ ПО СТРАНАМ

<sup>1</sup>Часов П.С., Маштаков Н.С.

ФГБОУ ВО «МИРЭА - РОССИЙСКИЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ», Москва, Россия (119454, г. Москва, пр-т Вернадского, д. 78, стр. 4), e-mail: <sup>1</sup>pasha\_chasov@mail.ru

В условиях растущего объема международных санкционных данных возникает необходимость в их систематическом анализе. В данной работе рассматривается подход к классификации санкционных объектов по странам с использованием методов машинного обучения. Предлагается структура анализа, включающая предобработку данных, выбор и обучение моделей, а также визуализацию результатов. Особое внимание уделено разделению объектов на категории и построению специализированных моделей для повышения точности классификации.

Ключевые слова: Санкции, анализ данных, классификация по странам, машинное обучение, санкционные списки, предобработка данных, логистическая регрессия, случайный лес, визуализация данных, геополитика.

## ANALYSIS OF SANCTIONS DATA FOR CLASSIFICATION BY COUNTRY

<sup>1</sup>Chasov P.S., Mashtakov N.S.

MIREA - RUSSIAN TECHNOLOGICAL UNIVERSITY, Moscow, Russia (119454, Moscow, avenue Vernadsky, 78, b. 4), e-mail: <sup>1</sup>pasha\_chasov@mail.ru

In the context of the growing volume of international sanctions data, there is a need for their systematic analysis. This paper considers an approach to classifying sanctioned objects by country using machine learning methods. An analysis structure is proposed that includes data preprocessing, model selection and training, and visualization of results. Special attention is paid to the division of objects into categories and the construction of specialized models to improve classification accuracy.

Keywords: Sanctions, data analysis, country classification, machine learning, sanctions lists, data preprocessing, logistic regression, random forest, data visualization, geopolitics.

Санкции — один из ключевых инструментов международной политики, направленный на ограничение деятельности отдельных физических и юридических лиц. С увеличением количества санкционных объектов возрастает потребность в автоматизированной классификации данных, особенно по географическому признаку. Это необходимо для оперативной аналитики и оценки направленности санкционной политики различных государств.

Целью настоящего исследования является разработка моделей, способных автоматически определять страну, к которой относится объект санкций, на основе открытых данных. В работе используются современные методы машинного обучения и визуализации, обеспечивающие высокую точность и наглядность результатов.

Структура данной статьи включают следующие ключевые аспекты:

1. Подготовка данных к анализу, включая очистку данных и устранение пропусков.
2. Классификация объектов по странам и других связанных данных. Исследование

различных методов и алгоритмов классификации для выбора, подходящего под имеющиеся данные.

3. Наглядное представление результатов анализа для выявления закономерностей. Применение географической визуализации.

4. Рассмотрение возможности применения машинного обучения.

5. Обеспечение достоверности и точности анализа. Проведение анализа пропущенных значений и выбросов. Использование метрик (точность, полнота, F1-мера и прочие) для оценки качества классификации.

6. Создание единого решения для анализа данных. Использование библиотек для обработки данных, создание отчетов.

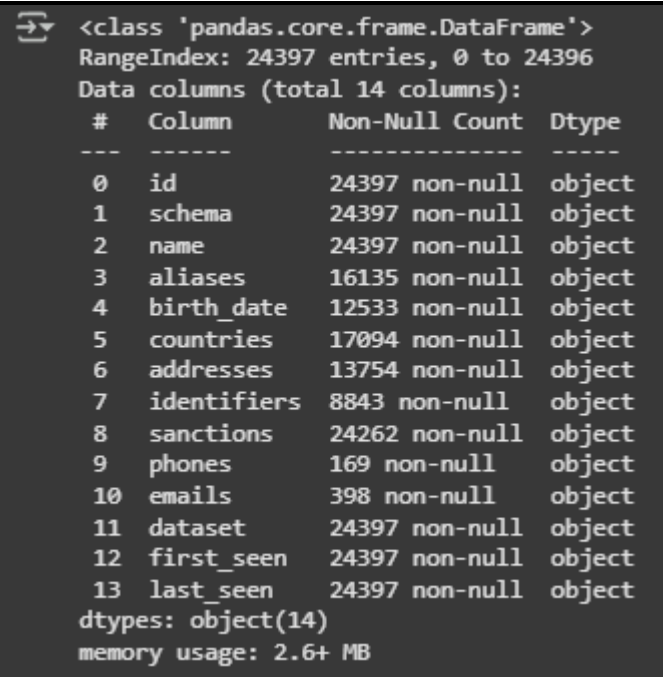
Данные взяты из открытого источника OpenSanctions и представляют собой набор структурированных записей о физических лицах, компаниях, организациях, судах и других объектах. Каждая запись включает в себя идентификаторы, адреса, страны, даты внесения в санкционные списки и дополнительные признаки [1].

Структура данных представлена в Таблице 1.

Таблица 1 — Структура данных

Колонка	Описание
id	уникальный идентификатор объекта
schema	тип объекта (например, физическое лицо, компания, организация)
name	отображаемое имя объекта
aliases	псевдонимы (например, другие написания, прозвища)
birth_date	дата рождения (для физических лиц)
countries	страны проживания, гражданства или юрисдикции компании
addresses	список известных адресов объекта
identifiers	идентификаторы (например, регистрационные номера компаний, паспорта, ИНН)
sanctions	детали о наложенных санкциях (если есть)
phones	список телефонных номеров в формате E.164
emails	список email-адресов, связанных с объектом
dataset	название набора данных, к которому относится объект
address	адрес
last seen	последний раз, когда объект был замечен в исходных данных
first seen	первая дата, когда объект был замечен в OpenSanctions

Краткая информация о данных представлена на Рисунке 1.



```
<class 'pandas.core.frame.DataFrame'>
RangeIndex: 24397 entries, 0 to 24396
Data columns (total 14 columns):
#   Column          Non-Null Count  Dtype
---  -
0   id               24397 non-null  object
1   schema           24397 non-null  object
2   name             24397 non-null  object
3   aliases          16135 non-null  object
4   birth_date       12533 non-null  object
5   countries        17094 non-null  object
6   addresses        13754 non-null  object
7   identifiers       8843 non-null   object
8   sanctions        24262 non-null  object
9   phones           169 non-null    object
10  emails           398 non-null    object
11  dataset          24397 non-null  object
12  first_seen       24397 non-null  object
13  last_seen        24397 non-null  object
dtypes: object(14)
memory usage: 2.6+ MB
```

Рисунок 1 — Краткая информация о данных

Первоначальный анализ показал, что данные содержат пропуски, большая часть которых приходится на персональные данные (даты рождения, идентификаторы, номера телефонов и e-mail почты). Данные представлены только качественными признаками, поэтому статистические данные выводить нет смысла.

Проанализировав информацию в разрезе типов объекта санкций были сделаны следующие выводы:

1. Дата рождения указана только у физических лиц.
2. У самолетов практически не указаны прозвища, страны и адреса, а у морских судов малое количество прозвищ и адресов (количество стран чуть меньше максимального количества строк).
3. У компаний, юридических лиц, организаций низкое количество прозвищ, стран и идентификаторов.

Эффективным было бы решение модернизации и добавления данных, например:

1. Найти прозвища вручную и добавить их в датасет.
2. Дату рождения преобразовать в дату рождения/создания, чтоб была информация не только по физическим лицам.
3. Определить страны по названию объекта при поиске в интернете.
4. Задать собственные идентификаторы.

Но данный подход требует слишком больших временных затрат и не гарантирует наличие данных: например, не всех физических лиц можно свободно найти в общем доступе. Поэтому было принято решение сделать следующим образом:

1. Разделенные датасеты объединим по смыслу: самолеты и суда; организации, компании и юридических лиц.
2. Избавиться от пропусков в зависимости от признаков.
3. Подобрать лучшие типы моделей и обучить их независимо на трех датасетах: транспортные средства, юридические субъекты и физические лица.

4. Подобрать лучший тип модели и обучить ее на исходных данных удалив столбцы с нулевыми значениями.

5. Сравнить модели между собой и выбрать лучшую.

Такой подход позволил повысить полноту данных в каждой из категорий и обеспечить возможность обучения специализированных моделей.

Классификация — это процесс сортировки данных по категориям. В рамках данной практики планируется группировать объекты по странам, что поможет увидеть общую картину санкционной политики. Такой подход упрощает анализ, выявляет тенденции и делает данные более наглядными.

Существует два основных подхода к решению этой задачи. Первый — ручная классификация. Она применяется, когда данных немного и важна максимальная точность. Эксперт вручную проверяет информацию и определяет, к какой стране относится тот или иной объект. Преимущество в том, что человек может учитывать контекст и неочевидные связи. Однако процесс занимает много времени, а результаты могут зависеть от субъективного мнения.

Второй подход — автоматическая классификация с использованием алгоритмов машинного обучения. Этот метод незаменим при работе с большими объемами данных. Сначала информация очищается и приводится к единому формату. Затем выбирается подходящий алгоритм — например, логистическая регрессия, метод опорных векторов или более сложные модели, такие как случайный лес и нейронные сети.

Выбор между ручной и автоматической классификацией зависит от нескольких факторов. Если данных немного и критически важна точность, лучше работать вручную. Для масштабных массивов информации, где скорость обработки играет ключевую роль, эффективнее использовать машинное обучение. При наличии в данных пробелов или неоднозначности, хорошо подходят алгоритмы, устойчивые к шумам, — например, ансамбли моделей.

Как итог, ручная классификация дает высокую точность, но требует значительных временных затрат. Автоматические методы ускоряют процесс, однако их эффективность зависит от качества данных и правильной настройки алгоритмов. В конечном счете результаты классификации служат основой для дальнейшего анализа, помогая лучше понимать структуру и динамику санкционных мер.

В рамках классификации данных существует множество подходов и методов, которые активно применяются в различных областях. Одним из наиболее распространенных решений является использование алгоритмов машинного обучения, таких как метод опорных векторов, случайные леса и градиентный бустинг. Эти методы хорошо зарекомендовали себя благодаря своей способности эффективно разделять данные на классы даже в условиях высокой размерности признаков. Однако их эффективность во многом зависит от качества предобработки данных и выбора гиперпараметров, что требует определенного уровня экспертизы [2].

Другой популярный подход — применение нейронных сетей, особенно глубокого обучения. Сверточные нейронные сети и рекуррентные нейронные сети часто используются для задач классификации изображений, текстов и временных рядов. Эти методы способны автоматически извлекать сложные паттерны из данных, что делает их мощным инструментом.



Однако их использование сопряжено с высокими вычислительными затратами и необходимостью большого объема размеченных данных для обучения.

Также стоит отметить методы, основанные на кластеризации, такие как k-средних или иерархическая кластеризация. Хотя они изначально предназначены для задач кластеризации, их можно адаптировать для классификации, например, путем присвоения меток кластерам. Эти методы особенно полезны, когда данные не имеют явной разметки, но их эффективность может снижаться при наличии шума или сложной структуры данных.

Также, существуют гибридные подходы, которые комбинируют несколько методов для достижения более высокой точности. Например, можно использовать кластеризацию для предварительной обработки данных, а затем применять алгоритмы машинного обучения для финальной классификации. Такие решения часто оказываются более гибкими и адаптивными, но требуют тщательной настройки и анализа.

Для автоматической классификации объектов по странам применяются различные методы машинного обучения: логистическая регрессия, случайный лес, градиентный бустинг и наивный байесовский классификатор. Каждый из методов обладает своими преимуществами: линейные модели обеспечивают интерпретируемость, ансамблевые — устойчивость к шуму, а байесовские — простоту и скорость работы.

Для начала были объединены датасеты самолетов и судов в датасет транспортных средств. На полученном датасете был замечен недостаток данных в столбцах прозвищ, дат рождения и адресов. Данным столбцы были удалены.

Далее объединили датасеты компаний, юридических лиц и организаций в датасет юридических субъектов. На полученном датасете был замечен недостаток данных в столбцах адресов и идентификаторов. Данным столбцы были удалены, после чего были удалены пропуски данных.

После чего был создан общий датасет из исходных данных, удалив столбцы прозвищ, дат рождения, адресов и идентификаторов, после чего удалены пропуски данных.

Далее был создан датасет на основе данных о физических лицах. На полученном датасете был замечен недостаток данных в столбцах прозвищ, дат рождения и идентификаторов. Данным столбцы были удалены.

В качестве признаков использовались доступные текстовые и категориальные поля, преобразованные в числовой формат с использованием one-hot encoding и других методов.

Были протестированы четыре алгоритма:

- логистическая регрессия — для простых линейных зависимостей [3];
- случайный лес — для устойчивой многоклассовой классификации [4];
- XGBoost — градиентный бустинг, показывающий высокую точность при наличии большого количества признаков [5];
- Multinomial Naive Bayes — для категориальных данных [6].

Оценка проводилась по метрике Ассурасу и с использованием матриц ошибок. Также использовалась кросс-валидация и настройка гиперпараметров для повышения качества. Результаты обучения представлены в Таблице 2.

Таблица 2 — Качество моделей по группам

Тип объектов	Лучшая модель	Accuracy
Транспортные средства	Логистическая регрессия	0.79
Юридические субъекты	Случайный лес	0.80
Физические лица	Случайный лес	0.64
Объединённый датасет	Случайный лес	0.65

Полученные результаты показывают, что использование отдельных моделей для различных типов объектов (транспортные средства, юридические субъекты, физические лица) значительно повышает точность классификации по сравнению с единым универсальным классификатором. Такой подход учитывает специфику признаков, характерную для каждой категории.

Важно отметить, что наибольшее качество достигнуто в группе юридических субъектов, что объясняется лучшей структурированностью данных: компании и организации часто имеют четко привязанные юрисдикции. В случае с физическими лицами, наоборот, разнообразие стран гражданства и частые пропуски делают классификацию более сложной.

Предлагаемый подход может быть масштабирован и на другие задачи — например, прогнозирование наложения санкций или поиск аномалий в распределении. Однако его эффективность ограничивается качеством исходных данных: высокая доля пропусков и необходимость ручного объединения подкатегорий требуют дополнительных временных затрат.

Для более глубокого анализа и представления данных была реализована визуализация географического распределения санкций на Рисунке 2. На карте наглядно показано, что основное количество санкций приходится на Россию, а также ряд других стран, находящихся под экономическим и политическим давлением.

Распределение количества санкций по странам

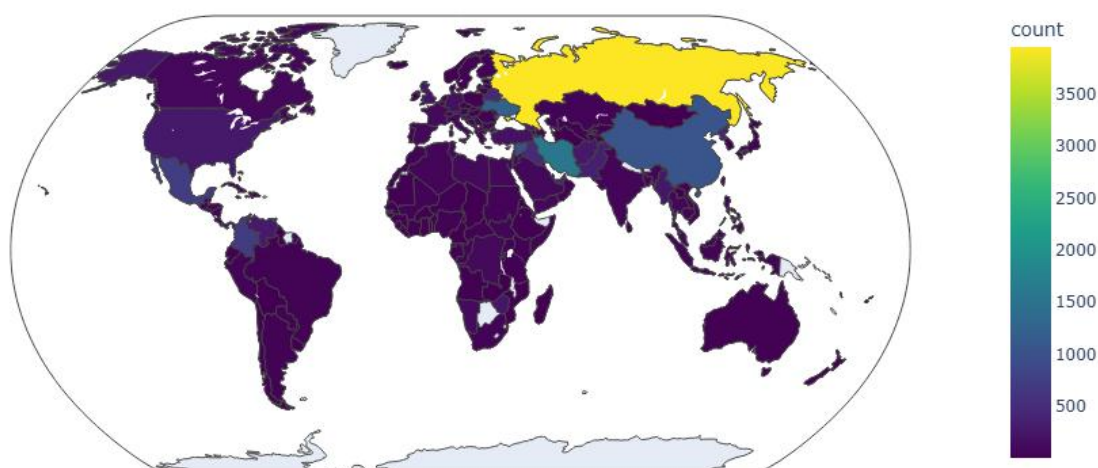


Рисунок 2— Географическое распределение данных

В ходе работы была реализована система классификации объектов санкций по странам. Основные этапы включали:

- предварительную очистку и структурирование данных;
- разделение по типам объектов;
- обучение и оценку моделей машинного обучения;
- визуализацию результатов.

Ключевой вывод — важность разделения объектов по типам перед обучением модели. Объединение гетерогенных данных приводит к снижению точности. Разработка специализированных моделей и минимизация пропусков позволяют значительно улучшить результаты. Использование визуализации помогает в интерпретации санкционной политики стран.

Ограничением является отсутствие многих персональных данных в открытых источниках. Расширение источников и дополнение данных (например, через внешние API) может улучшить модели.

Разработан и протестирован набор моделей, классифицирующих санкционные объекты по странам. Наиболее эффективной оказалась стратегия раздельного обучения по категориям объектов. Полученные результаты демонстрируют высокую применимость методов машинного обучения для анализа санкционных данных.

## Список литературы

1. Набор данных “Sanction list by countries” [Электронный ресурс] / Ravineesh // Kaggle. – Режим доступа: <https://www.kaggle.com/datasets/ravineesh/sanction-list-by-countries> (Дата обращения: 12.05.2025)
2. Документация “Scikit-learn: Machine Learning in Python” [Электронный ресурс] // Scikit-learn. – Режим доступа: <https://scikit-learn.org/stable> (Дата обращения: 12.05.2025)
3. Документация “Scikit-learn: LinearRegression” [Электронный ресурс] // Scikit-learn. – Режим доступа: [https://scikit-learn.org/stable/modules/generated/sklearn.linear\\_model.LinearRegression.html](https://scikit-learn.org/stable/modules/generated/sklearn.linear_model.LinearRegression.html) (Дата обращения: 16.05.2025)
4. Документация “Scikit-learn: RandomForestClassifier” [Электронный ресурс] // Scikit-learn. – Режим доступа: <https://scikit-learn.org/stable/modules/generated/sklearn.ensemble.RandomForestClassifier.html> (Дата обращения: 16.05.2025)
5. Документация “xgboost” [Электронный ресурс] // Scikit-learn. – Режим доступа <https://xgboost.ai/> (Дата обращения: 16.05.2025)
6. Документация “Scikit-learn: MultinomialNB” [Электронный ресурс] // Scikit-learn. – Режим доступа: [https://scikit-learn.org/stable/modules/generated/sklearn.naive\\_bayes.MultinomialNB.html](https://scikit-learn.org/stable/modules/generated/sklearn.naive_bayes.MultinomialNB.html) (Дата обращения: 16.05.2025)

## References

1. Dataset “Sanction list by countries” [Electronic resource] / Ravineesh // Kaggle. – Access mode: <https://www.kaggle.com/datasets/ravineesh/sanction-list-by-countries> (Дата обращения: 12.05.2025)
2. Documentation “Scikit-learn: Machine Learning in Python” [Electronic resource] // Scikit-learn. – Access mode: <https://scikit-learn.org/stable> (Дата обращения: 12.05.2025)
3. Documentation “Scikit-learn: LinearRegression” [Electronic resource] // Scikit-learn. – Access

- mode: [https://scikit-learn.org/stable/modules/generated/sklearn.linear\\_model.LinearRegression.html](https://scikit-learn.org/stable/modules/generated/sklearn.linear_model.LinearRegression.html) (Дата обращения: 16.05.2025)
4. Documentation of “Scikit-learn: RandomForestClassifier” [Electronic resource] // Scikit-learn. – Access mode: <https://scikit-learn.org/stable/modules/generated/sklearn.ensemble.RandomForestClassifier.html> (Дата обращения: 16.05.2025)
5. Documentation of “pypi: XGBoost” [Electronic resource] // Scikit-learn. – Access mode <https://pypi.org/project/xgboost/> / (Дата обращения: 16.05.2025)
6. Documentation “Scikit-learn: MultinomialNB” [Electronic resource] // Scikit-learn. – Access mode: [https://scikit-learn.org/stable/modules/generated/sklearn.naive\\_bayes.MultinomialNB.html](https://scikit-learn.org/stable/modules/generated/sklearn.naive_bayes.MultinomialNB.html) (Дата обращения: 16.05.2025)
-



Международный журнал информационных технологий и  
энергоэффективности

Сайт журнала:

<http://www.openaccessscience.ru/index.php/ijcse/>



УДК 004.8

## ИДЕНТИФИКАЦИЯ ПРОБЛЕМНЫХ ОБЛАСТЕЙ В ИСПОЛЬЗОВАНИИ ЭЛЕМЕНТОВ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ДЛЯ УПРАВЛЕНИЯ СЛОЖНОСТРУКТУРИРОВАННЫМИ ОРГАНИЗАЦИОННЫМИ СИСТЕМАМИ

<sup>1</sup>Николенко А.А., Юшков Е.С.

ФГАОУ ВО "НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ЯДЕРНЫЙ УНИВЕРСИТЕТ "МИФИ", Москва, Россия (115409, город Москва, Каширское ш., д.31), e-mail: <sup>1</sup>[alexander.nikolenko.lawyer@gmail.com](mailto:alexander.nikolenko.lawyer@gmail.com)

Статья исследует переход от традиционных вертикальных моделей управления к горизонтальным структурам в условиях цифровой трансформации, выделяя ключевые вызовы интеграции искусственного интеллекта (ИИ). В качестве решения предлагается внедрение комплексного фреймворка AI TRiSM для соблюдения баланса между автоматизацией, развитием человеческого капитала и адаптацией организационных процессов.

Ключевые слова: Искусственный интеллект в управлении, цифровая трансформация, организационные модели управления, риски ИИ, фреймворк AI TRiSM

## IDENTIFICATION OF PROBLEM AREAS IN THE USE OF ARTIFICIAL INTELLIGENCE ELEMENTS FOR MANAGING COMPLEX STRUCTURED ORGANIZATIONAL SYSTEMS

<sup>1</sup>Nikolenko A.A., Yushkov E.S.

"NATIONAL RESEARCH NUCLEAR UNIVERSITY "MEPHI", Moscow, Russia (115409, Moscow, Kashirskoye sh., 31), e-mail: <sup>1</sup>[alexander.nikolenko.lawyer@gmail.com](mailto:alexander.nikolenko.lawyer@gmail.com)

The article examines the shift from traditional vertical management models to horizontal structures in the context of digital transformation, highlighting key challenges of integrating artificial intelligence (AI). As a solution, it proposes implementing the comprehensive AI TRiSM framework to balance automation, human capital development, and adaptation of organizational processes.

Keywords: Artificial intelligence in management, digital transformation, organizational management models, ai risks, AI TRiSM framework.

### Эволюция управления сложноструктурированными организационными системами (в рамках цифровой трансформации)

Тип управления, который долгое время давал лучшие результаты, был так называемый «Тейлоризм» или вертикальная модель управления Тейлора, названный в честь американского инженера Фредерика Уинслоу Тейлора, создавшего научную организацию труда, разработанную, в частности, в рамках группы Форд в XIX веке.

С управленческой точки зрения такая организация работы основывается на следующих принципах:

1. Иерархичность: роли лиц, принимающих решения, и исполнителей четко разделены

и не взаимозаменяемы;

2. Цели и выделяемые средства устанавливаются лицами, принимающими решения;
3. У исполнителей мало места для маневра, и их оценивают на основе достижения поставленных целей;
4. Чем крупнее организация, тем больше в ней иерархических уровней;
5. Каждый знает свою миссию, определенную его «должностной инструкцией», и не намерен от нее отклоняться.

Модель Тейлора демонстрировала сильные стороны четкого определения курса организации, оптимизацию роли каждого человека, возможность легко измерять эффективность выполняемых действий и мотивацию сотрудников посредством достижения целей. Слабыми сторонами являлась жесткость организации, а также потенциальная потеря мотивации сотрудниками в их повседневной работе, особенно для тех, кто выполняет повторяющиеся задачи. В настоящее время компании, следующие путем цифровой трансформации все чаще видят угрозу в «Тейлоризме», из-за неспособности такого типа управления быстро адаптироваться к изменениям в потребностях бизнеса и сотрудников.

Современные модели организации труда задают новую логику производства и новые перспективы для инноваций. Яркими примерами являются организации с горизонтальными моделями управления. Менеджмент оказывается в центре текущих и будущих изменений, является движущей силой этих новых моделей. Цифровая трансформация существенно меняет управленческую практику по крайней мере по трем фундаментальным аспектам:

1. Повышение прозрачности и изменение коммуникаций. Цифровые технологии, например, социальные сети, способствуют усилению прозрачности не только снаружи, но и внутри организации. Изменение средств коммуникаций влечет за собой более открытое общение, сокращение иерархических барьеров и возможность коллективного обмена информацией. Развитие совместных цифровых платформ приводит к тому, что традиционные вертикальные структуры постепенно заменяются более плоскими и гибкими моделями взаимодействия.

2. Эволюция отношения к работе и границам между личным и профессиональным. Интеграция личной и профессиональной жизни, использование цифровых инструментов стирает границы между трудовым временем и личным пространством, создавая «мост» между ними<sup>1</sup>.

3. Мотивация сотрудников. Современный работник ищет не просто стабильность или комфорт, а смысловую нагрузку и возможность самовыражения через интенсивный профессиональный опыт<sup>2</sup>. В отличие от прошлого, где мотивацией были традиционные достижения и коллективное чувство выполненной миссии, сегодня сотруднику важно участие в динамичном, «интенсивном» процессе, где он может постоянно испытывать себя и развиваться.

Несмотря на перемены, теории и практики менеджмента многие компании так и не отошли полностью от первоначальной вертикальной модели управления. Во многих

---

<sup>1</sup> Социальная платформа СИБУР // Social.Sibur. URL: <https://social.sibur.ru/stream> (дата обращения: 12.02.2025).

<sup>2</sup> Жизненный цикл проекта в СИБУРе: от идеи к реализации — Личный опыт // VC.ru. URL: <https://vc.ru/life/673885-zhiznennyyi-cikl-proekta-v-sibure-ot-idei-k-realizacii?ysclid=m6ove8qqcz47579966> (дата обращения: 12.02.2025).

организациях административный вес по-прежнему влияет на инновации, на свободу творчества, поскольку он по-прежнему митигирует чрезмерный риск, а заодно и уверенность сотрудников в своей способности быть реальными участниками перемен.

Действительно, у «менеджера завтрашнего дня» будет более широкая миссия: гармонизация человеческих отношений и интеграция управления с интеллектуальными информационными системами. Поэтому ему, несомненно, придется освоить новые инструменты, понять тенденции цифрового бизнеса, автоматизации и роботизации деятельности. Только освоив эти новые процессы, можно будет организовать консолидацию всех рабочих сил организации. «Менеджер завтрашнего дня» знает, как создать сеть, внутреннюю или внешнюю, ставит своих сотрудников в наилучшее положение, чтобы иметь возможность обнаружить будущие таланты благодаря своей чувствительности и открытости. «Менеджер завтрашнего дня» становится ближе к своим командам и знает, как отойти в сторону на пользу своим коллегам, чтобы позволить им продемонстрировать инновации и креативность.

На диаграмме ниже представлены новые навыки, ожидаемые от менеджеров в контексте цифровых технологий и искусства.

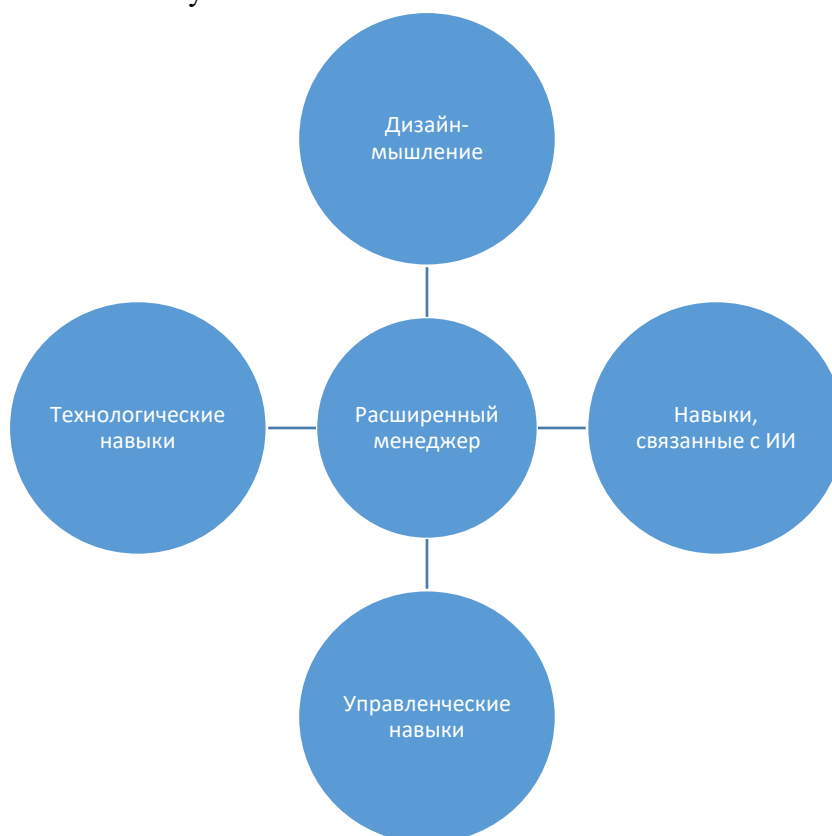


Рисунок 1 - Расширенный менеджер<sup>3</sup>

В дополнение к гибкости дизайн-мышление позволит менеджерам развивать как способность демонстрировать как креативность, так и способность разрабатывать быстрые и функциональные проекты. В эпоху цифровых технологий этот навык является

---

<sup>3</sup> Источник Селин Дежу в книге «Метаморфозы менеджеров в эпоху цифровых технологий и искусственного интеллекта».

управленческим активом.

Управленческие навыки, строго говоря, связанные с ИИ, делятся, с одной стороны, на навыки, связанные с технологическим инструментом, а с другой — на команды. Технологические навыки — это те, которые позволяют нам понимать данные, что мы можем с ними делать, какую добавленную стоимость может принести ИИ, как контролировать ИИ и сделать его дополнением к действиям человека. Навыки, связанные с командами, — это те, которые позволяют переосмыслить работу с ИИ, повысить культуру команд, поддержать интеграцию ИИ и, наконец, развить коллективный и совместный интеллект.

### **Влияние цифровых технологий и искусственного интеллекта на организации**

Одним из фундаментальных элементов появления ИИ в организациях является то, что он связан с принятием решений или деятельностью организации. Требуется объединение команд и новые формы совместного взаимодействия, что в свою очередь меняет методы управления.

Один из способов, адаптации к изменениям, является переосмысление отношений с заинтересованными сторонами: клиентами, пользователями, сотрудниками. Особенность Менеджмент 3.0 в отношении ее сотрудников состоит в том, что они создают то, что, можно рассматривать как «выученный опыт».<sup>4</sup> Менеджмент 3.0 — это концепция управления, в которой компании адаптируются к новым реалиям цифровой трансформации, гибкости и самоорганизации.

Сотрудник, который становится соавтором в горизонтальных и сбалансированных управленческих отношениях, больше не является тем, кто «просто будет выполнять задачи, порученные его руководителем», а становится «силой предложения», чье мнение и идеи могут иметь значение. Создание доверия внутри команд напрямую связано с последствиями цифровой трансформации. Сотрудник становится клиентом компании и может влиять на ее решения. Этот новый режим работы оказывает существенное влияние на вовлеченность и мотивацию сотрудников.

Цифровая трансформация также поддерживает структурные изменения в рабочих отношениях в организациях, предлагая технические возможности для их облегчения. Эти изменения касаются обмена информацией, аддитивных технологий и т. д. Компании переходят от логики инструментов, предназначенных для тех, кто им управляет, к логике инструментов для тех, кто им пользуется. Эта переконфигурация процессов ставит необходимость пересмотра методов управления.

Нынешнее и будущее появление ИИ поднимает три вопроса, связанных с социальными проблемами и влияющими на организацию бизнеса: Будет ли положительное влияние ИИ? Тогда изменит ли это человека? Наконец, смогут ли роботы заменить людей?

Замена человека роботами относится как к теории Й. Шумпетера<sup>5</sup>, так и к более пессимистической теории глубоких изменений. ИИ будет уничтожать рабочие места, но и создавать их аналогичным образом, в той степени, в которой организации демонстрируют

---

<sup>4</sup> Цитата Джейкоба Моргана в статье из публикации Huffington «Почему будущее работы зависит от опыта сотрудников», 6 декабря 2017 г.

<sup>5</sup> Теория созидательного разрушения Йозефа Шумпетера (1883-1950), австрийского экономиста и профессора науки: «Любое промышленное или экономическое развитие создает столько же рабочих мест, сколько и уничтожает».



инновации и предвкушение. Системам управления придется интегрировать новые профессии, развивать новые актуальные навыки. На этом уровне появляется понятие расширенного менеджера, определенное Сесиль Дежу<sup>6</sup>. На карту поставлена их конкурентоспособность или выживание.

Перспектива значительного повышения производительности труда, которую предлагает ИИ, некоторые эксперты оценивают до 40% <sup>7</sup>. Кроме того, стремление к большему удовлетворению пользователей, связанное с необходимой цифровизации продуктов, говорят в пользу интеграции информационных систем.

Ключевым вызовом становится баланс между автоматизацией и человеческим контролем. ИИ способен выступать в роли исполнительного оператора, конкурируя с сотрудниками в эффективности анализа данных. Однако его внедрение требует трансформации управленческих подходов, начиная с уровня высшего руководства. Целью является переход от интуитивных решений к системам, основанным на аналитике, что влечет реформу методов управления и перераспределение ответственности. Для успеха критически важны инвестиции в развитие компетенций сотрудников, а также создание реестра актуальных навыков, соответствующих новым технологическим реалиям.

Серьёзным ограничением остаётся проблема «чёрного ящика» в ИИ-моделях. Невозможность интерпретации решений нейросетей создаёт риски некорректных выводов, снижения доверия и проблем с регуляторным соответствием. Для минимизации этих рисков требуются методы объяснимого ИИ (SHAP, LIME), а также пересмотр подходов к управлению данными — прозрачности, коллективному обучению и обеспечению качества входных данных.

Трансформация организационной парадигмы предполагает переход от традиционного проектного управления с жёстким планированием к гибким схемам, основанным на итеративном экспериментировании. Управление должно сместиться от контроля к делегированию, фокусируясь на стратегическом видении и развитии коллективного интеллекта. Это требует перестройки коммуникационных цепочек и передачи оперативных решений командам, непосредственно взаимодействующим с бизнес-процессами.

Таким образом, успешная интеграция ИИ в организации зависит от трёх факторов: пересмотра управленческих практик в сторону горизонтальной коллаборации, инвестиций в развитие человеческого капитала и создания инфраструктуры для работы с данными. Эти изменения, требующие времени и культурной трансформации, становятся необходимым условием для сохранения конкурентоспособности в условиях цифровой эпохи.

СИБУР и Амурский газохимический комплекс (АГХК) уже используют элементы ИИ в своей деятельности. Современные технологии ИИ проникают во все сферы промышленности. Компании активно внедряют нейросетевые решения, системы анализа данных и комплексные ИИ-решения для поддержки управленческих и операционных процессов в СИБУРе.

АГХК внедрил систему управления инженерными данными на базе платформы AVEVA, которая аккумулирует инженерно-техническую информацию и 3D-модели в едином

---

<sup>6</sup> Профессор университета CNAM, автор совместно с Эммануэль Леон книги «Метаморфозы менеджеров в эпоху цифровых технологий и искусственного интеллекта», 2018, Pearson editions.

<sup>7</sup> Отчет об искусственном интеллекте, реальные последствия, государственные услуги в эпоху искусственного интеллекта, Accenture, 2018.

хранилище. Это позволяет сотрудникам оперативно находить актуальные данные и реагировать на изменения в режиме реального времени.<sup>8</sup> СИБУР активно внедряет ИИ в различные бизнес-процессы. Так, совместно с Сбербанком и группой компаний ЦРТ была разработана нейросетевая модель GigaChat, которая используется в нескольких направлениях:

- AI-ассистент инженера-диагноста: помогает анализировать неисправности оборудования на основе текстовых описаний и выдаёт гипотезы для устранения аномалий.
- AI-советчик по оптимизации закупок: система анализирует технические характеристики комплектующих, подбирает аналоги с лучшими показателями по цене, качеству и доступности, что особенно актуально в условиях импортозамещения.
- AI-помощник в R&D: применяется для моделирования полимеров и создания материалов с новыми свойствами, сокращая количество лабораторных экспериментов за счёт цифрового моделирования.
- AI-ассистент финансиста: агрегирует корпоративные данные, помогает прогнозировать динамику ключевых показателей и принимать обоснованные управленческие решения<sup>9</sup>.

По данным различных материалов, цифровая трансформация СИБУРа, в том числе внедрение ИИ-решений, позволила достичь значительного экономического эффекта – общий эффект за шесть лет превысил 45 млрд рублей, а само применение ИИ принесло порядка 15 млрд рублей экономии и прироста эффективности.<sup>10</sup> Комплексный подход к внедрению ИИ, реализуемый в СИБУРе и АГХК, демонстрирует широкий спектр возможностей – от автоматизации рутинных операций до стратегической поддержки принятия решений. Нейросетевые ассистенты, оптимизация закупок, цифровые платформы для управления данными и моделями – все эти направления способствуют повышению эффективности производства, снижению операционных издержек и обеспечению безопасности. Примеры, представленные в материалах, подтверждают, что интеграция ИИ становится ключевым фактором конкурентоспособности российских промышленных компаний.

### **Угрозы появления искусственного интеллекта и решение проблем, связанных с ИИ в управлении**

Введение современных технологий искусственного интеллекта в управленческие процессы сопровождается рядом существенных вызовов и угроз, требующих комплексного решения. Как отмечается в отчете France Strategie об искусственном интеллекте<sup>11</sup>, ИИ

---

<sup>8</sup> Амурский ГХК выбрал программное обеспечение AVEVA для развития направления Information Management <https://ru-bezh.ru/press-releases/42825-amurskij-gxk-vyibral-programmnoe-obespechenie-aveva-dlya-razviti?ysclid=m60tu7zi1168545940> 9дата обращения: 12.02.2025)

<sup>9</sup> СИБУР внедряет в свои процессы нейросетевую модель GigaChat <https://www.sibur.ru/ru/press-center/news-and-press/cibur-vnedryaet-v-svoi-protsessy-neyrosetevuyu-model-gigachat/> (дата обращения: 12.02.2025)

<sup>10</sup> "Сибур" делает ставку на ИИ в достижении экономических эффектов Об этом сообщает "Рамблер". [https://news.rambler.ru/tech/52421993/?utm\\_content=news\\_media&utm\\_medium=read\\_more&utm\\_source=copylink](https://news.rambler.ru/tech/52421993/?utm_content=news_media&utm_medium=read_more&utm_source=copylink) (дата обращения: 12.02.2025)

<sup>11</sup> Искусственный интеллект и работа, доклад France Strategie, представленный министру труда и государственному секретарю премьер-министра, отвечающему за цифровые вопросы, в марте 2018 года.

представляет собой двойственную технологию: с одной стороны, он открывает новые возможности для повышения производительности и оптимизации трудовых процессов, с другой - создает серьезные социальные и экономические риски.

Одной из ключевых проблем является растущий разрыв между существующими профессиональными навыками и новыми требованиями цифровой экономики. Этот разрыв особенно остро проявляется при интеграции ИИ-решений в традиционные бизнес-процессы. Параллельно наблюдается формирование "разрыва в ИИ" - неравенства между компаниями, способными внедрять передовые технологии, и организациями, не обладающими необходимыми ресурсами. Для преодоления этого дисбаланса требуется активное участие государства в создании инфраструктуры развития искусственного интеллекта.

Особую озабоченность вызывает вопрос доверия к ИИ-системам. Проблемы алгоритмической предвзятости, ярким примером которой стал случай с дискриминационным алгоритмом подбора персонала Amazon<sup>12</sup>, ставят под сомнение объективность решений, принимаемых искусственным интеллектом. Не менее серьезную угрозу представляет нарушение конфиденциальности данных, поскольку ИИ-системы требуют обработки значительных массивов персональной информации.

Однако успешная интеграция ИИ требует решения ряда фундаментальных вопросов. Необходимо развивать нормативно-правовую базу, обеспечивающую этическое использование технологий, инвестировать в образовательные программы для подготовки специалистов нового типа, а также создавать механизмы защиты данных. Особое внимание следует уделить разработке международных стандартов в области ИИ, что позволит минимизировать риски, связанные с безопасностью и злонамеренным использованием технологий. Несмотря на значительный потенциал искусственного интеллекта в области управления, его внедрение должно сопровождаться комплексом мер, направленных на минимизацию социальных и экономических рисков.

Таблица 1 - Баланс между доверием, риском и безопасностью ИИ в зависимости от типов угроз

Аспект	Типы векторов угроз	Виды повреждений
Доверительное управление ИИ	<p><b>Предвзятость и дискриминация</b>  Распространение вводящей в заблуждение информации и предвзятых нарративов с целью формирования негативного восприятия возможностей и намерений ИИ.</p> <p><b>Вторжение в частную жизнь</b>  Атаки с использованием манипулированных обучающих данных для обмана систем ИИ.</p>	<p>Подрыв общественного доверия, препятствование внедрению ИИ и препятствование общественному прогрессу путем поощрения страха, скептицизма и нежелания использовать системы ИИ.</p> <p>Подрыв доверия пользователей, компрометация конфиденциальных данных и возможность принятия дискриминационных или вредоносных решений.</p>

<sup>12</sup> Amazon отказались от алгоритма рекрутинга с ИИ из-за предвзятости против женщин  
[https://dzen.ru/a/ZGtFO\\_phnDQE\\_NjZ](https://dzen.ru/a/ZGtFO_phnDQE_NjZ) (дата обращения: 12.02.2025)

<p><b>Управление безопасностью с помощью ИИ</b></p>	<p><b>Злонамеренное использование ИИ</b> Кража данных или несанкционированный доступ с использованием уязвимостей в системах искусственного интеллекта. <b>Недостаточные меры безопасности</b> Неправильное обращение со слабой аутентификацией, шифрованием или контролем доступа в системах ИИ.</p>	<p>Утечка конфиденциальных данных, нарушение целостности системы, потенциальное отравление модели ИИ, что приводит к нарушениям безопасности и потере доверия к технологиям на основе ИИ. Несанкционированный доступ к конфиденциальной информации и потенциальное неправомерное использование систем ИИ, приводящие к нарушению конфиденциальности и потере доверия к технологиям ИИ.</p>
---	---	--

Анализ взаимосвязи между типами угроз и потенциальным ущербом демонстрирует необходимость комплексного подхода к обеспечению безопасности ИИ-систем. Особую актуальность эта проблема приобретает в контексте цифровой трансформации крупных промышленных предприятий [1].

Широкое признание и эффективная интеграция ИИ в различные сферы жизни во многом зависят от установления доверия к нему. Учитывая его многообразие и многогранность, при оценке этого доверия необходимо учитывать множество факторов, которые в настоящее время отсутствуют в существующих статических моделях. Ключевой урок, извлеченный из этих критически важных секторов, заключается в важности участия человека в процессах ИИ, например, когда ИИ передает решение о классификации человеку, когда он не уверен в конкретном случае. С другой стороны, методы ИИ для управления рисками все чаще распространяются на новые области, включая проверку обширных хранилищ документов, автоматизацию повторяющихся задач и выявление отмывания денег, что требует анализа значительных наборов данных. Поскольку системы искусственного интеллекта постоянно развиваются, системам управления рисками становится все труднее идти в ногу с новейшими разработками и потенциальными рисками.

Для решения этих проблем предлагается использовать комплексный фреймворк AI TRiSM (Trust, Risk and Security Management), который обеспечивает структурированный подход к управлению рисками ИИ. Данная концепция, получившая признание в отчете Gartner<sup>13</sup>, включает пять ключевых принципов: прозрачность, подотчетность, справедливость, надежность и конфиденциальность. Реализация этого подхода позволяет организациям минимизировать риски при внедрении ИИ-решений.

AI TRiSM — это комплексная структура, предназначенная для решения проблем, связанных с системами искусственного интеллекта, обеспечивающая справедливость, управление, эффективность, надежность и конфиденциальность. Структура AI TRiSM предназначена для помощи организациям, разрабатывающим систематический подход к управлению рисками, связанными с ИИ, включая конфиденциальность данных, риски,

<sup>13</sup> Gartner: 80% предприятий внедрят искусственный интеллект к 2026 году  
<https://www.itweek.ru/ai/article/detail.php?ID=227682> (дата обращения: 12.02.2025)

связанные с безопасностью и этическими проблемами. Идея AI TRiSM — относительно недавняя концепция, которая привлекла к себе внимание, поскольку люди все больше зависят от систем на базе искусственного интеллекта для решения сложных задач в современном обществе. Приняв структуру AI TRiSM, организации могут получить более глубокое понимание процессов, связанных с проектированием, разработкой и внедрением моделей искусственного интеллекта. Ожидается, что AI TRiSM обеспечит эффективный мониторинг и снижение рисков, обеспечивая при этом надежность и достоверность систем искусственного интеллекта [2].

Компоненты текущей структуры AI TRiSM следующие:

- *Мониторинг модели*

Одной из серьезных проблем, с которыми сегодня сталкиваются модели ИИ, является отсутствие доверия среди пользователей, в первую очередь связанное с проблемами, связанными с прозрачностью и этикой. Реализуя мониторинг и объяснимость моделей, мы гарантируем, что модели ИИ функционируют правильно и не добавляют предвзятости. Это способствует пониманию того, как работают модели ИИ, позволяет прийти к обоснованным выводам, а также способствует прозрачности и укреплению доверия к системе ИИ.

- *AI ModelOps*

Несмотря на потенциал, продемонстрированный ИИ в различных областях применения, его интеграция на предприятиях все еще находится на начальной стадии. Одним из возможных объяснений этого является отсутствие подходящих инструментов и методологий для облегчения полного жизненного цикла разработки решений ИИ, что включает в себя такие важные задачи, как подготовка данных, проектирование и обучение моделей, разработка приложений, обеспечение качества, развертывание, мониторинг, обратная связь, а также обеспечение воспроизводимости и возможности аудита на протяжении всего процесса[3].

- *Приложение безопасности ИИ*

Приложения безопасности ИИ используют сложные алгоритмы и методологии машинного обучения для быстрого выявления и устранения слабых мест, несанкционированного доступа и вредоносных действий. Эти приложения имеют возможность наблюдать за сетевыми закономерностями, оценивать действия пользователей и выявлять нарушения, которые могут сигнализировать о нарушении безопасности. Использование технологии искусственного интеллекта требует огромного количества данных, и обеспечение защиты этих данных имеет первостепенное значение. В контексте AI TRiSM безопасность данных имеет особое значение в жестко регулируемых секторах, таких как здравоохранение и финансы. Кроме того, применяются структуры защиты данных, такие как синтетические данные, дифференциальная конфиденциальность, а также такие протоколы, как полное гомоморфное шифрование (FHE) и Secure Multi Party Computation (SMPC).

- *Конфиденциальность модели*

Конфиденциальность данных предполагает подтверждение того, что системы ИИ собирают, хранят и обрабатывают личные и конфиденциальные данные, соблюдая при этом правила конфиденциальности и устоявшиеся передовые методы. Это влечет за собой получение надлежащего согласия, внедрение методов анонимизации данных и использование методов безопасной обработки данных для защиты прав людей на неприкосновенность частной жизни. Гарантии конфиденциальности необходимы для данных, используемых при

обучении или тестировании моделей ИИ[4].

В Таблице 2 показано сравнение ключевых параметров доверия, риска и безопасности в системах ИИ, проблемы и потенциальные улучшения до и после внедрения AI TRiSM Framework. В таблице основное внимание уделяется таким ключевым аспектам, как мониторинг модели, AI modelOps, приложение безопасности AI и конфиденциальность модели.

Таблица 2 - ИИ и потенциальные улучшения до и после внедрения AI TRiSM Framework

Аспект	До и после AI TRiSM Framework: проблемы и потенциальные улучшения	
<b>Мониторинг</b>	<p>Ограниченная прозрачность. Неопределенное поведение модели.</p> <p>Отсутствие ответственности за поведение системы ИИ.</p> <p>Потенциальные предвзятости и дискриминационные результаты.</p> <p>Ограниченные меры безопасности для мониторинга моделей.</p>	<p>Улучшенная объяснимость за счет самоанализа модели. Проверка ожидаемого поведения.</p> <p>Четкие структуры управления для повышения подотчетности, алгоритмы обеспечения справедливости и методы обнаружения/смягчения предвзятости.</p> <p>Расширенные протоколы безопасности и меры для мониторинга моделей.</p>
<b>AI ModelOps ИИ-безопасность Приложение Конфиденциальность</b>	<p>Ограниченное количество подходящих инструментов и методологий разработки систем искусственного интеллекта.</p> <p>Недостаточное рассмотрение этических последствий.</p> <p>Ограниченная защита от отравления моделей ИИ и состязательных атак.</p> <p>Физический вред, несчастные случаи или непредвиденные последствия.</p> <p>Ограниченная конфиденциальность данных и обработка конфиденциальной информации отдельных лиц моделируется ИИ.</p> <p>Повышенный риск неправомерного использования персональных данных, несанкционированного доступа и нарушения конфиденциальности.</p>	<p>Управление жизненным циклом системы искусственного интеллекта, управление всей инфраструктурой и средой модели искусственного интеллекта.</p> <p>Методика проектирования надежных систем искусственного интеллекта.</p> <p>Этические руководящие принципы и нормативная база для решения этических проблем. протоколы безопасности и принять меры, защищающие от несанкционированного доступа или взлома.</p> <p>Надежная конструкция системы, отказоустойчивые механизмы, тщательное тестирование и человеческий контроль. Повышенное доверие за счет четкого информирования о мерах конфиденциальности.</p> <p>Соблюдение правил и снижение потенциальных рисков конфиденциальности, связанных с системами искусственного интеллекта.</p>

Современные системы управления сталкиваются с принципиально новыми вызовами при внедрении технологий искусственного интеллекта. Традиционные подходы к обеспечению доверия, управления рисками и безопасности, основанные на ручном контроле экспертов, становятся недостаточно эффективными в условиях масштабирования ИИ-решений. Автоматизация этих процессов через фреймворк AI TRiSM предлагает новый подход к решению системных проблем.

Эффективное управление рисками ИИ требует сочетания автоматизированных решений и экспертной оценки. AI TRiSM позволяет перераспределить ресурсы, освобождая специалистов для решения стратегических задач, в то время как алгоритмы берут на себя рутинный мониторинг и первичный анализ угроз. Такой подход способствует формированию устойчивой экосистемы доверия к искусственному интеллекту в корпоративном управлении [5].

### **Выводы**

Идентификация проблемных областей в применении искусственного интеллекта (ИИ) в управлении сложноструктурированными организационными системами требует тщательного анализа множества аспектов, включая технические, организационные, этические и регуляторные. Ключевые проблемные области включают следующие:

Во-первых, технические проблемы. Здесь можно выделить несколько аспектов. Качество данных – это одна из основных проблем. Недостаточное количество данных, плохое качество данных или их нерепрезентативность могут существенно повлиять на эффективность ИИ. Кроме того, интеграция систем часто вызывает трудности, так как ИИ-системы могут не интегрироваться должным образом с существующими ИТ-инфраструктурами. Еще одна важная техническая проблема – это надежность и масштабируемость ИИ-систем. Обеспечение надежности работы ИИ-систем и их способность масштабироваться с ростом данных и нагрузки является критически важным.

Во-вторых, организационные проблемы. Они включают в себя сопротивление изменениям со стороны сотрудников, что может быть вызвано страхом перед неизвестностью или потерей рабочих мест. Отсутствие квалифицированного персонала для работы с ИИ также является серьезной проблемой, как и необходимость в постоянном обучении и повышении квалификации сотрудников. Более того, изменение организационной структуры и процессов для интеграции ИИ может быть сложным и требовать значительных усилий [6].

В-третьих, этические проблемы. Внедрение ИИ может привести к вопросам, связанным с конфиденциальностью данных, так как ИИ-системы часто обрабатывают большие объемы личной информации. Кроме того, существует риск дискриминации, поскольку ИИ может унаследовать предвзятость из данных, на которых он был обучен. Прозрачность и подотчетность ИИ-систем также являются важными этическими вопросами.

В-четвертых, регуляторные проблемы. В разных странах и отраслях существуют различные законы и регуляции, которые могут ограничивать применение ИИ. Соответствие этим нормам требует дополнительных ресурсов и усилий, а также может замедлять процесс внедрения ИИ.

Таким образом, успешное применение ИИ в управлении сложноструктурированными организационными системами требует комплексного подхода к идентификации и решению различных проблемных областей.

### Список литературы

1. Об интеграции интеллекта человека и искусственного интеллекта: теория и применение в науке, образовании и бизнесе : монография / М. П. Фархадов, Ю. В. Таратухина, О. В. Блинова [и др.]. – Москва : Русайнс, 2023. – 171 с. – ISBN 978-5-466-04033-3. – URL: <https://book.ru/book/950973>
2. Инвестиционный климат и искусственный интеллект: взаимосвязи и проблемы трансформации мегаполиса : сборник статей / под ред. А. А. Шестемирова, Ю. В. Евдокимовой ; коллектив авторов. – Москва : Русайнс, 2022. – 129 с. – ISBN 978-5-466-01442-6. – URL: <https://book.ru/book/945666>
3. Конев С.И. Искусственный интеллект как фактор, оказывающий влияние на принятие управленческих решений // Новеллы Конституции Российской Федерации и задачи юридической науки : в 5 частях. – Москва : Проспект : РГ-Пресс, 2021. – Ч. 5. – С. 171-182. –URL: [https://megapro.msal.ru/MegaPro/UserEntry?Action=Link\\_FindDoc&id=73441&idb=0](https://megapro.msal.ru/MegaPro/UserEntry?Action=Link_FindDoc&id=73441&idb=0)
4. Попова Е.В. Российский опыт внедрения искусственного интеллекта в менеджмент предприятия // Инновации и инвестиции. – 2023. – №6. – URL: <https://cyberleninka.ru/article/n/rossiyskiy-opyt-vnedreniya-iskusstvennogo-intellekta-v-menedzhment-predpriyatiya>
5. Ai Stewardship. Internal Auditor [Internet]. 2019 Feb [cited 2023 Oct 25];76(1):10. Available from: <https://search.ebscohost.com/login.aspx?direct=true&db=lgs&AN=134559606&lang=ru>
6. Bloch-Wehba H. Algorithmic Governance from the Bottom Up. Brigham Young University Law Review [Internet]. 2022 Nov [cited 2023 Oct 25];48(1):69–136. Available from: <https://search.ebscohost.com/login.aspx?direct=true&db=lgs&AN=160926986&lang=ru>

### References

1. On the integration of human intelligence and artificial intelligence: theory and application in science, education and business : a monograph / M. P. Farkhadov, Yu. V. Taratukhina, O. V. Blinova [et al.]. – Moscow : Rusains, 2023. – 171 p. – ISBN 978-5-466-04033-3. – URL: <https://book.ru/book/950973>
2. Investment climate and artificial intelligence: interrelations and problems of megalopolis transformation : collection of articles / edited by A. A. Shestemirov, Yu.V. Evdokimova ; team of authors. – Moscow : Rusains, 2022. 129 p. – ISBN 978-5-466-01442-6. – URL: <https://book.ru/book/945666>
3. Konev S.I. Artificial intelligence as a factor influencing managerial decision-making // Novelties of the Constitution of the Russian Federation and the tasks of legal science : in 5 parts. – Moscow : Prospekt : RG-Press, 2021. – Part 5. – pp. 171-182. –URL: [https://megapro.msal.ru/MegaPro/UserEntry?Action=Link\\_FindDoc&id=73441&idb=0](https://megapro.msal.ru/MegaPro/UserEntry?Action=Link_FindDoc&id=73441&idb=0)



4. Popova E.V. The Russian experience of introducing artificial intelligence into enterprise management // Innovation and investment. – 2023. – №6. – URL: <https://cyberleninka.ru/article/n/rossiyskiy-opyt-vnedreniya-iskusstvennogo-intellekta-v-menedzhment-predpriyatiya>
  5. Ai Stewardship. Internal Auditor [Internet]. 2019 Feb [cited 2023 Oct 25];76(1):10. Available from: <https://search.ebscohost.com/login.aspx?direct=true&db=lgs&AN=134559606&lang=ru>
  6. Bloch-Wehba H. Algorithmic Governance from the Bottom Up. Brigham Young University Law Review [Internet]. 2022 Nov [cited 2023 Oct 25];48(1):69–136. Available from: <https://search.ebscohost.com/login.aspx?direct=true&db=lgs&AN=160926986&lang=ru>
-



Международный журнал информационных технологий и  
энергоэффективности

Сайт журнала:

<http://www.openaccessscience.ru/index.php/ijcse/>



УДК 004.056

## АТАКИ С ПОМОЩЬЮ "PROMPT INJECTION" В ГОЛОСОВЫХ LLM: ФОРМИРОВАНИЕ ОПАСНЫХ АУДИО-КОМАНД

**Васильев Б.А.**

ФГБОУ ВО САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ  
ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФЕССОРА М. А. БОНЧ-БРУЕВИЧА, Санкт-Петербург,  
Россия (193232, г. Санкт-Петербург, просп. Большевиков, 22, корп. 1), e-mail:  
boris.2003@mail.ru

В условиях стремительного развития голосовых больших языковых моделей (Voice-LLM) повышается внимание к вопросам безопасности их взаимодействия с аудиовходом. В данной статье рассматриваются атаки с помощью внедрения запросов (prompt injection) в аудиоформате, демонстрирующие уязвимости систем, воспринимающих голосовые команды. Определены механизмы формирования опасных аудиосообщений, способных изменить поведение модели, включая обход фильтров, выполнение нежелательных инструкций и компрометацию пользовательских данных. Описаны возможные сценарии атак, обсуждаются направления повышения устойчивости Voice-LLM к вредоносным аудиовоздействиям.

Ключевые слова: Голосовые LLM, аудио-команды, внедрение запросов, атаки на ИИ, безопасность.

## PROMPT INJECTION ATTACKS IN VOICE LLMS: GENERATING DANGEROUS AUDIO COMMANDS

**Vasiliev B.A.**

ST. PETERSBURG STATE UNIVERSITY OF TELECOMMUNICATIONS NAMED AFTER  
PROFESSOR M. A. BONCH-BRUEVICH, St. Petersburg, Russia (193232, St. Petersburg, ave.  
Bolshevikov, 22, bldg. 1), e-mail: boris.2003@mail.ru

As voice-based large language models (Voice-LLMs) rapidly evolve, attention to the security of their audio input processing increases. This paper explores prompt injection attacks delivered via audio, revealing vulnerabilities in systems that respond to spoken instructions. It identifies mechanisms for constructing malicious audio prompts that can alter model behavior, including bypassing filters, executing harmful commands, and compromising user data. The article presents examples of real-world attack scenarios and discusses potential mitigation strategies to enhance the robustness of Voice-LLMs against audio-based prompt injections.

Keywords: Voice LLMs, audio prompts, prompt injection, AI attacks, security.

### Введение

Голосовые технологии активно трансформируют взаимодействие человека с цифровыми системами. В последние годы наблюдается взрывной рост применения голосовых помощников, виртуальных агентов и голосовых интерфейсов в самых разных сферах: от потребительской электроники и умных домов до корпоративных решений, здравоохранения и транспорта. Одним из ключевых факторов этого роста стало внедрение больших языковых моделей (LLM), адаптированных к восприятию и обработке голосового сигнала — так называемых Voice-LLM. Эти модели демонстрируют способность воспринимать,

интерпретировать и выполнять сложные голосовые команды, приближаясь по качеству взаимодействия к человеческому диалогу.

Однако, вместе с широким распространением таких технологий значительно возрастает и потенциальная поверхность атак. Как и в случае с текстовыми LLM, голосовые модели оказываются уязвимыми к специфическим типам атак, связанным с манипуляцией входными данными. Одним из наиболее тревожных направлений является так называемая «prompt injection» — инъекция команд или инструкций, встроенных в пользовательский ввод с целью изменить поведение модели. Если в текстовых системах это явление уже хорошо исследовано, то его аудиоверсия — относительно новая угроза, сочетающая в себе как особенности акустической обработки, так и риски, характерные для машинного восприятия речи.

Особенность аудиоформата заключается в сложности обнаружения скрытых команд. В отличие от текста, аудиосигналы трудно анализировать вручную, а существующие фильтры часто не способны отличить вредоносное содержание от легитимных фраз, особенно если они произнесены в естественной манере. Более того, учитывая повсеместность голосовых систем и их всё большую автономность, вредоносные аудиокоманды могут применяться без ведома пользователя, например, транслироваться через динамики, радиостанции, открытые каналы связи.

Таким образом, перед исследовательским сообществом и разработчиками Voice-LLM встаёт задача не только улучшать функциональность моделей, но и обеспечивать их безопасность в условиях новых угроз. Данная статья направлена на систематизацию подходов к созданию вредоносных аудио-команд, анализ уязвимостей голосовых LLM к prompt injection и обсуждение возможных стратегий защиты. Это направление на стыке искусственного интеллекта, кибербезопасности и обработки речи требует срочного внимания в условиях стремительного роста голосовых ИИ-систем.

### **Атаки с помощью "prompt injection" в голосовых LLM: формирование опасных аудио-команд**

Внедрение запросов (prompt injection) представляет собой манипуляцию входными данными с целью изменения поведения языковой модели. Первоначально этот тип атак был характерен для текстовых систем, однако его аудиоверсия оказалась не менее эффективной в голосовых LLM. Аудиоформат усложняет детектирование атакующих фрагментов, особенно если вредоносные команды замаскированы под естественную речь или сопровождаются фоновыми шумами [1] (с. 572).

Голосовые LLM интерпретируют входные аудиосигналы, преобразуя их в текст для дальнейшей обработки. Если злоумышленник способен внедрить скрытые инструкции на этапе формирования аудиосообщения, система может ошибочно интерпретировать эти команды как легитимные. Примером может служить запись, содержащая фразу, звучащую как часть запроса пользователя, но на деле являющуюся директивой для модели выполнить определённое действие [2] (с. 410).

Формирование опасных аудиокоманд требует использования синтеза речи с высоким уровнем реализма и контекстуального соответствия. Используя современные TTS-системы, возможно создать аудиофайлы, в которых вредоносная часть незаметна для пользователя, но успешно интерпретируется моделью. Такие команды могут быть использованы для получения

несанкционированного доступа к функциям приложения, изменения внутреннего состояния системы или обхода фильтров безопасности [3] (с. 62).

Опасность подобных атак усугубляется тем, что модель может «поверить» команде, даже если её источник не подтверждён. Многие голосовые интерфейсы по умолчанию предполагают, что полученная аудиокоманда поступила от пользователя, что делает возможным применение атак через поддельные или перехваченные аудиопотоки. В сценариях, где используется пассивное прослушивание, модель становится особенно уязвимой [4] (с. 26).

Для противодействия подобным атакам необходимо внедрение многоуровневых систем верификации, включая проверку происхождения аудиосигнала, анализ интонации и семантическую фильтрацию. Также возможно использование метаобучения, позволяющего модели отличать подозрительные шаблоны поведения. Однако такие меры требуют дополнительных вычислительных ресурсов и могут замедлять обработку, что создаёт компромисс между безопасностью и производительностью [5] (с. 48).

### **Заключение**

Изучение атак с использованием prompt injection в голосовых больших языковых моделях выявляет серьёзные пробелы в современной системе аудиобезопасности. В отличие от традиционных уязвимостей, где источник угрозы может быть локализован или заблокирован средствами фильтрации, голосовые атаки обладают высокой степенью незаметности, особенно при использовании высококачественного синтеза речи. Подобные атаки способны инициироваться удалённо, без прямого доступа к устройству, что существенно расширяет возможности злоумышленников.

Рассмотренные механизмы демонстрируют, что даже высокообученные модели легко поддаются манипуляциям, если они не снабжены дополнительными модулями анализа контекста и верификации источника команды. Текущая архитектура многих Voice-LLM ориентирована на удобство и скорость обработки, при этом игнорируя важность многоуровневой проверки достоверности голосового сигнала. Это создаёт парадокс: чем умнее и адаптивнее становится голосовой ИИ, тем выше риск его эксплуатации в злонамеренных целях.

Дальнейшее развитие этой области должно опираться на междисциплинарный подход, объединяющий достижения в области искусственного интеллекта, лингвистики, цифровой акустики и кибербезопасности. Противодействие атакам через аудио prompt injection потребует внедрения новых стандартов аутентификации голосовых данных, анализа просодии, анализа латентных признаков речевых паттернов, а также машинного обучения, способного отличать «естественные» команды от потенциально вредоносных. Кроме того, важно развивать правовые и этические рамки, регулирующие использование голосовых ИИ, включая меры ответственности за распространение аудио-контента с внедрёнными командами.

В условиях стремительно увеличивающегося доверия к голосовым интерфейсам и автоматизированным системам принятия решений, пренебрежение безопасностью может иметь критические последствия. Поэтому понимание, обнаружение и предотвращение атак с использованием аудиоформата prompt injection должно стать неотъемлемой частью жизненного цикла разработки и эксплуатации голосовых LLM. Только так можно обеспечить надёжную и безопасную интеграцию этих систем в повседневную жизнь.

### Список литературы

1. Волкогонов В. Н. и др. Применение физически неклонированных функций для выполнения аутентификации в среде интернета вещей // \*Актуальные проблемы инфотелекоммуникаций в науке и образовании\*. – 2021. – С. 409-414.
2. Калинин М. О., Штеренберг С. И. Анализ информационной безопасности предприятия на основе мониторинга информационных ресурсов с использованием машинного обучения // \*Интеллектуальные технологии на транспорте\*. – 2018. – № 3 (15). – С. 47-54.
3. Кушнир Д. В., Шемякин С. Н., Орлов Г. А. Представление некоторых аспектов отсеивания составных чисел для криптографических приложений // \*Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки\*. – 2020. – № 1. – С. 25-28.
4. Петрова Т. В. и др. Подходы обнаружения беспроводной точки доступа злоумышленника в локальной вычислительной сети // \*Региональная информатика (РИ-2022)\*. – 2022. – С. 572-573.
5. Шемякин С. Н., Ахметшина М. Э., Катасонов А. И. Поиск функций, обладающих наилучшими характеристиками в классе от 4 переменных // \*Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки\*. – 2020. – № 4. – С. 61-65.

### References

1. Volkogonov V. N. et al. The use of physically non-cloned functions to perform authentication in the Internet of Things environment // \*Actual problems of infotelec communications in science and education\*. 2021. pp. 409-414.
  2. Kalinin M. O., Shterenberg S. I. Analysis of information security of an enterprise based on monitoring of information resources using machine learning // \*Intelligent technologies in transport\*. – 2018. – № 3 (15). – Pp. 47-54.
  3. Kushnir D. V., Shemyakin S. N., Orlov G. A. Presentation of some aspects of screening composite numbers for cryptographic applications // \*Bulletin of the St. Petersburg State University of Technology and Design. Series 1: Natural and Technical Sciences\*. – 2020. – № 1. – pp. 25-28.
  4. Petrova T. V. and others. Approaches to detecting an attacker's wireless access point in a local computer network // \*Regional Informatics (RI-2022)\*. – 2022. – pp. 572-573.
  5. Shemyakin S. N., Akhmetshina M. E., Katasonov A. I. Search for functions with the best characteristics in a class of 4 variables // \*Bulletin of the St. Petersburg State University of Technology and Design. Series 1: Natural and Technical Sciences\*. – 2020. – № 4. – pp. 61-65.
-



Международный журнал информационных технологий и  
энергоэффективности

Сайт журнала:

<http://www.openaccessscience.ru/index.php/ijcse/>



УДК 004.056: 004.7

## ЭКСПЛУАТАЦИЯ LATENCY В МЕТАВЕРС-СРЕДЕ КАК КАНАЛ УТЕЧКИ ИНФОРМАЦИИ

**Васильев Б.А.**

ФГБОУ ВО САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ  
ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФЕССОРА М. А. БОНЧ-БРУЕВИЧА, Санкт-Петербург,  
Россия (193232, г. Санкт-Петербург, просп. Большевиков, 22, корп. 1), e-mail:  
[boris.2003@mail.ru](mailto:boris.2003@mail.ru)

Современные метаверс-среды становятся не только пространствами для взаимодействия и развлечений, но и потенциальными векторами информационной безопасности. Одним из малоизученных, но перспективных каналов утечки данных является эксплуатация задержек (latency), присущих сетевому взаимодействию в виртуальных мирах. В данной статье рассматриваются теоретические и практические аспекты использования сетевой латентности как скрытого канала передачи информации в метаверсе. Приводится классификация типов задержек и анализ их зависимости от архитектуры и инфраструктуры метаверс-среды. Также предложены модели атак, использующих изменения времени отклика в качестве сигнала, а также возможные подходы к их обнаружению и нейтрализации. Исследование акцентирует внимание на важности разработки новых методов мониторинга и обеспечения безопасности в виртуальных пространствах.

Ключевые слова: Мета-вселенная, латентность, утечка данных, скрытые каналы, информационная безопасность.

## EXPLOITATION OF LATENCY IN THE METAVERSE ENVIRONMENT AS AN INFORMATION LEAKAGE CHANNEL

**Vasiliev B.A.**

ST. PETERSBURG STATE UNIVERSITY OF TELECOMMUNICATIONS NAMED AFTER  
PROFESSOR M. A. BONCH-BRUEVICH, St. Petersburg, Russia (193232, St. Petersburg, ave.  
Bolshevikov, 22, bldg. 1), e-mail: [boris.2003@mail.ru](mailto:boris.2003@mail.ru)

Modern metaverse environments are becoming not only spaces for interaction and entertainment, but also potential vectors of information security. One of the little-studied but promising channels of data leakage is the exploitation of latency inherent in network interaction in virtual worlds. This article discusses the theoretical and practical aspects of using network latency as a hidden channel for transmitting information in the metaverse. The types of delays are classified and their dependence on the architecture and infrastructure of the metaverse environment is analyzed. Attack models using changes in response time as a signal are also proposed, as well as possible approaches to their detection and neutralization. The study focuses on the importance of developing new methods for monitoring and ensuring security in virtual spaces.

Keywords: Meta-universe, latency, data leakage, hidden channels, information security.

### Введение

Развитие технологий виртуальной и дополненной реальности дало начало масштабным проектам в области метаверса — сетевых цифровых миров, способных обеспечить погружение, взаимодействие и создание цифровых экономик. Однако с расширением их функционала возрастает и спектр угроз, связанных с безопасностью пользовательских данных.

Современные угрозы информационной безопасности все чаще используют нестандартные векторы атаки, включая каналы, которые сложно отследить традиционными методами мониторинга. Одним из таких векторов становится латентность — временные задержки в передаче данных, которые изначально рассматривались лишь как технический параметр сетевого соединения. Возможность манипуляции задержками открывает путь к созданию скрытых каналов передачи информации, что представляет собой серьезную угрозу как для персональных данных, так и для корпоративной безопасности в условиях мета-вселенной.

### **Эксплуатация latency в метаверс-среде как канал утечки информации**

Метаверс-среды, функционирующие на базе распределённых вычислений, зависят от сетевой инфраструктуры, облачных вычислений и клиент-серверных архитектур. В таких системах даже незначительные изменения сетевой латентности могут повлиять на поведение аватаров, взаимодействие объектов и визуальную синхронизацию. Эти особенности позволяют использовать латентность в качестве скрытого канала передачи информации между пользователями или между клиентом и злоумышленником.

Принцип действия подобных атак основан на кодировании информации в форму задержек. Например, заранее установленный алгоритм может интерпретировать высокую или низкую задержку как логическую единицу или ноль. Визуально такие изменения не заметны, особенно в условиях высокой нагрузки на сервер, что делает их идеальным инструментом для сокрытия передачи данных [1] (с. 260). Исследования показали, что даже без доступа к исходному коду платформы можно внедрить такие каналы, используя стандартные функции API метаверса.

Основной проблемой обнаружения подобных каналов является их интеграция в естественные процессы работы системы. Задержки могут возникать по объективным причинам: колебания нагрузки, маршрутизация пакетов, обработка пользовательских запросов. Поэтому различить намеренно созданный скрытый канал от случайного поведения сети — нетривиальная задача [2] (с. 347).

Условно можно выделить три уровня латентности в метаверс-среде: задержка на клиенте, задержка на уровне сети и задержка в облачной обработке. Каждый из этих уровней может быть использован для кодирования данных. Например, пользователь может искусственно нагружать локальные ресурсы для увеличения задержки на клиентской стороне, тогда как сетевая латентность может управляться изменением маршрутов передачи данных или симуляцией сбоев [3] (с. 380).

Примером успешного использования такого подхода являются атаки типа timing-based, в которых злоумышленник посылает зашифрованные сигналы через последовательность запросов к объектам метаверса. Ответы с различной скоростью обработки интерпретируются как биты информации. В зависимости от архитектуры платформы эти атаки могут быть как пассивными, так и активными — с вмешательством в среду или без него [4] (с. 240).

Немаловажным фактором является и возможность масштабирования подобных атак. При наличии нескольких точек контроля в метаверс-пространстве можно организовать сложную схему обмена информацией, аналогичную peer-to-peer сети. Это особенно актуально для случаев корпоративного шпионажа или несанкционированной передачи конфиденциальных данных. При этом традиционные средства обнаружения, такие как анализ

сетевого трафика, оказываются неэффективными, так как атака маскируется под типичное поведение пользователя в метаверсе [5] (с. 572).

### **Заключение**

Эксплуатация сетевой латентности как канала утечки информации в метаверс-среде представляет собой сложный вызов для специалистов в области информационной безопасности. Учитывая сложность выявления подобных каналов и их высокую степень маскировки, необходима разработка специализированных инструментов анализа поведения в виртуальных средах. Предложенные модели атак показывают, что даже при высокой степени защищенности на уровне протоколов, метаверс-платформы остаются уязвимыми к нестандартным формам утечки информации. Будущее обеспечение безопасности в цифровых мирах требует пересмотра подходов к мониторингу активности, включая поведенческий анализ и машинное обучение для выявления аномалий. Только сочетание технических и организационных мер может обеспечить устойчивость метаверс-сред к подобным угрозам.

### **Список литературы**

1. Гельфанд А. М. Способы выбора стегоконтейнеров для передачи данных //Региональная информатика и информационная безопасность. – 2020. – С. 260-262.
2. Горбань С. А., Красов А. В., Цветков А. Ю. Оценка эффективности механизмов контроля правами доступа в ОС Linux //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2023). – 2023. – С. 345-348.
3. Кушнир Д. В. Исследование и разработка методов распределения конфиденциальных данных по квантовым каналам : дис. – Санкт-Петербург. гос. ун-т телекоммуникаций им. МА Бонч-Бруевича, 1996. - С. 378-390.
4. Леснова Е. М., Пестов И. Е. Разработка метода обнаружения и коррекции ошибок для распределенной информационной сети на основе больших данных //Региональная информатика и информационная безопасность. – 2018. – С. 236-240.
5. Петрова Т. В. и др. Подходы обнаружения беспроводной точки доступа злоумышленника в локальной вычислительной сети //Региональная информатика (РИ-2022). – 2022. – С. 572-573.

### **References**

1. Gelfand A. M. Ways to choose stegocontainers for data transmission. – 2020. – pp. 260-262.
  2. Gorban S. A., Krasov A. V., Tsvetkov A. Y. Assessment of the effectiveness of access rights control mechanisms in Linux OS // Actual problems of infotelecommunications in science and education (APINO 2023). – 2023. – pp. 345-348.
  3. Kushnir D. V. Research and development of methods for the distribution of confidential data on quantum channels. –Saint Petersburg. State University of Telecommunications named after MA Bonch-Bruevich, 1996. - pp. 378-390.
  4. Lesnova E. M., Pestov I. E. Development of a method for detecting and correcting errors for a distributed information network based on big data. – 2018. – pp. 236-240.
  5. Petrova T. V. et al. Approaches to Detecting an Attacker's Wireless Access Point in a Local Computing Network // Regional Informatics (RI-2022). – 2022. – pp. 572-573.
-





Международный журнал информационных технологий и  
энергоэффективности

Сайт журнала:

<http://www.openaccessscience.ru/index.php/ijcse/>



УДК 004.9

## СЕГМЕНТАЦИЯ КЛИЕНТОВ БАНКА НА ОСНОВЕ ДЕМОГРАФИЧЕСКИХ ХАРАКТЕРИСТИК С ПРИМЕНЕНИЕМ МЕТОДОВ КЛАСТЕРИЗАЦИИ

**Маштаков Н.С., <sup>1</sup>Часов П.С.**

*ФГБОУ ВО «МИРЭА - РОССИЙСКИЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ», Москва, Россия (119454, г. Москва, пр-т Вернадского, д. 78, стр. 4), e-mail: <sup>1</sup>pasha\_chasov@mail.ru*

**В данной работе выполнена кластеризация клиентов банка на основе демографических и финансовых признаков с использованием алгоритмов KMeans, DBSCAN и GMM. Проведено сравнение моделей по качеству сегментации, выполнена визуализация и интерпретация полученных кластеров. Определены основные клиентские группы и предложены направления их практического применения в бизнес-задачах.**

**Ключевые слова:** Кластеризация, KMeans, DBSCAN, Gaussian Mixture Model, сегментация клиентов, банковские данные, машинное обучение, анализ данных, предобработка, визуализация данных.

## SEGMENTATION OF BANK CLIENTS BASED ON DEMOGRAPHIC CHARACTERISTICS USING CLUSTERIZATION METHODS

**Mashtakov N.S., <sup>1</sup>Chasov P.S.**

*MIREA - RUSSIAN TECHNOLOGICAL UNIVERSITY, Moscow, Russia (119454, Moscow, avenue Vernadsky, 78, b. 4), e-mail: <sup>1</sup>pasha\_chasov@mail.ru*

**In this paper, clusterization of the bank's clients based on demographic and financial characteristics was performed using the KMeans, DBSCAN and GMM algorithms. The models were compared in terms of segmentation quality, visualization and interpretation of the obtained clusters were performed. The main client groups are identified and the directions of their practical application in business tasks are proposed.**

**Keywords:** Clustering, K Means, DBSCAN, Gaussian Mixture Model, customer Segmentation, banking data, machine learning, data analysis, preprocessing, data visualization.

Данные о клиентах банков содержат множество параметров, таких как возраст, уровень образования, профессия, наличие кредитов и ипотек. Эти характеристики могут существенно влиять на финансовые привычки людей, в том числе на их среднегодовой баланс. Однако выявить закономерности в таких данных вручную затруднительно, поэтому применение методов машинного обучения, в частности кластерного анализа, позволяет группировать клиентов на основе их финансовых факторов.

Целью настоящего исследования является изучение и анализ существующих методов сегментации клиентов банка на основе финансовых факторов.

Структура данной статьи включают следующие ключевые аспекты:

1. Изучить предметную область темы исследования.
2. Изучить существующие решения.
3. Описать логику разработки проекта.
4. Обосновать выбор инструментального средства для разработки проекта.

5. Подготовить данные и реализовать модель.

6. Проанализировать результаты модели.

Данные для анализа были взяты из открытого набора данных UCI Machine Learning Repository — Bank Marketing Dataset [1]. Этот датасет содержит информацию о клиентах португальского банка, участвовавших в телемаркетинговой кампании по привлечению депозитов. В таблице представлены демографические и финансовые характеристики клиентов, такие как возраст, профессия, образование, семейное положение, наличие кредитов, а также данные о балансе на счёте и других параметрах.

Таблица 1 — Описание атрибутов датасета

Переменная	Тип данных	Описание
age	Числовой	Возраст клиента
job	Категориальный	Тип работы (например, 'admin.', 'blue-collar', 'entrepreneur')
marital	Категориальный	Семейное положение ('divorced', 'married', 'single')
education	Категориальный	Уровень образования ('basic.4y', 'high.school', 'university.degree')
default	Бинарный	Наличие кредита в дефолте ('yes', 'no')
balance	Числовой	Средний годовой баланс в евро
housing	Бинарный	Наличие ипотечного кредита ('yes', 'no')
loan	Бинарный	Наличие персонального кредита ('yes', 'no')
contact	Категориальный	Тип связи ('cellular', 'telephone')
day_of_week	Категориальный	День недели последнего контакта
month	Категориальный	Месяц последнего контакта
duration	Числовой	Продолжительность последнего контакта в секундах
campaign	Числовой	Количество контактов в текущей кампании для данного клиента
pdays	Числовой	Количество дней с момента последнего контакта клиента в предыдущей кампании
previous	Числовой	Количество контактов до текущей кампании для клиента
poutcome	Категориальный	Результат предыдущей маркетинговой кампании ('failure', 'success', 'nonexistent')
y	Бинарный	Подписался ли клиент на срочный депозит ('yes', 'no')

Необходимо разработать модель кластеризации, поскольку традиционные методы сегментации, основанные на статистическом анализе, не всегда могут определить скрытые закономерности [2].

Основной целью разработки модели является автоматизация процесса сегментации клиентов банка с использованием методов машинного обучения. Для достижения этой цели требуется:

- разработать и реализовать алгоритм кластеризации на основе имеющихся данных о клиентах банка;
- определить оптимальное количество кластеров и интерпретировать их содержимое;
- выявить закономерности в финансовом поведении клиентов;
- оценить эффективность предложенного метода сегментации и его применимость для банковского сектора.

Перед разработкой модели требуется подготовить данные для анализа. Целью является проверка данных на пропуски, соответствие типам данных, приведение категориальных признаков к числовому виду, масштабирование числовых признаков, исключение признаков, которые не влияют на сегментацию клиентов.

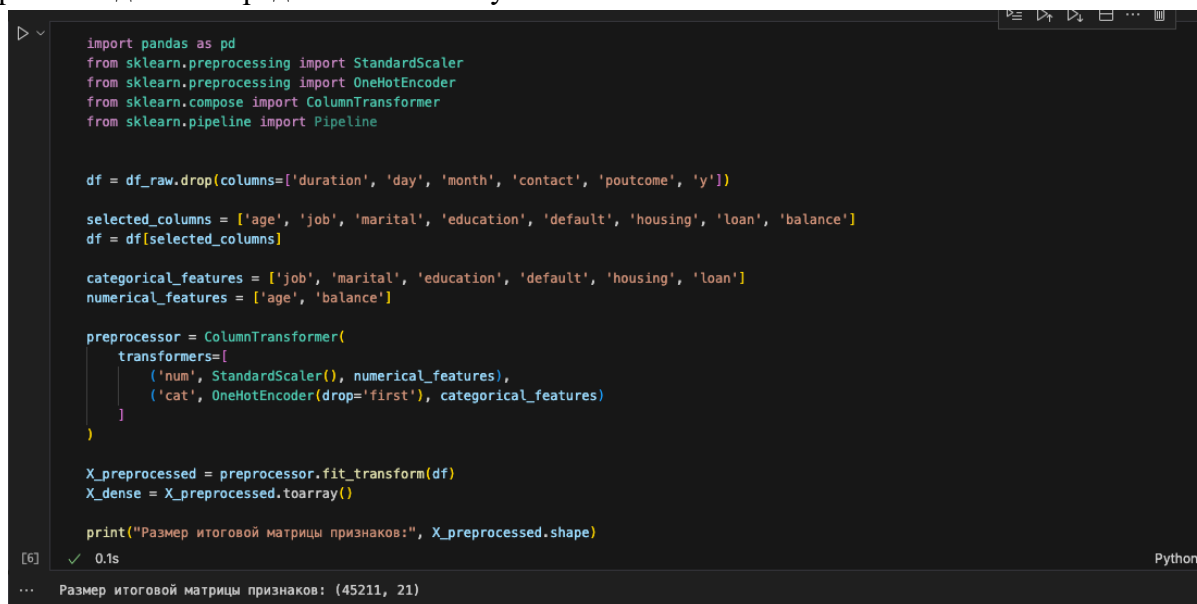
В первую очередь данные были проверены на пропуски и типы данных. Поскольку в данных нет пропусков, а типы данных соответствуют тому, которые должны быть, можно переходить к обработке атрибутов датасета. Были удалены следующие атрибуты:

- duration: длительность последнего контакта;
- day, month: день и месяц звонка клиенту;
- contact, poutcome, y: атрибуты, связанные с результатом или способом взаимодействия с клиентом.

Все эти атрибуты понадобились бы для анализа эффективности работы маркетинговых инструментов, но не для общей кластеризации клиентов. Для кластеризации были отобраны только те признаки, которые являются постоянными для клиента: возраст, баланс, профессия, семейное положение, образование, наличие кредита в дефолте, наличие ипотечного кредита, наличие потребительского кредита.

Эти атрибуты были разделены на два типа: числовые и категориальные. Категориальные признаки были преобразованы с помощью one-hot кодирования, то есть каждый атрибут был разделен на столбцы, где каждый атрибут являлся отдельным столбцом. К числовым признакам было применено стандартное масштабирование с помощью StandardScaler, чтобы все атрибуты были одной размерности и не выбивались при анализе.

Итоговый вариант датасета был конвертирован в плотный формат для работы с моделями, итоговая матрица признаков составила 45211 клиента, 21 признак у каждого. Код обработки данных представлен на Рисунке 1.



```
import pandas as pd
from sklearn.preprocessing import StandardScaler
from sklearn.preprocessing import OneHotEncoder
from sklearn.compose import ColumnTransformer
from sklearn.pipeline import Pipeline

df = df_raw.drop(columns=['duration', 'day', 'month', 'contact', 'poutcome', 'y'])

selected_columns = ['age', 'job', 'marital', 'education', 'default', 'housing', 'loan', 'balance']
df = df[selected_columns]

categorical_features = ['job', 'marital', 'education', 'default', 'housing', 'loan']
numerical_features = ['age', 'balance']

preprocessor = ColumnTransformer(
    transformers=[
        ('num', StandardScaler(), numerical_features),
        ('cat', OneHotEncoder(drop='first'), categorical_features)
    ]
)

X_preprocessed = preprocessor.fit_transform(df)
X_dense = X_preprocessed.toarray()

print("Размер итоговой матрицы признаков:", X_preprocessed.shape)
```

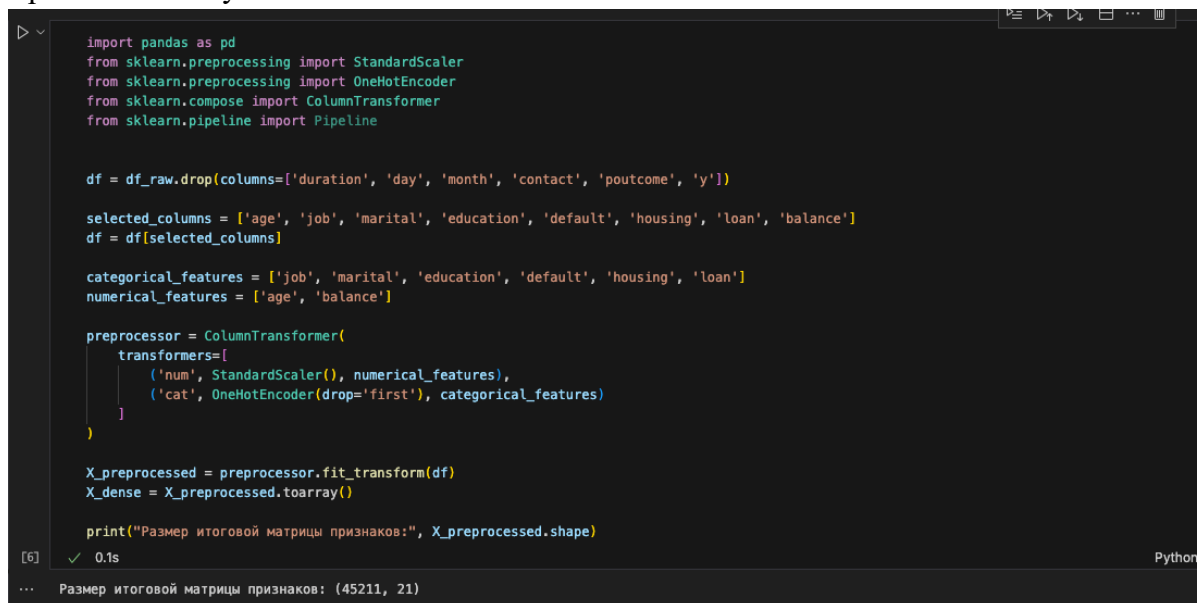
[6] ✓ 0.1s Python

... Размер итоговой матрицы признаков: (45211, 21)

Рисунок 1 — Предобработка данных

Далее была осуществлена разработка модели машинного обучения для кластеризации данных. Для каждой модели требуется подбор параметров и визуализация результата.

Первой моделью является модель KMeans [3]. Для определения оптимального значения  $k$  были использованы два подхода: метод локтя и метод силуэта. Визуализация методов изображена на Рисунке 2.



```
import pandas as pd
from sklearn.preprocessing import StandardScaler
from sklearn.preprocessing import OneHotEncoder
from sklearn.compose import ColumnTransformer
from sklearn.pipeline import Pipeline

df = df_raw.drop(columns=['duration', 'day', 'month', 'contact', 'poutcome', 'y'])

selected_columns = ['age', 'job', 'marital', 'education', 'default', 'housing', 'loan', 'balance']
df = df[selected_columns]

categorical_features = ['job', 'marital', 'education', 'default', 'housing', 'loan']
numerical_features = ['age', 'balance']

preprocessor = ColumnTransformer(
    transformers=[
        ('num', StandardScaler(), numerical_features),
        ('cat', OneHotEncoder(drop='first'), categorical_features)
    ]
)

X_preprocessed = preprocessor.fit_transform(df)
X_dense = X_preprocessed.toarray()

print("Размер итоговой матрицы признаков:", X_preprocessed.shape)
```

[6] ✓ 0.1s Python

... Размер итоговой матрицы признаков: (45211, 21)

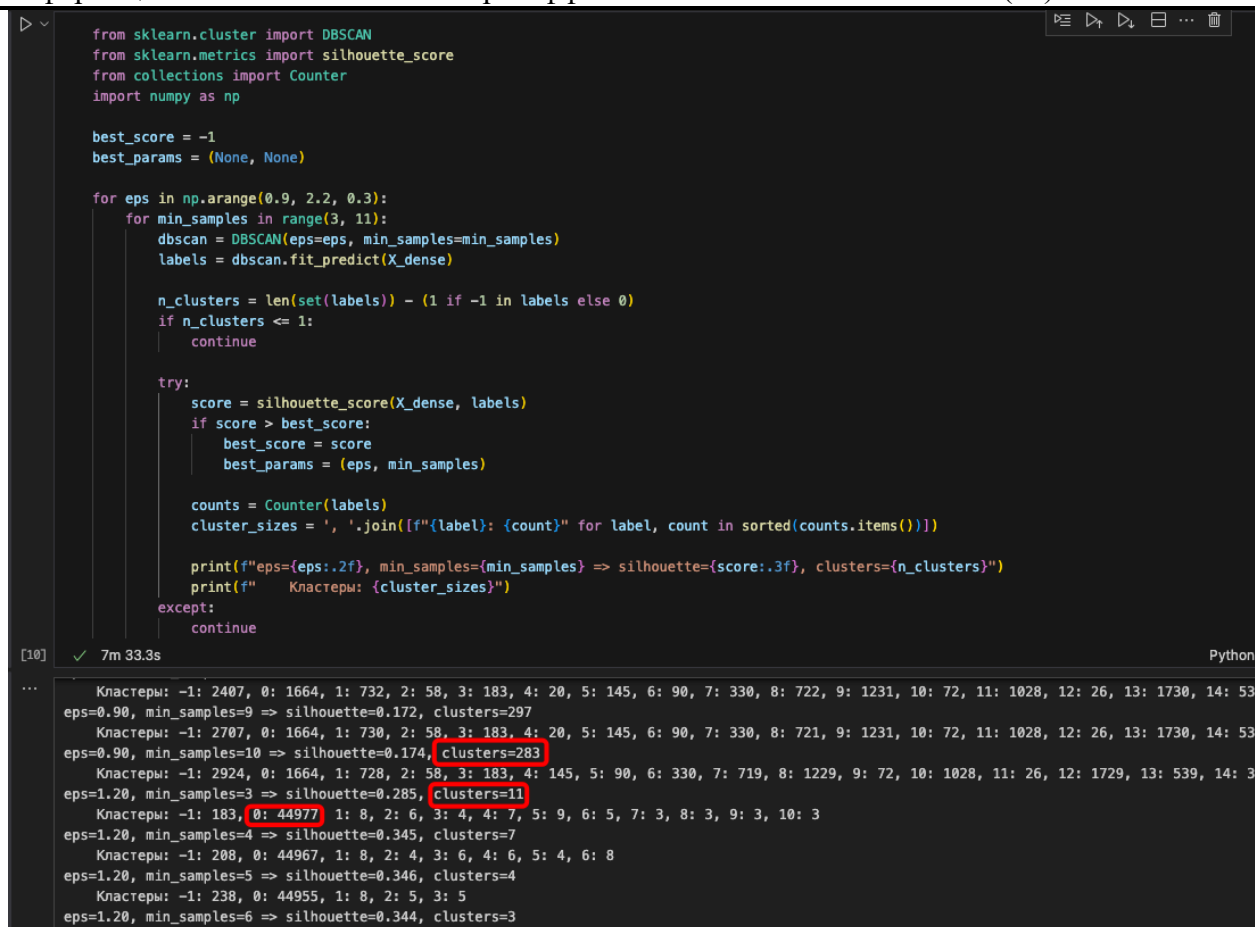
Рисунок 2 — Визуализация методов локтя и силуэта

Визуализация метода локтя показала, что резкое снижение внутрикластерной суммы квадратов происходит от 2 до 4 кластера, затем снижение становится постепенным. Точка перегиба, то есть локоть, наблюдается в точке 4. В методе силуэта видно, что метрика Silhouette Score показывает свой максимум в двойке, однако это слишком малое количество кластеров для деления клиентов, поэтому подходящим для нас будет количество 4.

После определения числа кластеров была обучена модель KMeans на предобработанном наборе данных. Следом идет алгоритм DBSCAN [4], который не требует заранее задания числа кластеров. Однако к нему необходимо подобрать два параметра:

- `eps` — радиус окрестности;
- `min_samples` — минимальное количество точек окрестности, необходимое для формирования кластера.

Было принято решение перебрать комбинации этих параметров для поиска наилучшего. Однако в процессе перебора обнаружилось, что модель при малых `eps` (до 1) давала сотни маленьких кластеров, но при увеличении `eps` сваливала все значения в один большой кластер. Подбор параметров для модели DBSCAN изображен на Рисунке 3.



```
from sklearn.cluster import DBSCAN
from sklearn.metrics import silhouette_score
from collections import Counter
import numpy as np

best_score = -1
best_params = (None, None)

for eps in np.arange(0.9, 2.2, 0.3):
    for min_samples in range(3, 11):
        dbscan = DBSCAN(eps=eps, min_samples=min_samples)
        labels = dbscan.fit_predict(X_dense)

        n_clusters = len(set(labels)) - (1 if -1 in labels else 0)
        if n_clusters <= 1:
            continue

        try:
            score = silhouette_score(X_dense, labels)
            if score > best_score:
                best_score = score
                best_params = (eps, min_samples)

            counts = Counter(labels)
            cluster_sizes = ', '.join([f'{label}: {count}' for label, count in sorted(counts.items())])

            print(f"eps={eps:.2f}, min_samples={min_samples} => silhouette={score:.3f}, clusters={n_clusters}")
            print(f"    Кнастеры: {cluster_sizes}")
        except:
            continue
```

[10] ✓ 7m 33.3s Python

... Кнастеры: -1: 2407, 0: 1664, 1: 732, 2: 58, 3: 183, 4: 20, 5: 145, 6: 90, 7: 330, 8: 722, 9: 1231, 10: 72, 11: 1028, 12: 26, 13: 1730, 14: 53  
eps=0.90, min\_samples=9 => silhouette=0.172, clusters=297  
Кнастеры: -1: 2707, 0: 1664, 1: 730, 2: 58, 3: 183, 4: 20, 5: 145, 6: 90, 7: 330, 8: 721, 9: 1231, 10: 72, 11: 1028, 12: 26, 13: 1730, 14: 53  
eps=0.90, min\_samples=10 => silhouette=0.174, clusters=283  
Кнастеры: -1: 2924, 0: 1664, 1: 728, 2: 58, 3: 183, 4: 145, 5: 90, 6: 330, 7: 719, 8: 1229, 9: 72, 10: 1028, 11: 26, 12: 1729, 13: 539, 14: 3  
eps=1.20, min\_samples=3 => silhouette=0.285, clusters=11  
Кнастеры: -1: 183, 0: 44977, 1: 8, 2: 6, 3: 4, 4: 7, 5: 9, 6: 5, 7: 3, 8: 3, 9: 3, 10: 3  
eps=1.20, min\_samples=4 => silhouette=0.345, clusters=7  
Кнастеры: -1: 208, 0: 44967, 1: 8, 2: 4, 3: 6, 4: 6, 5: 4, 6: 8  
eps=1.20, min\_samples=5 => silhouette=0.346, clusters=4  
Кнастеры: -1: 238, 0: 44955, 1: 8, 2: 5, 3: 5  
eps=1.20, min\_samples=6 => silhouette=0.344, clusters=3

Рисунок 3 — Подбор параметров DBSCAN

Очевидно, что с таким результатом модель является непригодной для использования, однако для сравнения с другими моделями были выбраны следующие параметры, на которых обучилась модель:  $\text{eps}=1.50$ ,  $\text{min\_samples}=7$ ,  $\text{silhouette}=0.644$ ,  $\text{clusters}=3$ .

Последней моделью являлась модель Gaussian Mixture Model (GMM) [5]. Первоначально был произведен подбор параметра `covariance_type`, который отвечает за конфигурацию ковариационной матрицы. Лучшим параметром оказался `covariance_type=spherical`. Далее были подобраны число компонентов (от 2 до 8) и метод инициализации (`kmeans` или `random`). Лучшее качество было достигнуто при  $n=2$ , `init=random`, однако уже было написано о том, что 2 кластера мало для сегментации клиентов, поэтому для финальной модели были выбраны следующие параметры:  $n=3$ , `init=random`,  $\text{silhouette}=0.196$ . Подбор параметров модели изображен на Рисунке 4.

```
from sklearn.mixture import GaussianMixture
from sklearn.metrics import silhouette_score

best_score = -1
best_config = None

for n in range(2, 9):
    for init in ['kmeans', 'random']:
        gmm = GaussianMixture(
            n_components=n,
            covariance_type='spherical', # лучший из прошлого эксперимента
            init_params=init,
            n_init=10,
            max_iter=500,
            reg_covar=1e-4,
            random_state=42
        )
        labels = gmm.fit_predict(X_dense)
        score = silhouette_score(X_dense, labels)

        if score > best_score:
            best_score = score
            best_config = (n, init)

        print(f'n={n}, init={init} => silhouette={score:.3f}')

print(f'\nЛучшие параметры: n_components={best_config[0]}, init={best_config[1]}, silhouette={best_score:.3f}')

[27] ✓ 4m 14.5s
...
n=2, init=kmeans => silhouette=0.214
n=2, init=random => silhouette=0.218
n=3, init=kmeans => silhouette=0.197
n=3, init=random => silhouette=0.196
n=4, init=kmeans => silhouette=0.176
n=4, init=random => silhouette=0.176
n=5, init=kmeans => silhouette=0.163
n=5, init=random => silhouette=0.162
```

Рисунок 4 — Подбор параметров для модели GMM

Для анализа и интерпретации результатов моделей будут использоваться методы снижения размерности: PCA [6], t-SNE [7], UMAP, TriMap, PaCMAP с последующей визуализацией.

После подбора параметров стало понятно, что модель, которая имеет наилучшую метрику Silhouette Score (0,644) является модель DBSCAN, однако она сваливает почти все значения в один огромный кластер. На Рисунке 5 изображено 5 визуализаций модели DBSCAN.

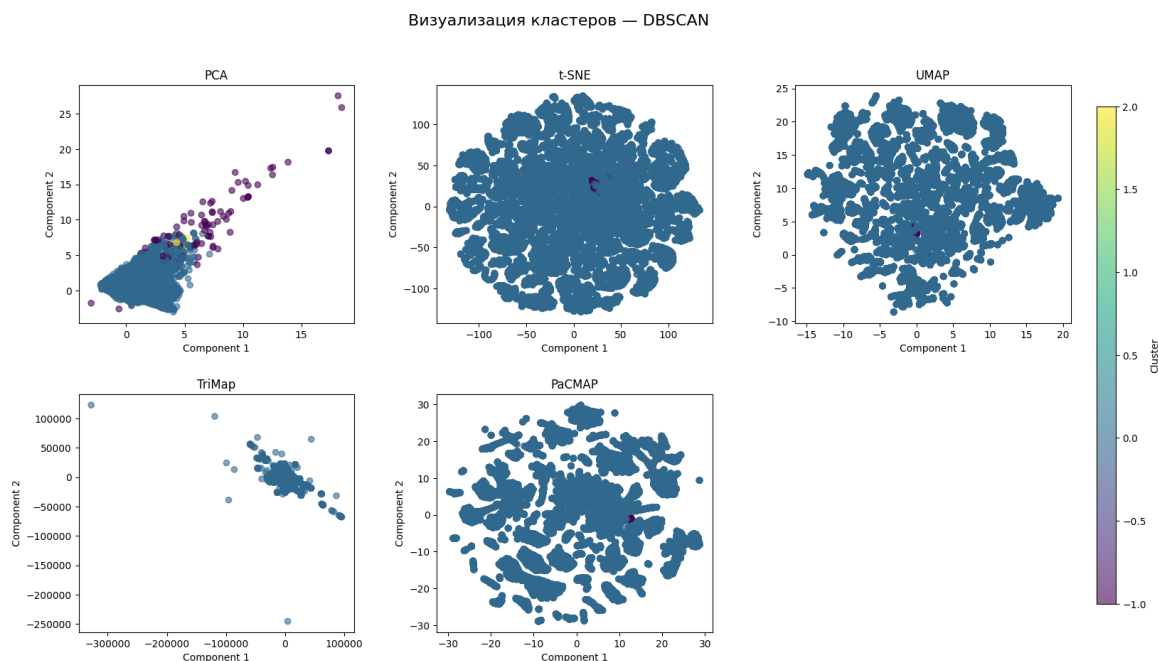


Рисунок 5 — Визуализация модели DBSCAN

На графиках четко видно, все данные состоят почти полностью из одного кластера, что делает модель невозможным для использования в сегментации клиентов банка.

Модель KMeans имеет Silhouette Score равным 0,18 и количество кластеров равным 4, модель GMM имеет Silhouette Score равным 0,197 и количество кластеров равным 3 соответственно. На Рисунке 3.7 изображена визуализация модели KMeans, на Рисунке 3.8 — модель GMM.

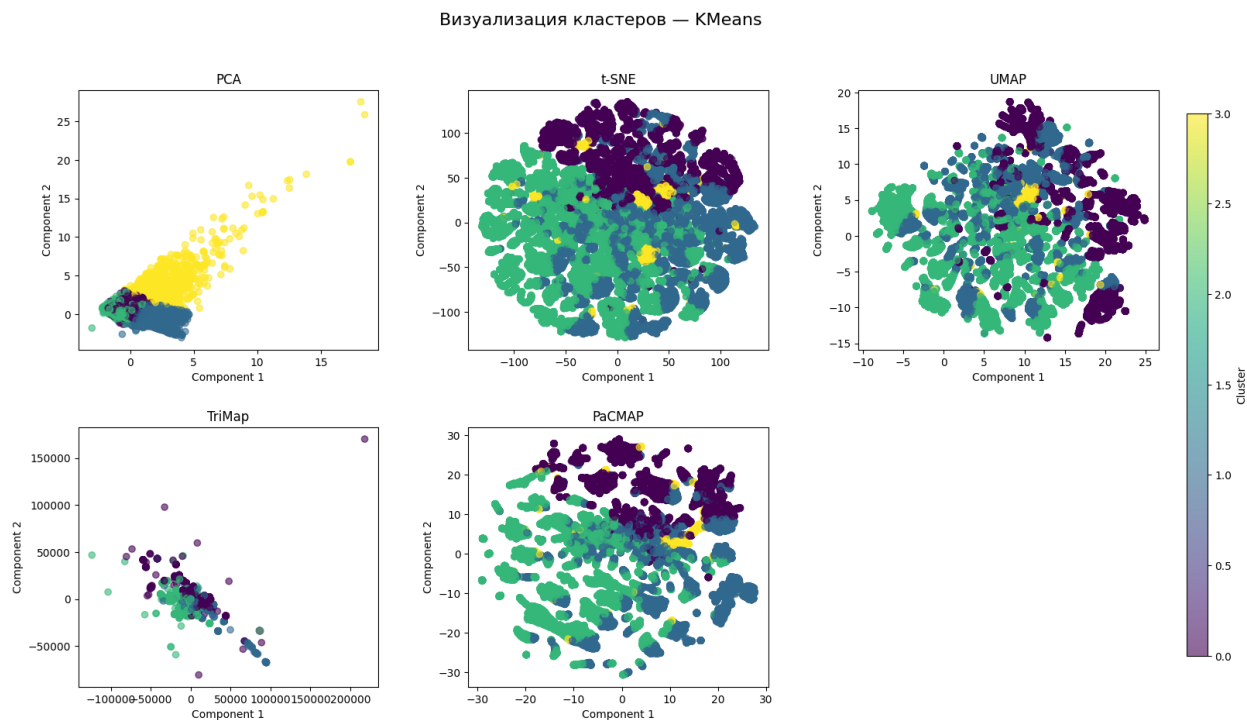


Рисунок 6 — Визуализация модели KMeans

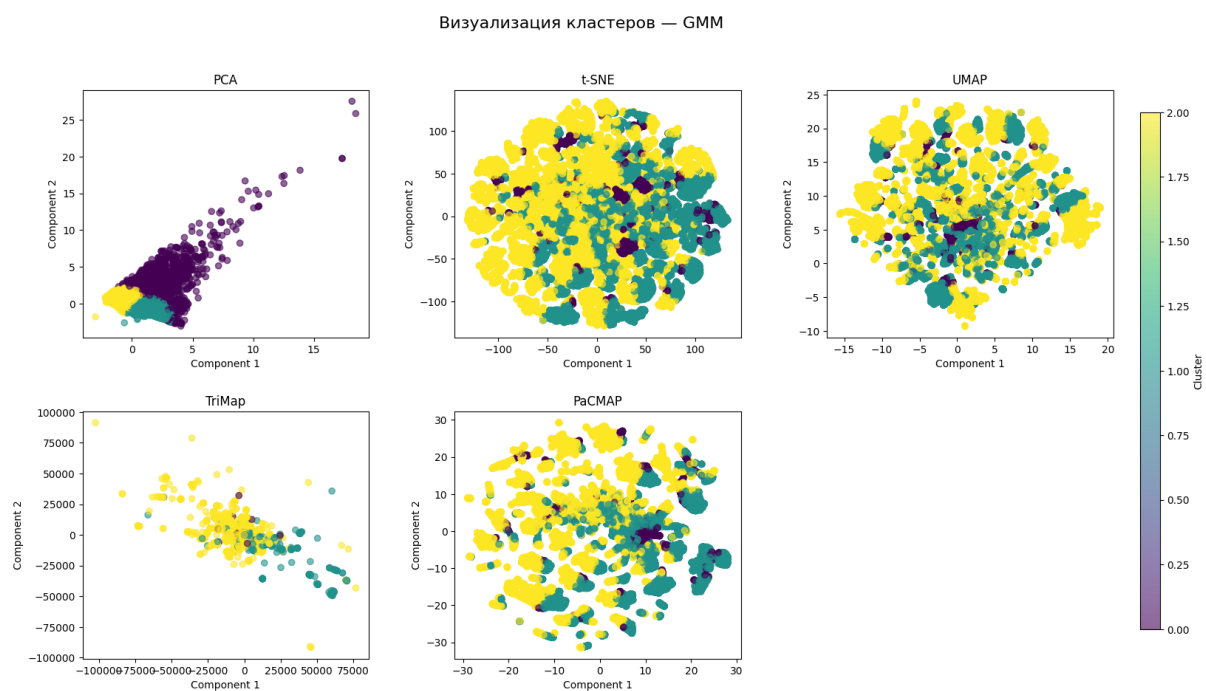


Рисунок 7 — Визуализация модели GMM



На графиках видно, что что на обеих моделях возможно увидеть кластерную структуру, результат возможно интерпретировать. Обе модели имеют схожие показатели по метрике Silhouette Score, что позволяет предположить, что обе модели возможно использовать для сегментации клиентов банка.

После технической реализации модели и сравнения метрик качества важно понять, на какие группы были разбиты клиенты и чем они друг от друга отличаются с точки зрения бизнес составляющей. Для этого были проанализированы средний возраст и баланс клиентов в группах и распределение категориальных признаков: профессии, образования, семейного положения, наличия кредитов и других.

Модель KMeans создало 4 группы клиентов банка:

1. Молодые образованные специалисты без кредитов Выя
2. Пожилые, консервативные клиенты.
3. Молодые заемщики с невысоким балансом.
4. Высокодоходные клиенты с крупными остатками.

Модель GNN создало 3 группы клиентов банка:

1. Состоявшиеся клиенты с умеренным доходом.
2. Старшие клиенты с рабочим или техническим профилем.
3. Молодая аудитория с активным поведением.

Модели схожи в том, что обе выделили группы с высоким балансом, а также группы с молодой аудиторией с низким балансом, которая является массовым сегментом. Однако различаются они тем, что KMeans выделила довольно маленькую группу премиум сегмента (всего 1202 клиента), против 20838 клиентов в модели GMM. Вследствие этого средний баланс премиум группы у KMeans составляет на 30% больше, чем в GNN.

Разные модели могут быть использованы для разных целей, и являются взаимозаменяемыми в зависимости от потребности бизнеса.

KMeans можно использовать для задач, где важно точное и однозначное выделение групп, например:

- определить наиболее состоятельных клиентов (например, кластер из 2% клиентов с максимальным балансом), чтобы предложить им премиальное обслуживание;
- выявить молодую группу с кредитной нагрузкой для таргетированной программы рефинансирования.

GMM полезен там, где нужно учитывать вероятности и размытые границы между сегментами, например:

- найти крупную группу клиентов, имеющих высокий или потенциально высокий уровень дохода, даже если они пока не относятся к элитным клиентам по балансу;
- построить риск-профили клиентов с распределением вероятности принадлежности к «рисковым» или «надёжным» группам.

## Список литературы

1. Набор данных “Sanction list by countries” [Электронный ресурс] / Ravineesh // Kaggle. – Режим доступа: <https://www.kaggle.com/datasets/ravineesh/sanction-list-by-countries> (Дата обращения: 12.05.2025)
2. Документация “Scikit-learn: Machine Learning in Python” [Электронный ресурс] // Scikit-learn. – Режим доступа: <https://scikit-learn.org/stable> (Дата обращения: 12.05.2025)



3. Документация “Scikit-learn: LinearRegression” [Электронный ресурс] // Scikit-learn. – Режим доступа: [https://scikit-learn.org/stable/modules/generated/sklearn.linear\\_model.LinearRegression.html](https://scikit-learn.org/stable/modules/generated/sklearn.linear_model.LinearRegression.html) (Дата обращения: 16.05.2025)
4. Документация “Scikit-learn: RandomForestClassifier” [Электронный ресурс] // Scikit-learn. – Режим доступа: <https://scikit-learn.org/stable/modules/generated/sklearn.ensemble.RandomForestClassifier.html> (Дата обращения: 16.05.2025)
5. Документация “pypi: XGBoost” [Электронный ресурс] // Scikit-learn. – Режим доступа <https://pypi.org/project/xgboost/> (Дата обращения: 16.05.2025)
6. Документация “Scikit-learn: MultinomialNB” [Электронный ресурс] // Scikit-learn. – Режим доступа: [https://scikit-learn.org/stable/modules/generated/sklearn.naive\\_bayes.MultinomialNB.html](https://scikit-learn.org/stable/modules/generated/sklearn.naive_bayes.MultinomialNB.html) (Дата обращения: 16.05.2025)

## References

1. Dataset “Sanction list by countries” [Electronic resource] / Ravineesh // Kaggle. – Access mode: <https://www.kaggle.com/datasets/ravineesh/sanction-list-by-countries> (Дата обращения: 12.05.2025)
  2. Documentation “Scikit-learn: Machine Learning in Python” [Electronic resource] // Scikit-learn. – Access mode: <https://scikit-learn.org/stable> (Дата обращения: 12.05.2025)
  3. Documentation “Scikit-learn: LinearRegression” [Electronic resource] // Scikit-learn. – Access mode: [https://scikit-learn.org/stable/modules/generated/sklearn.linear\\_model.LinearRegression.html](https://scikit-learn.org/stable/modules/generated/sklearn.linear_model.LinearRegression.html) (Дата обращения: 16.05.2025)
  4. Documentation of “Scikit-learn: RandomForestClassifier” [Electronic resource] // Scikit-learn. – Access mode: <https://scikit-learn.org/stable/modules/generated/sklearn.ensemble.RandomForestClassifier.html> (Дата обращения: 16.05.2025)
  5. Documentation of “pypi: XGBoost” [Electronic resource] // Scikit-learn. – Access mode <https://pypi.org/project/xgboost/> (Дата обращения: 16.05.2025)
  6. Documentation “Scikit-learn: MultinomialNB” [Electronic resource] // Scikit-learn. – Access mode: [https://scikit-learn.org/stable/modules/generated/sklearn.naive\\_bayes.MultinomialNB.html](https://scikit-learn.org/stable/modules/generated/sklearn.naive_bayes.MultinomialNB.html) (Дата обращения: 16.05.2025)
-



Международный журнал информационных технологий и  
энергоэффективности

Сайт журнала:

<http://www.openaccessscience.ru/index.php/ijcse/>



УДК 004.738.5: 519.2: 004.9

## МЕТОДЫ ПРОГНОЗИРОВАНИЯ ПОСЕЩАЕМОСТИ ВЕБ-САЙТОВ: КРИТЕРИИ ВЫБОРА И ПРАКТИЧЕСКИЕ РЕКОМЕНДАЦИИ

**Кипилова А.**

ФГАОУ ВО "НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО", Санкт-Петербург, Россия (197101, город Санкт-Петербург, Кронверкский пр-кт, д. 49 литер а), e-mail: [akipilova@gmail.com](mailto:akipilova@gmail.com)

В статье представлен обзор современных методов прогнозирования посещаемости веб-сайтов, в том числе ARIMA, экспоненциальное сглаживание, LSTM, GRU, XGBoost, DWT и прогнозирование по аналогии. Проведён сравнительный анализ моделей с учётом наиболее частых факторов (сезонность, нестабильность трафика, вычислительные ресурсы и точность прогноза). Представлены практические рекомендации по выбору подходящего метода в зависимости от типа сайта и особенностей пользовательского поведения.

Ключевые слова: Прогнозирование веб-трафика, временные ряды, нейронные сети, LSTM, ARIMA, XGBoost, DWT, GRU, веб-аналитика, сезонность.

## WEB SITE TRAFFIC FORECASTING METHODS: SELECTION CRITERIA AND PRACTICAL RECOMMENDATIONS

**Kipilova A.**

"NATIONAL RESEARCH UNIVERSITY ITMO", St. Petersburg, Russia (197101, St. Petersburg, Kronverksky prospekt, 49 letter a), e-mail: [akipilova@gmail.com](mailto:akipilova@gmail.com)

This article presents an overview of modern web traffic forecasting methods, including ARIMA, exponential smoothing, LSTM, GRU, XGBoost, DWT and analogy forecasting. A comparative analysis of the models considering the most frequent factors (seasonality, traffic instability, computational resources and forecast accuracy). Practical recommendations for selecting the appropriate method depending on the type of site and user behavior peculiarities are presented.

Keywords: Web-traffic forecasting, time series, neural networks, LSTM, ARIMA, XGBoost, DWT, GRU, web analytics, seasonality.

### Введение

В связи с быстро растущей популярностью цифровой экономики и глобальной конкуренцией прогнозирование посещаемости веб-сайтов становится одной из наиболее важных областей. Надежное прогнозирование трафика обеспечивает конкурентное преимущество, особенно в условиях высокой динамики поведения пользователей.

При прогнозировании посещаемости сайта необходимо учитывать множество факторов. Временные ряды имеют значительную сезонность, содержат тенденции и могут быть подвержены значительным случайным колебаниям, вызванным внешними событиями или внутренними изменениями в структуре сайта. Кроме того, характер поведения пользователей варьируется в зависимости от типа сайта (информационный, коммерческий, сервисный), региона, целевой группы и других факторов. Эти особенности требуют индивидуального подхода в каждом конкретном случае.

Современные методы анализа временных рядов включают в себя широкий спектр инструментов. От классических статистических моделей, таких как ARIMA и экспоненциальное сглаживание, до моделей машинного обучения и глубоких нейронных сетей, к которым мы относим, например, LSTM и GRU. Количество и качество доступных данных, сложность поведения пользователей, требования к точности прогноза, доступные вычислительные ресурсы, способ интерпретации результатов и уровень квалификации. Именно эти факторы необходимо учитывать при выборе метода.

## **1. Классификация методов прогнозирования**

В этом разделе описаны основные принципы работы каждого метода и область их применения.

### **1.1. Статистические методы прогнозирования**

Модель *ARIMA* (AutoRegressive Integrated Moving Average) включает дифференцирование (интегрирование) начальных данных временного ряда. Дифференцирование временных рядов означает формирование нового временного ряда путём вычитания предшествующего наблюдения из текущего. Смысл этого состоит в исключении определённых тенденций, таких как сезонность, тренды или нестабильная дисперсия в данных временного ряда. [1]

Создается линейная регрессионная модель, в которую входят заданные количество и тип параметров. Данные предварительно обрабатываются с помощью дифференцирования для достижения стационарности, что позволяет устранить трендовые и сезонные компоненты, оказывающие негативное влияние на регрессионную модель. [2]

Метод *экспоненциального сглаживания*. Его ключевым преимуществом являются простые вычисления. Этот метод позволяет выявить тенденцию, сложившуюся на момент последнего наблюдения. Важно отметить, что для достижения надежного прогноза главным аспектом является правильный выбор параметра сглаживания и начальных условий. [3]

### **1.2. Методы машинного обучения**

*LSTM* (Long Short-Term Memory). Долговременная краткосрочная память является специфическим типом архитектуры рекуррентных нейронных сетей, обладающим способностью использовать ранее обработанные данные. В зависимости от процесса обучения сети она может как предсказывать будущие события, так и классифицировать текущее состояние на основе ретроспективной информации. Возможность изучения долгосрочных зависимостей обусловлена структурой блоков LSTM, которая включает в себя элементы, регулирующие процесс обучения. [4]

*GRU* (Gated Recurrent Unit). Это улучшенная версия модели LSTM, с меньшим количеством параметров, что позволяет ускорить обучение и снизить вычислительные затраты, но при этом сохраняя эффективность в прогнозировании. [5]

*XGBoost*. Архитектура этой модели состоит из ансамбля деревьев решений, каждое из которых последовательно обучается для исправления ошибок своих предшественников. Этот метод бустинга позволяет модели улавливать сложные закономерности и взаимодействия в данных временных рядов. В основе модели XGBoost лежат алгоритмы градиентного усиления, которые итеративно минимизируют функцию потерь, добавляя деревья решений в ансамбль. В XGBoost используется техника, называемая градиентным наращиванием, когда каждое

последующее дерево обучается на остатках предыдущих деревьев, тем самым фокусируясь на экземплярах, которые наиболее трудно предсказать. Кроме того, XGBoost использует различные методы регуляризации, такие как сокращение (или скорость обучения) и подвыборка столбцов, чтобы контролировать сложность модели и повышать ее предсказательную способность. [6]

### **1.3. Гибридные модели и альтернативные подходы**

*DWT* (Discrete Wavelet Transform) применяется к числовому ряду, разлагая его на приближённые и детализирующие коэффициенты с использованием фильтров низких и высоких частот. В результате получается представление данных в виде низкочастотной и высокочастотной составляющих, которые впоследствии могут быть восстановлены с помощью обратного преобразования. [7]

*Прогнозирование по аналогии* основано на использовании исторических данных, схожих по паттернам, для предсказания будущего трафика. Этот метод лучше применять в задачах, где явно выражена сезонность. [8]

## **2. Сравнительный анализ выполнения методов**

На основе принципов работы рассматриваемых методов можно сделать некоторые выводы и определить преимущества и недостатки данных моделей прогнозирования веб-трафика.

Модель *ARIMA* можно использовать для анализа данных, содержащих тренды и сезонность. Хорошо работает с данными, которые имеют предсказуемые изменения во времени и требуют стационарности. Часто нужно провести предварительное преобразование данных таким образом, чтобы временный ряд был стационарным. Однако, *ARIMA* может показывать ограниченную точность в случае нестабильных данных, которые могут быть последствием маркетинговых акций, которые приводят к резким изменениям или неожиданным пикам активности.

Модели на основе *LSTM* способны учитывать долгосрочные зависимости и эффективно работать с большими объёмами данных. Это является базой для предсказания трафика с высокой вероятностью появления цикличностей. При этом нужно учитывать значительно больше вычислительных ресурсов и времени для обучения модели. Также в некоторых случаях, результаты модели *LSTM* трудно правильно интерпретировать. [9]

Модель *GRU* является улучшенной версией *LSTM*, которая имеет упрощённую архитектуру (использует меньшее количество параметров). Однако стоит учитывать, что это может негативно повлиять на точность результатов.

Метод *XGBoost* использует алгоритм градиентного бустинга, который строит ансамбли решающих деревьев для получения более точных прогнозов. Этот метод может учитывать сложные взаимозависимости и нелинейные связи в данных. Но *XGBoost* может быть не таким гибким, как *LSTM*, в случае временных рядов, где необходимо учитывать долгосрочные зависимости.

Метод *DWT* позволяет разделить временный ряд на компоненты различной частоты, что помогает выявить как краткосрочные, так и долгосрочные колебания. Поэтому его можно применить при анализе данных с сезонными пиками и резкими изменениями. В отличие от традиционных моделей, позволяет глубже анализировать временные ряды, выделяя различные частотные компоненты, что может привести к более точным прогнозам.

Метод прогнозирования по аналогии не требует сложных вычислений, но его точность часто бывает низкая, особенно на нестабильных или уникальных данных. Этот метод эффективен для сайтов с выраженной сезонностью, когда можно использовать аналогичные периоды из прошлого для предсказания будущих пиков активности.

### **3. Практические рекомендации по выбору метода прогнозирования**

На основании проведённого анализа можно сформулировать следующие выводы.

Для сайтов с относительно предсказуемым трафиком и чётко выраженной сезонностью, таких как интернет-магазины с регулярными акциями или новостные порталы с пиковыми нагрузками в определённые периоды, покажут лучшие результаты более простые статистические методы, в том числе ARIMA или экспоненциальное сглаживание. Они являются достаточно быстрыми в обучении и не требуют больших вычислительных затрат.

Для крупных сайтов с нестабильным трафиком и длительными зависимостями, где трафик может сильно колебаться и зависеть от множества факторов (например, от рекламных акций, внешних событий или сезонных колебаний), предпочтительнее использовать методы машинного обучения LSTM, GRU или XGBoost. XGBoost также можно использовать в работе с данными, где присутствуют сложные взаимодействия между переменными.

Для сайтов с частыми пиками трафика и выраженной сезонностью, где трафик подвержен быстрым и частым колебаниям может быть лучшим решением метод DWT, поскольку позволяет выделять различные частоты и компоненты сигнала, что даёт возможность точнее прогнозировать пиковые значения трафика.

Прогнозирование по аналогии можно использовать для сайтов с ограниченными вычислительными ресурсами и при этом, точность не является критичной.

### **Заключение**

Проведённое исследование позволило систематизировать современные подходы к прогнозированию посещаемости веб-сайтов и провести их сравнительный анализ. Было выявлено, что эффективность метода во многом определяется характером временного ряда, уровнем шума, наличием сезонных и трендовых компонентов, а также ресурсными ограничениями и требованиями к точности прогноза.

Результаты анализа подтверждают, что универсального решения не существует, поскольку модели демонстрируют различную эффективность в зависимости от условий задачи. Простые статистические методы целесообразны при работе со стабильными, слабофлуктуирующими данными, в то время как более сложные архитектуры машинного обучения и гибридные схемы лучше применять при высокой динамике и множестве факторов, влияющих на поведение пользователей.

Таким образом, выбор метода прогнозирования всегда должен быть обоснованным. Практические рекомендации, изложенные в работе, могут служить ориентиром для специалистов, занимающихся веб-аналитикой, при проектировании систем прогнозирования и принятии решений на основе данных.

### **Список литературы**

1. Shelatkar T. et al. Web traffic time series forecasting using ARIMA and LSTM RNN // ITM Web of Conferences. – EDP Sciences, 2020. – Т. 32. – С. 03017.

2. Ho S. L., Xie M. The use of ARIMA models for reliability forecasting and analysis // *Computers & industrial engineering*. – 1998. – Т. 35. – №. 1-2. – С. 213-216.
3. Лажауникас Ю. В., Кочегарова О. С. Применение метода экспоненциального сглаживания при разработке прогнозов экономических процессов // *Закономерности и тенденции развития науки в современном обществе. Сборник статей международной научно-практической конференции*. – 2016. – №. 3. – С. 145-148.
4. Фомичев С. С., Терешков А. А. Прогнозирование посещаемости веб-сайтов из необработанных данных с использованием сетей LSTM // *Modern Science*. 2020. № 5–3. С. 591–597.
5. Chung J. et al. Empirical evaluation of gated recurrent neural networks on sequence modeling // *arXiv preprint arXiv:1412.3555*. – 2014.
6. KC S., Rone S. Comparing Prophet, XGBoost, and LSTM Models for Web Traffic Forecasting: Assessing Model Performance Across Various Time Series Forecasting Scenarios. – 2024.
7. Madan R., Mangipudi P. S. Predicting computer network traffic: a time series forecasting approach using DWT, ARIMA and RNN // *2018 Eleventh International Conference on Contemporary Computing (IC3)*. – IEEE, 2018. – С. 1-5.
8. Борисевич А. С. Математическое прогнозирование в интернет-статистике. – 2003.
9. Telo J. Web Traffic Prediction Using Autoregressive, LSTM, and XGBoost Time Series Models // *Applied Research in Artificial Intelligence and Cloud Computing*. – 2020. – Т. 3. – №. 1. – С. 1-15.

## References

1. Shelatkar T. et al. Web traffic time series forecasting using ARIMA and LSTM RNN // *ITM Web of Conferences*. – EDP Sciences, 2020. – Т. 32. – С. 03017.
  2. Ho S. L., Xie M. The use of ARIMA models for reliability forecasting and analysis // *Computers & industrial engineering*. – 1998. – Т. 35. – №. 1-2. – pp. 213-216.
  3. Lazauninkas J.V., Kochegarova O. S. Application of the exponential smoothing method in the development of forecasts of economic processes. Collection of articles of the international scientific and practical conference. – 2016. – №. 3. – pp. 145-148.
  4. Fomichev S. S., Tereshkov A. A. Forecasting website attendance from raw data using LSTM networks. 2020. № 5–3. pp. 591–597.
  5. Chung J. et al. Empirical evaluation of gated recurrent neural networks on sequence modeling // *arXiv preprint arXiv:1412.3555*. – 2014.
  6. KC S., Rone S. Comparing Prophet, XGBoost, and LSTM Models for Web Traffic Forecasting: Assessing Model Performance Across Various Time Series Forecasting Scenarios. – 2024.
  7. Madan R., Mangipudi P. S. Predicting computer network traffic: a time series forecasting approach using DWT, ARIMA and RNN // *2018 Eleventh International Conference on Contemporary Computing (IC3)*. – IEEE, 2018. – pp. 1-5.
  8. Borisevich A. S. Mathematical Forecasting in Internet Statistics. – 2003.
  9. Telo J. Web Traffic Prediction Using Autoregressive, LSTM, and XGBoost Time Series Models // *Applied Research in Artificial Intelligence and Cloud Computing*. – 2020. – Т. 3. – №. 1. – pp. 1-15.
-



Международный журнал информационных технологий и  
энергоэффективности

Сайт журнала:

<http://www.openaccessscience.ru/index.php/ijcse/>



УДК 004.3: 004.47: 004.49

## ОПТИМИЗАЦИЯ МЕХАНИЗМА ВИРТУАЛИЗАЦИИ В ОПЕРАЦИОННЫХ СИСТЕМАХ ДЛЯ РАБОТЫ С МНОГОЗАДАЧНЫМИ ГРАФИЧЕСКИМИ ИНТЕРФЕЙСАМИ

**Васильев Б.А.**

ФГБОУ ВО САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФЕССОРА М. А. БОНЧ-БРУЕВИЧА, Санкт-Петербург, Россия (193232, г. Санкт-Петербург, просп. Большевиков, 22, корп. 1), e-mail: [boris.2003@mail.ru](mailto:boris.2003@mail.ru)

Современные операционные системы сталкиваются с вызовами, связанными с обработкой многозадачных графических интерфейсов в виртуализированных средах. Увеличение нагрузки на графические подсистемы требует улучшения производительности виртуализации для обеспечения плавности интерфейса и быстрого отклика. В статье рассматриваются подходы к оптимизации механизмов виртуализации, включая аппаратное ускорение, использование технологий GPU-паравиртуализации и оптимизацию управления ресурсами. Предложенные решения способствуют повышению производительности виртуализированных приложений и улучшению пользовательского опыта.

Ключевые слова: Виртуализация, графические интерфейсы, многозадачность, GPU-паравиртуализация, оптимизация ресурсов, операционные системы.

## OPTIMIZATION OF THE VIRTUALIZATION MECHANISM IN OPERATING SYSTEMS FOR WORKING WITH MULTITASKING GRAPHICAL INTERFACES

**Vasiliev B.A.**

ST. PETERSBURG STATE UNIVERSITY OF TELECOMMUNICATIONS NAMED AFTER PROFESSOR M. A. BONCH-BRUEVICH, St. Petersburg, Russia (193232, St. Petersburg, ave. Bolshhevikov, 22, bldg. 1), e-mail: [boris.2003@mail.ru](mailto:boris.2003@mail.ru)

Modern operating systems face challenges in handling multitasking graphical interfaces in virtualized environments. Increased load on graphical subsystems requires enhanced virtualization performance to ensure smooth interfaces and fast responsiveness. This article explores approaches to optimizing virtualization mechanisms, including hardware acceleration, GPU paravirtualization technologies, and resource management optimization. The proposed solutions improve the performance of virtualized applications and enhance user experience.

Keywords: Virtualization, graphical interfaces, multitasking, GPU paravirtualization, resource optimization, operating systems.

### Введение

Современные задачи в области вычислений всё чаще требуют эффективной работы графических интерфейсов в условиях виртуализации. Быстрое развитие технологий виртуализации предоставляет новые возможности для многозадачности, но также ставит новые вызовы. Особенно это касается обработки графических данных, где традиционные механизмы виртуализации сталкиваются с ограничениями производительности. Работа с

виртуализированными графическими интерфейсами, будь то в корпоративных облачных средах или на персональных устройствах, требует высокой производительности, минимальных задержек и плавности интерфейса.

Графические интерфейсы играют ключевую роль в пользовательском опыте, особенно при работе с требовательными к ресурсам приложениями, такими как системы проектирования, редактирования видео или виртуальной реальности. В виртуализированных средах такие задачи сталкиваются с дополнительными ограничениями: необходимо эффективно распределять вычислительные ресурсы между виртуальными машинами, минимизировать задержки передачи графических данных и обеспечивать совместимость различных аппаратных платформ.

Эти проблемы особенно актуальны в условиях роста популярности облачных рабочих столов и виртуальных машин с поддержкой графических приложений. Оптимизация механизмов виртуализации для работы с графическими интерфейсами требует использования современных технологий, таких как GPU-паравиртуализация, аппаратное ускорение и интеллектуальное управление ресурсами.

### **Оптимизация механизма виртуализации в операционных системах для работы с многозадачными графическими интерфейсами**

Виртуализация стала неотъемлемой частью современных операционных систем, особенно в условиях многозадачности и использования облачных вычислений. Однако поддержка многозадачных графических интерфейсов представляет собой особый вызов, так как стандартные механизмы виртуализации не были изначально разработаны для обработки высоких графических нагрузок. Традиционные подходы, основанные на эмуляции графического процессора (GPU), часто не обеспечивают достаточной производительности, что приводит к задержкам интерфейса, низкой частоте кадров и ухудшению пользовательского опыта.

Одним из наиболее эффективных решений является использование GPU-паравиртуализации, которая позволяет разделять графические ресурсы между виртуальными машинами. Технологии, такие как NVIDIA GRID или Intel GVT-g, предоставляют возможность совместного использования GPU на уровне аппаратного обеспечения, что существенно снижает нагрузку на центральный процессор и увеличивает производительность графических приложений. GPU-паравиртуализация также минимизирует задержки передачи данных между хост-системой и гостевыми виртуальными машинами, что особенно важно для приложений, требующих высокой скорости отклика[1] (с. 261).

Аппаратное ускорение, реализованное через современные технологии, такие как Intel VT-d или AMD-Vi, также играет ключевую роль в оптимизации. Эти технологии позволяют виртуальным машинам напрямую использовать аппаратные ресурсы, обеспечивая почти нативную производительность. Виртуализация с аппаратным ускорением значительно снижает задержки ввода-вывода, что критически важно для работы с графическими интерфейсами в режиме реального времени[2] (с. 75).

Другим направлением оптимизации является улучшение управления ресурсами операционной системы. Для эффективной работы графических интерфейсов в условиях многозадачности необходимо динамическое распределение вычислительных мощностей между виртуальными машинами. Современные гипервизоры, такие как VMware ESXi и



Microsoft Hyper-V, используют механизмы прогнозирования нагрузки, чтобы адаптировать распределение ресурсов в зависимости от текущих требований приложений. Например, при увеличении графической нагрузки одной виртуальной машины гипервизор может временно перераспределить ей больше ресурсов GPU, уменьшая нагрузку на менее активные машины[3] (с. 574).

Помимо аппаратных и системных улучшений, важным аспектом является оптимизация программного обеспечения. Современные API, такие как Vulkan или DirectX 12, предоставляют приложениям низкоуровневый доступ к графическому оборудованию, что позволяет минимизировать накладные расходы на обработку данных. Использование этих API в виртуализированных средах требует дополнительных усилий по оптимизации драйверов и программных интерфейсов, чтобы обеспечить совместимость с виртуальными машинами[4] (с. 238).

Также нельзя забывать о пользовательских настройках. Операционные системы должны предлагать гибкие инструменты конфигурации, позволяющие адаптировать производительность виртуализированных графических интерфейсов под конкретные сценарии. Например, использование заранее настроенных профилей производительности для офисной работы, игр или 3D-рендеринга позволяет оптимизировать ресурсы и достичь лучших результатов[5] (с. 719).

Совокупность этих подходов позволяет не только улучшить производительность графических интерфейсов, но и обеспечить их стабильную работу в условиях высоких нагрузок. Это особенно важно для корпоративных пользователей, которые полагаются на облачные рабочие столы и виртуализированные среды для выполнения повседневных задач.

### **Заключение**

Оптимизация механизмов виртуализации для работы с многозадачными графическими интерфейсами является важной задачей для современных операционных систем. С ростом требований к графической производительности виртуализированных приложений традиционные подходы становятся всё менее эффективными. Решение этих проблем требует внедрения передовых технологий GPU-паравиртуализации, использования аппаратного ускорения и совершенствования управления ресурсами.

Эти улучшения позволяют операционным системам лучше адаптироваться к новым вызовам, связанным с развитием облачных сервисов и многозадачности. Пользователи получают более плавный интерфейс, высокую скорость отклика и стабильную работу даже при выполнении ресурсоёмких задач.

В будущем можно ожидать дальнейшего развития виртуализации, включая более глубокую интеграцию с искусственным интеллектом для прогнозирования нагрузок и автоматической оптимизации. Такие инновации сделают виртуализированные графические интерфейсы ещё более эффективными, обеспечивая максимальный комфорт работы в условиях стремительного роста вычислительных мощностей и сетевых технологий.

### **Список литературы**

1. Гельфанд А. М. Способы выбора стежоконтейнеров для передачи данных //Региональная информатика и информационная безопасность. – 2020. – С. 260-262.

2. Красов А. В., Сахаров Д. В., Тасюк А. А. Проектирование системы обнаружения вторжений для информационной сети с использованием больших данных //Научные технологии в космических исследованиях Земли. - 2020. - Т. 12. - № 1. - С. 70-76.
3. Кушнир Д. В. Исследование и разработка методов распределения конфиденциальных данных по квантовым каналам : дис. - Санкт-Петербург. гос. ун-т телекоммуникаций им. МА Бонч-Бруевича, 1996 – С. 570-575.
4. Леснова Е. М., Пестов И. Е. Разработка метода обнаружения и коррекции ошибок для распределенной информационной сети на основе больших данных //Региональная информатика и информационная безопасность. - 2018. - С. 236-240.
5. Миняев А. А. Метод оценки эффективности системы защиты информации территориально-распределенных информационных систем персональных данных //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2020). - 2020. - С. 716-719.

## References

1. Gelfand A.M. Ways of choosing stegocontainers for data transmission //Regional informatics and information security. 2020. pp. 260-262.
  2. Krasov A.V., Sakharov D. V., Tasyuk A. A. Designing an intrusion detection system for an information network using big data //High-tech technologies in space exploration of the Earth. 2020. - Vol. 12. - No. 1. - pp. 70-76.
  3. Kushnir D. V. Research and development of methods for distributing confidential data over quantum channels : St. Petersburg State University of Telecommunications named after MA Bonch-Bruevich, 1996, pp. 570-575.
  4. Lesnova E. M., Pestov I. E. Development of an error detection and correction method for a distributed information network based on based on big data //Regional informatics and information security. - 2018. - pp. 236-240.
  5. Minyaev A. A. Method of evaluating the effectiveness of the information protection system of geographically distributed personal data information systems //Actual problems of infotelec communications in science and education (APINO 2020), 2020, pp. 716-719.
-



Международный журнал информационных технологий и  
энергоэффективности

Сайт журнала:

<http://www.openaccessscience.ru/index.php/ijcse/>



УДК 004.051: 621.38: 615.47: 616-07: 615.8

## ДАТЧИКИ НА ЧИПЕ ДЛЯ ДИАГНОСТИКИ И ТЕРАПИИ

<sup>1</sup> Соловьев В.А., <sup>2</sup>Мухамеджанов Т.М., <sup>3</sup>Гамируллина Д.Р., <sup>4</sup>Орлова О.Д.  
ФГБОУ ВО "МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ  
ИМЕНИ Н.Э. БАУМАНА (НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ)",  
Москва, Россия, (105005, город Москва, 2-Я Бауманская ул, д. 5 стр. 1), e-mail:  
<sup>1</sup>volodimer@bmstu.ru, <sup>2</sup>mtim20@gmail.com, <sup>3</sup>baum.gamirullina@gmail.com,  
<sup>4</sup>or.oksana062@yandex.ru

Развитие микро- и нанoeлектроники привело к появлению LOC — миниатюрных устройств, способных выполнять сложные биомедицинские функции в режиме реального времени. В статье рассматриваются принципы работы и технологии производства LOC, их применение в диагностике и терапии, а также обсуждаются этические, правовые и регуляторные аспекты их внедрения в клиническую практику. Отдельное внимание уделено перспективам развития LOC в контексте персонализированной медицины и интеллектуальных медицинских систем.

Ключевые слова: Lab-on-a-Chip (LOC), биосенсоры, диагностика, терапия, персонализированная медицина, телемедицина, имплантируемые и носимые устройства.

## SENSORS ON A CHIP FOR DIAGNOSTICS AND THERAPY

<sup>1</sup> Soloviev V.A., <sup>2</sup> Mukhamedzhanov T.M., <sup>3</sup>Gamirullina D.R., <sup>4</sup>Orlova O.D.  
BAUMAN MOSCOW STATE TECHNICAL UNIVERSITY (NATIONAL RESEARCH UNIVERSITY),  
Moscow, Russia, (105005, Moscow, 2nd Bauman'skaya ul, 5 bld. 1), e-mail: <sup>1</sup>volodimer@bmstu.ru,  
<sup>2</sup>mtim20@gmail.com, <sup>3</sup>baum.gamirullina@gmail.com, <sup>4</sup>or.oksana062@yandex.ru

The development of micro- and nanoelectronics has led to the emergence of nanochips—miniature devices capable of performing complex biomedical functions in real time. The article discusses the principles of operation and production technologies of nanochips, their application in diagnostics and therapy, as well as discusses the ethical, legal and regulatory aspects of their implementation in clinical practice. Special attention is paid to the prospects for the development of nanochips in the context of personalized medicine and intelligent medical systems.

Keywords: Lab-on-a-Chip (SOC), biosensors, diagnostics, therapy, personalized medicine, telemedicine, implantable and wearable devices.

### Введение

Современная медицина стремительно развивается в направлении персонализированной, быстрой и высокоточной диагностики, а также эффективного и минимально инвазивного лечения. Одной из ключевых движущих сил этой трансформации является внедрение достижений микро- и нанoeлектроники в биомедицинские технологии. Особенно актуальными становятся lab-on-a-chip (далее LOC) — миниатюрные устройства, способные выполнять сложные функции анализа, мониторинга и управления физиологическими процессами организма в реальном времени. Их применение открывает новые горизонты в диагностике заболеваний на ранних стадиях, целевой доставке лекарств и постоянном мониторинге состояния пациента [1].

В условиях растущей нагрузки на системы здравоохранения и увеличения числа хронических заболеваний, интеграция LOC в клиническую практику может значительно повысить эффективность диагностики и терапии, снизить стоимость медицинских процедур и улучшить качество жизни пациентов.

### **Цели и задачи исследования**

*Целью* данной работы является анализ текущего состояния и перспектив развития LOC как одного из наиболее значимых направлений применения микроэлектроники в медицине.

Для достижения этой цели были поставлены следующие *задачи*:

- Рассмотреть теоретические и технологические основы микроэлектроники и производства LOC;
- Проанализировать существующие и перспективные применения LOC в медицинской диагностике и лечении;
- Оценить преимущества, ограничения и вызовы, связанные с использованием LOC в клинической практике;
- Определить ключевые направления дальнейших исследований и разработок в данной области.

### **Краткий обзор состояния исследований**

За последние два десятилетия наблюдается экспоненциальный рост научных публикаций и патентов, посвященных LOC в медицине. Разработаны десятки платформ, включая Lab-on-a-chip, Organ-on-a-chip, а также наноструктурированные биосенсоры, способные анализировать биомаркеры с высокой чувствительностью и специфичностью. Особое внимание уделяется биосовместимости, миниатюризации, автономности питания и беспроводной передаче данных.

Большой вклад в развитие данной области внесли достижения в нанотехнологиях, материаловедении, микрофлюидике и молекулярной биологии. Несмотря на значительный прогресс, ряд проблем, включая стандартизацию, этическую оценку и интеграцию с существующей медицинской инфраструктурой, остаются нерешенными.

### **1. Эволюция микроэлектроники в биомедицине**

Первоначально микроэлектронные технологии применялись преимущественно в составе диагностического оборудования, такого как электрокардиографы (ЭКГ) и магнитно-резонансные томографы (МРТ). С развитием технологий миниатюризации и беспроводной передачи данных стало возможным создавать компактные устройства, способные функционировать внутри организма или в составе носимых систем [4].

Особое развитие получила концепция *Lab-on-a-Chip* (LOC) — интеграция лабораторных функций на микрочипе, которая объединила достижения в области микроэлектроники, микрофлюидики и сенсорных технологий. LOC-устройства позволяют выполнять анализы биологических жидкостей, мониторинг биомаркеров и проведение диагностических процедур в реальном времени, часто без необходимости участия лаборатории или медицинского персонала [4].



Рисунок 1 - Эволюция микроэлектроники в биомедицине.

Эти достижения позволили перейти от эпизодической диагностики к непрерывному мониторингу состояния организма и к использованию устройств, обеспечивающих активное вмешательство и терапию в реальном времени [2,4].

## 2. LOC для медицинской диагностики

### 2.1. Диагностические платформы на основе LOC

LOC в диагностике представляют собой миниатюрные электронные устройства, интегрирующие биосенсоры, микрофлюидные элементы и схемы обработки сигнала. Эти платформы способны обнаруживать биомаркеры — молекулы, указывающие на наличие патологических процессов в организме, — с высокой чувствительностью, специфичностью и скоростью. Диагностические LOC могут быть как стационарными, используемыми в лабораторных условиях, так и портативными, предназначенными для индивидуального или мобильного применения.

Наиболее распространёнными типами LOC, используемых для диагностики, являются биосенсорные чипы, микрофлюидные нанолатформы и оптоэлектронные с электрохимическими LOCи. Биосенсорные чипы используют антитела, ДНК-зонды, ферменты или наночастицы для распознавания специфических биомолекул, что позволяет обеспечивать высокочувствительное выявление различных биологических маркеров. Микрофлюидные нанолатформы позволяют манипулировать малыми объёмами жидкости и проводить множественные анализы на одном чипе, что значительно повышает эффективность диагностики. Оптоэлектронные и электрохимические LOC фиксируют изменения оптических или электрических характеристик при взаимодействии с анализируемым веществом, что способствует точному мониторингу химических и биологических изменений на молекулярном уровне [3].



Рисунок 2 - Типы LOC, используемых для диагностики.

Благодаря своей масштабируемости и интеграции с цифровыми технологиями, LOC могут быть легко объединены с мобильными устройствами и облачными системами, формируя основу для цифровой и дистанционной медицины.

## 2.2. Примеры применения

В качестве примера применения LOC в медицине можно привести анализ биологических жидкостей (кровь, слюна, пот). Одним из важнейших преимуществ является их способность анализировать разнообразные биологические жидкости, что делает диагностику более универсальной и неинвазивной. Наиболее часто используются:

**Кровь:** определение уровня глюкозы, холестерина, тропонинов (при инфаркте), циркулирующих опухолевых ДНК и РНК, гормонов и антител.

**Слюна:** выявление вирусных и бактериальных инфекций (например, COVID-19, грипп, ВИЧ), а также стрессовых и гормональных показателей.

**Пот:** мониторинг уровня электролитов, глюкозы и маркеров обезвоживания, полезно при спортивной медицине и терапии хронических заболеваний.

Использование LOC в анализе жидкостей позволяет сократить время диагностики с нескольких часов или суток до нескольких минут, что особенно важно в экстренных ситуациях. Раннее выявление онкологических, инфекционных и генетических заболеваний.

LOC находят активное применение в ранней диагностике заболеваний, когда клинические симптомы ещё не проявились, но уже можно зафиксировать изменения на молекулярном уровне.

Онкологические заболевания: LOC способны обнаруживать циркулирующие опухолевые клетки, ДНК с мутациями, специфические онкомаркеры (например, PSA, HER2, CA-125) при раке простаты, молочной железы, яичников и др. Ранняя диагностика увеличивает шансы на успешное лечение и снижает затраты.

Инфекционные болезни: использование LOC для экспресс-анализа вирусов (гепатитов, ВИЧ, SARS-CoV-2), бактерий (туберкулёз, стрептококк) и паразитов (малярия) позволяет ускорить изоляцию и начать лечение до распространения заболевания.

Генетические заболевания: LOC, работающие на основе ДНК-гибридизации, используются для выявления наследственных мутаций, полиморфизмов, предрасположенности к заболеваниям (например, BRCA1/2 для рака груди) и фармакогенетического тестирования.

## 2.3. Преимущества по сравнению с традиционными методами

По сравнению с классическими лабораторными и инструментальными методами диагностики [7], LOC обладают рядом преимуществ, которые делают их перспективными для массового внедрения представленных на рисунке .

№ п/п	Преимущества
1	Миниатюризация: позволяют проводить анализы при минимальных объемах биоматериала
2	Скорость: обеспечивают экспресс-результаты в течение минут, тогда как традиционные методы требуют от нескольких часов до суток.
3	Чувствительность и специфичность: использование наноматериалов
4	Автоматизация и цифровизация: интеграция с ИИ и мобильными устройствами упрощает интерпретацию результатов и позволяет проводить диагностику без участия медицинского персонала.
5	Низкая стоимость при массовом производстве: наночипы дешевле в производстве по сравнению с громоздкими лабораторными приборами.
6	Возможность мультиплексного анализа: одновременное определение нескольких маркеров на одном чипе.

Рисунок 3 - Преимущества LOC.

### 3. LOC для терапии и лечения

#### 3.1. Целевая доставка лекарств с использованием LOC

Одним из ключевых направлений применения LOC в терапии является контролируемая поставка лекарственных средств непосредственно к патологическим очагам. В традиционной фармакотерапии действующее вещество распределяется по всему организму, что снижает его эффективность и увеличивает риск побочных эффектов. LOC позволяют осуществлять таргетную терапию, при которой лекарство высвобождается строго в нужное время и в нужном месте.

Механизмы реализации:

- Имплантируемые микросистемы, управляемые по беспроводному каналу (например, по Bluetooth или радиочастоте);
- Триггеры, реагирующие на внешние сигналы (например, ультразвук, инфракрасное излучение, магнитное поле) или внутренние параметры (pH, температура, уровень глюкозы);
- Микро- и нанопомпы, встроенные в чип, осуществляющие дозированную подачу препарата;
- Интеллектуальные полимерные матрицы, высвобождающие активные вещества под контролем электроники.

Применение LOC в терапии иллюстрируется рядом перспективных решений. Так, разработаны управляемые имплантируемые микросистемы, способные осуществлять прицельную доставку химиотерапевтических препаратов непосредственно в опухолевую ткань, минимизируя воздействие на здоровые клетки. Другим примером служат инсулиновые LOC, которые в режиме реального времени определяют уровень глюкозы в крови и автоматически регулируют дозировку вводимого инсулина, функционируя как элемент искусственной поджелудочной железы. Кроме того, активно внедряются имплантируемые устройства длительного действия, обеспечивающие анальгезию и нейростимуляцию, что особенно актуально при лечении хронического болевого синдрома.

### 3.2. Имплантируемые устройства для мониторинга и терапии

Имплантируемые LOC формируют основу новой парадигмы в медицине — концепции постоянной терапии с обратной связью, известной как closed-loop система. Такие технологии обеспечивают непрерывное наблюдение за физиологическими параметрами организма, включая уровень электролитов, артериальное давление и нейронную активность. При выявлении отклонений от нормы система способна автоматически инициировать терапевтическое вмешательство — будь то дозированное высвобождение лекарственного препарата, активация стимуляции органа или передача тревожного сигнала медицинскому специалисту для дальнейших действий [8].

Среди наиболее перспективных терапевтических решений на основе LOC особое внимание привлекают имплантируемые устройства, обеспечивающие таргетное и адаптивное воздействие на организм. Так, нейростимуляторы, применяемые при лечении эпилепсии и болезни Паркинсона, непрерывно регистрируют электрическую активность головного мозга и способны предотвращать развитие приступов путём своевременной модуляции нейронных сигналов. Кардиомониторы и кардиостимуляторы нового поколения автоматически адаптируют параметры стимуляции в зависимости от физической активности пациента и текущих характеристик сердечного ритма, обеспечивая персонализированное кардиологическое вмешательство. Кроме того, в онкологии используются имплантаты, отслеживающие биохимические параметры опухолевой среды и активирующие локализованную терапию — например, высвобождение препаратов или физическое воздействие — исключительно при наличии патологических признаков.



Рисунок 4 - Имплантируемые устройства на основе LOC

### 3.3. Управление терапией в реальном времени

Одна из главных задач современной терапии — сделать её адаптивной, то есть реагирующей на изменяющееся состояние пациента в режиме реального времени. LOC решают эту задачу, обеспечивая непрерывный сбор данных, анализ и автономное принятие решений.

Современные LOC находят широкое применение в системах автономного медицинского вмешательства, обеспечивая управление терапией в режиме реального времени. Так, устройства, предназначенные для пациентов с сахарным диабетом, осуществляют непрерывный мониторинг уровня глюкозы в крови и автоматически регулируют подачу



инсулина, формируя функциональный аналог «искусственной поджелудочной железы». Антибактериальные имплантаты способны адаптивно контролировать высвобождение антибиотиков в зависимости от наличия патогенных микроорганизмов или признаков воспаления, тем самым предотвращая развитие инфекции. В онкологии применяются так называемые онкочипы, которые отслеживают температурные и метаболические показатели в опухолевой ткани и при необходимости активируют локальную терапию, включая точечную термотерапию или радиочастотное воздействие. Внедрение подобных систем существенно снижает необходимость в постоянном медицинском контроле и минимизирует влияние человеческого фактора на лечебный процесс.

### **3.4. Биосовместимость и энергоэффективность устройств**

Для успешного внедрения LOC в терапию необходимо учитывать два критически важных аспекта: биосовместимость и энергообеспечение.

Биосовместимость материалов, используемых для изготовления LOC, играет ключевую роль, так как они должны быть устойчивыми к воздействию биологических жидкостей и не вызывать иммунных реакций. Для этого применяются биосовместимые полимеры, такие как PDMS (полидиметилсилоксан) и полиэтиленгликоль, а также биостабильные металлы, например, титан, золото и платина. Чтобы предотвратить образование фиброзной капсулы вокруг устройства, используются покрытия из гидрогелей.

Важным аспектом для эффективной работы LOC является энергообеспечение. Поскольку многие из этих устройств функционируют автономно, ключевым моментом становится миниатюризация источников энергии. Это включает использование микробатарей и суперконденсаторов, а также разработку технологий для энергосбора из окружающей среды, таких как тепловая, механическая и электромагнитная энергия. Важным шагом является внедрение беспроводных зарядных систем, таких как индуктивная и резонансная зарядка, а также оптимизация схем управления для снижения общего энергопотребления.

LOC для терапии и лечения представляют собой не просто технологическое достижение, а революционный подход к медицине, обеспечивая точность, индивидуализированность и управление лечением в реальном времени. Эти устройства открывают путь к созданию полностью автоматизированных и интеллектуальных систем ухода за пациентом.

## **4. Этические, правовые и регуляторные аспекты использования LOC в медицине**

### **4.1. Вопросы конфиденциальности и защиты персональных медицинских данных**

Одной из ключевых проблем при внедрении LOC в медицину является сбор, хранение и обработка персональной информации о состоянии здоровья пациента. Современные LOC способны в реальном времени фиксировать физиологические параметры и передавать их по беспроводным каналам, что создает риски утечки конфиденциальных данных. Основными вызовами являются несанкционированный доступ к медицинской информации, включая генетические данные, отсутствие прозрачности в использовании полученных данных и возможность дискриминации, например, при приеме на работу или страховании на основе здоровья. В ответ на эти угрозы разрабатываются меры защиты, включая использование протоколов шифрования и аутентификации, хранение данных на защищенных облачных

серверах, соответствующих международным стандартам (таким как GDPR и HIPAA), а также создание этических кодексов и соглашений о конфиденциальности между пациентами, медицинскими учреждениями и разработчиками устройств [9].

#### **4.2. Биобезопасность и потенциальные риски для здоровья**

Использование LOC в клинической практике сопряжено с рядом биологических рисков. Среди них можно выделить иммунные реакции и воспалительные процессы, возникающие в ответ на имплантацию инородных объектов. Потенциальная токсичность наноматериалов также вызывает опасения, особенно в случае их разрушения или деградации в тканях организма. Проблемы с биodeградацией становятся особенно актуальными, когда устройства не растворяются полностью и не выводятся естественным путем. Дополнительные риски связаны с возможным перегревом или механическим повреждением окружающих тканей при длительной работе устройств или при возникновении системных сбоев. Для минимизации этих рисков разрабатываются новые поколения биосовместимых материалов, а также внедряются технологии дистанционного отключения или извлечения LOC в случае необходимости. Ведутся долговременные испытания на безопасность, которые охватывают все стадии жизненного цикла устройств, включая пострегистрационный мониторинг побочных эффектов в реальной клинической практике.

#### **4.3. Регуляторные барьеры и стандарты**

Регулирование медицинских LOC требует согласования законодательства в области медицины, информационных технологий и нанотехнологий. Быстрый прогресс технологий создает сложности с сертификацией и допуском на рынок, так как нормативная база часто отстает от темпов развития. Основными аспектами регулирования являются классификация устройств (диагностические, терапевтические, комбинированные), процедуры сертификации и допуск на рынок, которые включают доклинические и клинические испытания. Также важно учитывать международные стандарты, такие как FDA в США, EMA в Европейском Союзе и ISO, которые устанавливают требования безопасности и качества. В настоящее время разрабатываются новые нормативные рамки для цифровых и имплантируемых медицинских устройств, включая алгоритмы на базе искусственного интеллекта, встраиваемые в LOC.

#### **4.4. Этические дилеммы и общественное восприятие**

Интеграция LOC в повседневную медицинскую практику порождает множество этических вопросов, которые вызывают дискуссии среди врачей, исследователей и общества. Основными проблемами являются инвазивность — допустимость внедрения устройств в тело человека, особенно если пациент не может их отключить, а также свобода выбора, когда пациент может быть под давлением использовать технологии вопреки своей воле. Другим важным вопросом является «техническое неравенство», то есть доступность наномедицинских технологий в развивающихся странах и среди малообеспеченного населения, а также граница между лечением и усилением (enhancement), когда LOC используются для улучшения когнитивных или физических функций у здоровых людей. Для решения этих проблем необходимо вовлекать общество в обсуждение на ранних стадиях разработки технологий, создавать этические комитеты при исследовательских учреждениях и

государственных органах, а также развивать междисциплинарный диалог между учеными, юристами, философами, пациентскими организациями и производителями [9].

Этические и правовые аспекты являются неотъемлемой частью интеграции LOC в медицину. Их учет необходим для создания безопасной, справедливой и устойчивой системы наномедицинских технологий, способной приносить пользу каждому пациенту.

## **5. Перспективы и направления будущих исследований**

### **5.1. Интеграция LOC в персонализированную медицину**

Перспективы использования LOC в медицине выходят за рамки только диагностики и лечения. Эти устройства открывают новые возможности для персонализированной медицины, ориентированной на индивидуальные особенности пациента, его генетический профиль, поведение и экосистему микробиома. LOC могут стать важным элементом этой парадигмы, позволяя анализировать генетические, эпигенетические и молекулярные особенности пациента, что будет способствовать разработке персонализированных терапевтических стратегий. Кроме того, они смогут осуществлять непрерывный мониторинг состояния здоровья в реальном времени, предоставляя данные, на основе которых можно адаптировать лечение. Также с их помощью станет возможным применение таргетированной терапии, основанной на глубоком понимании биологических процессов в организме пациента. Например, чипы, отслеживающие текущие биомаркеры, смогут предсказывать развитие заболеваний, помогая пациентам и врачам принимать обоснованные решения о лечении и профилактике [10].

### **5.2. Развитие многофункциональных LOC**

Будущее LOC в медицине связано с их многофункциональностью. В ближайшие годы исследователи планируют интегрировать несколько ключевых функций в одном устройстве, что позволит более комплексно подходить к диагностике и терапии. Например, планируется создание LOC, которые смогут одновременно проводить анализы, выявлять заболевания и при необходимости высвобождать лекарства прямо на месте. Помимо этого, разрабатываются комбинированные устройства, которые будут не только собирать данные о состоянии здоровья, но и учитывать внешние факторы, такие как температура окружающей среды или физическая активность, с целью предсказания возможных проблем и предложений оптимальных решений. Технологии многозадачности на базе LOC могут радикально изменить подходы к лечению и профилактике заболеваний, обеспечивая более целостный и персонализированный подход к медицинским вмешательствам.

### **5.3. Совершенствование биосовместимости и наноматериалов**

Одним из самых активных направлений будущих исследований является совершенствование биосовместимости материалов, из которых изготавливаются LOC. Современные чипы должны быть не только функциональными, но и безопасными для организма. В будущем особое внимание будет уделяться использованию биоразлагаемых материалов, которые полностью растворяются в организме, устраняя необходимость в их удалении. Также продолжится разработка новых биоматериалов, таких как полимеры, углеродные нанотрубки и графен, которые помогут минимизировать воспалительные реакции и продлить срок службы чипов. Важным шагом станет создание самовосстанавливающихся

систем, что повысит долговечность и эффективность LOC, позволяя им восстанавливаться после повреждений или износа. Эти исследования направлены на создание таких устройств, которые будут «невидимы» для организма, не вызывая реакции отторжения и не нарушая функциональность клеток.

#### **5.4. Разработка интеллектуальных систем на базе LOC**

Следующим значимым этапом в развитии LOC станет интеграция искусственного интеллекта (ИИ) и машинного обучения для принятия решений в реальном времени. Будущее медицинских LOC связано с их способностью автономно анализировать данные о состоянии пациента и, используя алгоритмы машинного обучения, вырабатывать оптимальные рекомендации или принимать решения. Такие устройства смогут обеспечивать предсказательную аналитику, отслеживая изменения в организме до появления симптомов, что позволит проводить профилактику и лечить заболевания на ранних стадиях. Кроме того, LOC будут взаимодействовать с внешними медицинскими системами, синхронизируя данные с базами знаний и экспертными системами, что улучшит диагностику и обмен информацией. Эти интеллектуальные LOC значительно повысят точность диагностики, улучшат эффективность лечения и сделают медицинскую помощь более доступной и своевременной.

#### **5.5. Улучшение источников энергии и беспроводных технологий**

Одной из ключевых проблем при использовании LOC в терапии и диагностике является обеспечение их энергией. Будущие исследования будут сосредоточены на нескольких направлениях. Одним из них является разработка миниатюрных источников питания, таких как беспроводные или микробатареи, которые смогут обеспечивать устройства энергией на протяжении длительного времени без необходимости их замены. Важным аспектом также станет развитие энергосборных технологий, таких как использование тепла тела или механических движений для питания чипов. Это обеспечит долгосрочную работу устройств без внешнего вмешательства. Кроме того, исследуются беспроводные зарядные системы для имплантируемых устройств, что значительно упростит процесс обслуживания и продлит срок их эксплуатации. Все эти технологии сделают использование LOC более удобным, безопасным и эффективным.

Источники энергии для наночипов
Миниатюрные источники питания
Энергосборные технологии
Беспроводные зарядные системы

Рисунок 5 - Источники энергии для LOC

#### **5.6. Мобильные и носимые медицинские устройства на базе LOC**

Носимые устройства на базе LOC, такие как умные браслеты, часы и патчи, которые собирают данные о состоянии здоровья в реальном времени, становятся одним из наиболее быстро развивающихся сегментов медицины. Направления исследований в этой области включают разработку биосенсоров, способных постоянно отслеживать важнейшие параметры здоровья, такие как уровень глюкозы, артериальное давление, пульс и температура тела, с

последующей передачей данных в мобильные приложения или медицинские учреждения. Кроме того, разрабатываются мобильные лаборатории для диагностики различных заболеваний в любых условиях, что значительно улучшит доступ к медицинской помощи в удаленных и развивающихся регионах.

Такие устройства будут играть ключевую роль в телемедицине, позволяя врачам дистанционно следить за состоянием пациентов и своевременно вмешиваться при необходимости.

Будущее LOC в медицине связано с созданием более совершенных и функциональных устройств, которые смогут значительно улучшить диагностику, лечение и профилактику заболеваний. Эти технологии также повысят качество жизни пациентов, а их интеграция с искусственным интеллектом, мобильными приложениями и беспроводными системами откроет новые возможности для персонализированной медицины, повышая доступность и эффективность медицинских услуг.



**Рисунок 6** - Направление для дальнейших исследований.

### **Выводы**

LOC представляют собой перспективную технологию, способную значительно повысить эффективность диагностики, лечения и мониторинга здоровья. Эти устройства могут революционизировать диагностику заболеваний, обеспечить таргетированное лечение и непрерывный мониторинг состояния пациента. В перспективе LOC сыграют ключевую роль в персонализированной медицине, обеспечивая более точный и эффективный подход к лечению [11].

Однако для реализации их полного потенциала необходимо решить ряд технических, этических и регуляторных проблем. Будущее LOC в медицине зависит от дальнейших исследований в области биосовместимости, энергообеспечения, интеграции с искусственным интеллектом и защиты данных. Важно также обеспечить доступность этих технологий для широкой аудитории, что будет способствовать улучшению здоровья населения и доступности медицинской помощи.

### Список литературы

1. Новиков, Ю. Н. Основы микро- и нанoeлектроники: учебник для вузов / Ю. Н. Новиков. — 2-е изд., испр. и доп. — Москва: Радио и связь, 2020. — 480 с.
2. Филиппов, А. В. Микросистемная техника в биомедицине / А. В. Филиппов, С. В. Жуков. — СПб.: Политехника, 2019. — 328 с.
3. Шабатина Т. И. Нанохимия и наноматериалы: учебное пособие. — Москва: МГТУ им. Н.Э. Баумана, 2014. — 63 с.
4. Под редакцией Киселева, А. Н. Биомедицинская электроника: технологии и устройства / А. Н. Киселев (ред.). — Москва: МИР, 2022. — 352 с.
5. Харьков, В. М. Введение в нанотехнологии: учебное пособие / В. М. Харьков. — Москва: Высшая школа, 2020. — 480 с.
6. Сивцов, И. И. Нанопотоника в биомедицинских устройствах / И. И. Сивцов. — Москва: МГТУ, 2022. — 398 с.
7. Белоусов, В. Л. Основы нанопотоники и нанобиотехнологий / В. Л. Белоусов, Д. А. Кузнецов. — Москва: Наука, 2018. — 340 с.
8. Петров, Д. В. Микроэлектронные системы в медицине: диагностика и терапия / Д. В. Петров. — Москва: Энергоатомиздат, 2021. — 276 с.
9. Климов, В. В. Применение наноматериалов в медицине: перспективы и вызовы / В. В. Климов. — Москва: Физматлит, 2019. — 280 с.
10. Гречкин, Н. В. Наночастицы и их применение в биомедицине: от теории к практике / Н. В. Гречкин, А. А. Лобанов. — СПб.: Политехника, 2020. — 220 с.
11. Чистяков, А. И. Биотехнологические аспекты применения наноматериалов в медицине / А. И. Чистяков. — Москва: Вузовская книга, 2021. — 360 с.
12. Иванов, М. П. Современные технологии в биомедицине / М. П. Иванов. — СПб.: БХВ-Петербург, 2019. — 512 с.
13. Денисов, А. А. Учебно-методический комплекс по тематическому направлению деятельности ННС «Наноинженерия»: учебное пособие : в 17 книгах / А. А. Денисов, В. А. Кальнов, В. А. Шахнов ; под редакцией В. А. Шахнова. — Москва : МГТУ им. Баумана, [б. г.]. — Книга 6 : Проектирование наносенсоров — 2011. — 128 с.

### References

1. Novikov, Y. N. Fundamentals of Micro- and Nanoelectronics: Textbook for Higher Education / Y. N. Novikov. — 2nd ed., revised and expanded. — Moscow: Radio i Svyaz, 2020. — 480 p.
2. Filippov, A. V. Microsystems Technology in Biomedicine / A. V. Filippov, S. V. Zhukov. — St. Petersburg: Polytechnika, 2019. — 328 p.
3. Shabatina, T. I. Nanochemistry and Nanomaterials: A Study Guide. — Moscow: Bauman Moscow State Technical University, 2014. — 63 p.
4. Edited by Kiselev, A. N. Biomedical Electronics: Technologies and Devices / A. N. Kiselev (Ed.). — Moscow: MIR, 2022. — 352 p.
5. Kharkov, V. M. Introduction to Nanotechnologies: A Study Guide / V. M. Kharkov. — Moscow: Vysshaya Shkola, 2020. — 480 p.
6. Sivtsov, I. I. Nanophotonics in Biomedical Devices / I. I. Sivtsov. — Moscow: MSTU, 2022. — 398 p.

7. Belozov, V. L. Fundamentals of Nanophotonics and Nanobiotechnologies / V. L. Belozov, D. A. Kuznetsov. — Moscow: Nauka, 2018. — p.340
  8. Petrov, D. V. Microelectronic Systems in Medicine: Diagnostics and Therapy / D. V. Petrov. — Moscow: Energoatomizdat, 2021. — p.276.
  9. Klimov, V. V. Application of Nanomaterials in Medicine: Perspectives and Challenges / V. V. Klimov. — Moscow: Fizmatlit, 2019. — p.280 .
  10. Grechkin, N. V. Nanoparticles and Their Application in Biomedicine: From Theory to Practice / N. V. Grechkin, A. A. Lobanov. — St. Petersburg: Polytechnika, 2020. — p.220.
  11. Chistyakov, A. I. Biotechnological Aspects of the Application of Nanomaterials in Medicine / A. I. Chistyakov. — Moscow: Vuzovskaya Kniga, 2021. — p.360.
  12. Ivanov, M. P. Modern Technologies in Biomedicine / M. P. Ivanov. — St. Petersburg: BHV-Petersburg, 2019. — p.512.
  13. Denisov, A. A. Educational and methodological complex on the thematic area of the NNS "Nanoengineering" : textbook : in 17 books / A. A. Denisov, V. A. Kalnov, V. A. Shakhnov ; edited by V. A. Shakhnov. — Moscow : Bauman Moscow State Technical University, [B. G.]. — Book 6 : Designing nanosensors — 2011. — p.128.
-



Международный журнал информационных технологий и  
энергоэффективности

Сайт журнала: <http://www.openaccessscience.ru/index.php/ijcse/>



УДК 621.3.087.92: 621.383.72

## СРАВНИТЕЛЬНЫЙ АНАЛИЗ АКТИВНОЙ ЭЛЕМЕНТНОЙ БАЗЫ, ИСПОЛЬЗУЕМОЙ В ЯЧЕЙКАХ ТРАКТА ОБРАБОТКИ СИГНАЛА ДЛЯ ОПТОЭЛЕКТРОННЫХ ПРЕОБРАЗОВАТЕЛЕЙ.

<sup>1</sup>Шаренков А.С., Евстафьев С.С.

ФГАОУ ВО "НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ "МОСКОВСКИЙ ИНСТИТУТ ЭЛЕКТРОННОЙ ТЕХНИКИ", Москва, Россия, (124498, город Москва, город Зеленоград, пл. Шокина, д. 1), e-mail: <sup>1</sup>sanya16shar@gmail.com

Рассмотрены основные разновидности активных элементов ячейки тракта обработки сигнала (ТОС). Охарактеризованы существующие типы применяемой активной элементной базы, отмечены их основные достоинства и недостатки. Сравнение аналогов выполнено на основе общих критериев. Даны рекомендации по практическому использованию активной элементной базы в ячейках ТОС.

Ключевые слова. Тракт обработки сигнала (ТОС), аналого-цифровой преобразователь (АЦП), оптоэлектронный преобразователь (ОЭП), двойная коррелированная выборка (ДКВ).

## COMPARATIVE ANALYSIS OF THE ACTIVE ELEMENT BASE USED IN SIGNAL PROCESSING CELLS FOR OPTOELECTRONIC CONVERTERS

<sup>1</sup>Sharenkov A.S., Evstafyev S.S.

"NATIONAL RESEARCH UNIVERSITY "MOSCOW INSTITUTE OF ELECTRONIC TECHNOLOGY", Moscow, Russia, (124498, Moscow, Zelenograd, Shokina Square, 1), e-mail: <sup>1</sup>sanya16shar@gmail.com

The main types of active elements of the signal processing cell (SPP) are considered. The existing types of active element base used are characterized; their main advantages and disadvantages are noted. Comparison of analogues was made on the basis of general criteria. Recommendations are given for the practical use of the active element base in SPP cells.

Keywords. Signal processing path (TOC), analog-to-digital converter (ADC), optoelectronic converter (OP), double correlated sampling (DQ).

### Введение

В настоящее время тема оптоэлектронных преобразователей (ОЭП) для космической промышленности является особенно актуальной, так как именно с их помощью возможно получать различное изображение, даже имея при этом достаточно низкий уровень освещённости. ОЭП - это гибридные фотоприёмные устройства, которые не имеют аналогов в мировом приборостроении по сочетанию качественных параметров и их стоимости. ОЭП предназначен для усиления слабых световых потоков и преобразования излучения в видеосигнал.

В ОЭП осуществляется обработка оптических сигналов, что определяет специфику входящих в его состав элементов, алгоритмов, используемых для обработки сигналов.



В современных оптоэлектронных системах – ячейка тракта обработки сигнала (ТОС) выполняет функцию усиления, фильтрации, модуляции и демодуляции сигнала. Также ячейка ТОС обеспечивает адаптацию сигнала к характеристикам следующих компонентов системы.

Электронный тракт – структурный элемент, который позволяет описывать преобразование сигнала, осуществляемого в электронном тракте ОЭП.

Стоит отметить, что, так как разработка я ТОС для ОЭП имеет очень узкую направленность, не представляется возможным проведение сравнительного анализа из-за малого количества аналогов или вовсе их отсутствия, а также, что немало важно, сами ячейки ТОС выполняют одинаковые функции преобразования сигнала в разных случаях.

Поэтому рациональнее будет выполнить сравнительный анализ по активной элементной базе, применяемой в ячейках ТОС, с обоснованием их выбора.

**Целью** данной работы является выполнение сравнительного анализа применяемых в составе ячейки ТОС аналого-цифровых преобразователей (АЦП), а также анализ функции двойной коррелированной выборки (ДКВ) в составе АЦП и реализация с матрицей прибора с зарядовой связью (ПЗС-матрицей).

### **Основные параметры АЦП**

Основными активными элементами ячейки ТОС являются АЦП.

АЦП находят широкое применение в различных областях современной науки и техники. Они являются неотъемлемой составной частью цифровых измерительных приборов, систем преобразования и отображения информации и т.д. [1].

Как и следует из названия, АЦП выполняет функцию преобразования из аналогового в цифровой сигнал, чтобы система сбора данных могла обрабатывать этот сигнал для отображения, хранения или анализа данных.

Параметры АЦП можно разделить на 2 группы:

- Статические
- Динамические

Статические параметры - характеризуют АЦП при постоянном или очень медленно изменяющемся входном сигнале. К ним относятся: максимальное и минимальное допустимое значение входного сигнала, разрядность, интегральная и дифференциальная нелинейность и др.

Динамические – определяют максимальную скорость преобразования, предельную частоту входного сигнала, шумы и нелинейности [2].

Основными характеристиками при выборе АЦП является:

- Частота преобразования (обычно выражается в отсчетах в секунду);
- Разрядность (выражается в битах);
- Время преобразования (выражается в мс);
- Диапазон напряжения входного сигнала.

Частота преобразования – это показатель, отражающий, как быстро АЦП способен преобразовывать аналоговый сигнал в цифровой. Важно, что при дальнейшей оцифровке АЦП сигналов напряжения нужна точная установка частоты выборки. При задании очень большого значения, расходуется вычислительная мощность и полученные файловые данные очень

велики и неудобны для анализа. При задании очень малого значения частоты преобразования уже появляются две следующие проблемы:

- Утрата важных компонентов динамического сигнала;
- Появление паразитных сигналов.

Разрядность – показатель, отражающий, с какой точностью АЦП преобразовывает сигнал аналога в цифру. Время преобразования – определяет интервал времени от начала преобразования до появления на выходе АЦП устойчивого кода выходного сигнала [3]. Чем выше характеристики скорости и разрядности, тем сложнее и дороже получится преобразователь. Скорость преобразования и разрядность тесно связаны между собой, поэтому, повышая разрядность преобразования, приходится жертвовать скоростью. Диапазон напряжения входного сигнала – определяет максимальную амплитуду сигнала, которую можно подать на вход преобразователя, не вызвав обрезание выходного сигнала. При максимальном диапазоне входного сигнала, на выходе АЦП устанавливается максимальный и минимальный код.

Все представленные характеристики являются ключевыми, при подборе необходимого АЦП, используемого в устройстве, поэтому, в дальнейшем, следует опираться именно на данные характеристики и требования.

Таблица 1 – Сравнительные характеристики типов АЦП [4]

Тип АЦП	Преимущества	Недостатки	Макс. Разрешение	Макс. частота выборки сферы	Сферы применения
Последовательного приближения (РПП)	Хорошее соотношение скорости и разрешения	Отсутствие внутренней защиты от искажения	18 бит	10 МГц	Сбор данных
Дельта-сигма	Высокая динамическая производительность	Отставание на искусственных сигналах	32 бит	1 МГц	Сбор данных, шум и вибрация, аудио
Сдвоенный	Точный, недорогой	Низкая скорость	20 бит	100 Гц	Вольтметры
Конвейерный	Очень быстрый	Ограниченное разрешение	16 бит	1 ГГц	Осциллографы
Параллельный	Самый быстрый	Низкое битовое разрешение	12 бит	10 ГГц	Осциллографы

Существует множество типов АЦП, но в рамках данной статьи в Таблице 1, рассмотрены основные и чаще всего используемые типы, в силу того, что данные архитектуры АЦП занимают определенную нишу в общем диапазоне скорость-разрядность.

Так как в случае с оптоэлектронной аппаратурой ключевым фактором является высокая скорость преобразования, тогда при выборе разрядности, АЦП должны иметь от 12-ти до 16-ти битов дискретизации, что обеспечит оптимальные показатели по точности измерения сигналов.

Также, ключевым фактором при подборе АЦП ячейки ТОС стало наличие функции ДКВ. Здесь важно отметить, что при выполнении сравнительного анализа накладывались ограничения по подбору АЦП с функцией ДКВ, из-за условий дефицита Российских аналогов.

### **Функция ДКВ**

ДКВ – это метод, используемый для подавления низкочастотных шумов и дрейфа уровня сигнала в аналоговых трактах. Он особенно важен в системах с высокими требованиями к точности, например таких как обработка сигналов поступающих с ПЗС-матриц в камерах, медицинском оборудовании или других приборах.

Принцип работы ДКВ основывается на двух этапах сэмплирования:

- Сэмпл шума: измеряется уровень шума (например, темновой заряд ПЗС-матрицы или шум аналогового тракта) в отсутствие полезного сигнала.
- Сэмпл сигнала: измеряется полный сигнал, включающий полезную информацию и шум.
- Вычитание: из значения сигнального сэмпла вычитается значение шумового сэмпла. Это позволяет устранить низкочастотные шумы (например, тепловой шум, дрейф напряжения)

### **Реализация АЦП:**

В АЦП AD9944 (о котором будет говориться чуть позже) ДКВ реализована на аналоговом уровне. Схема включает:

- Интегратор для накопления заряда ПЗС-матрицы.
- Ключи сброса для фиксации уровня шума
- Компаратор для сравнения и коррекции сигнала.

### **Реализация ДКВ с ПЗС-матрицей**

ПЗС - достаточно давно и успешно применяются для регистрации двумерных и одномерных оптических изображений.

Двумерные изображения регистрируются матричными фотоприемниками при получении фотографий и видеоматериалов. Одномерные изображения регистрируются линейными ПЗС-фотоприемниками как в бытовых электронных устройствах, например в сканерах, так и в промышленных и научных приборах, наиболее интересными из которых являются оптические спектрометры, используемые для анализа свойств веществ и параметров источников излучения [5–9].

ПЗС-матрица преобразует свет в электрический заряд, который затем считывается через аналоговый тракт. Шумы при этом возникают на этапах:

- Темновой ток (накопление заряда в отсутствие света).
- Шум считывания (включая шум КМОП-ключей и усилителей).

Схема взаимодействия ПЗС-матрицы и АЦП с ДКВ:

1. Сброс ПЗС-ячейки: ПЗС-матрица сбрасывается, и измеряется уровень шума.
2. Накопление заряда: Ячейка накапливает заряд в течение заданного времени экспозиции.

3. Считывание сигнала: Заряд передается в аналоговый тракт, где измеряется сэмпл сигнала.

4. Коррекция: АЦП вычитает сэмпл шума из сэмпла сигнала, удаляя шумы и дрейф.

Обработка и анализ сигнала ПЗС-матриц производится с применением микропроцессоров или персональных компьютеров, и для этого он должен быть преобразован в цифровую форму с помощью АЦП. Выходной сигнал ПЗС-матрицы формируется транзистором с плавающим затвором (либо с плавающей диффузионной областью), под который последовательно подаются зарядовые пакеты, сформированные в соответствующих элементах секции накопления и пропорциональные количеству поглощенных фотонов.

Для получения корректного преобразования каждого последующего зарядового пакета в выходной сигнал прошлый пакет удаляется импульсом сброса. В результате получается что, в выходном сигнале присутствует уровень напряжения, пропорциональный зарядовому пакету, а также уровень напряжения, который соответствует его отсутствию (уровень нуля).

Тем не менее, после сброса выходной сигнал имеет некоторые флуктуации – так называемый КТС-шум, который зависит от остаточного заряда, температуры и емкости плавающего затвора. КТС-шум возможно практически полностью устранить с помощью ДКВ, применяемой в подавляющем большинстве устройств с ПЗС-матрицами [10]. Для этого в ДКВ с помощью соответствующих управляющих импульсов производится фиксация уровня нуля  $U_R$  после сброса зарядового пакета, а затем выборка сигнала  $U_S$  (Рисунок 1). Разница этих напряжений и дает итоговую амплитуду полезного сигнала.

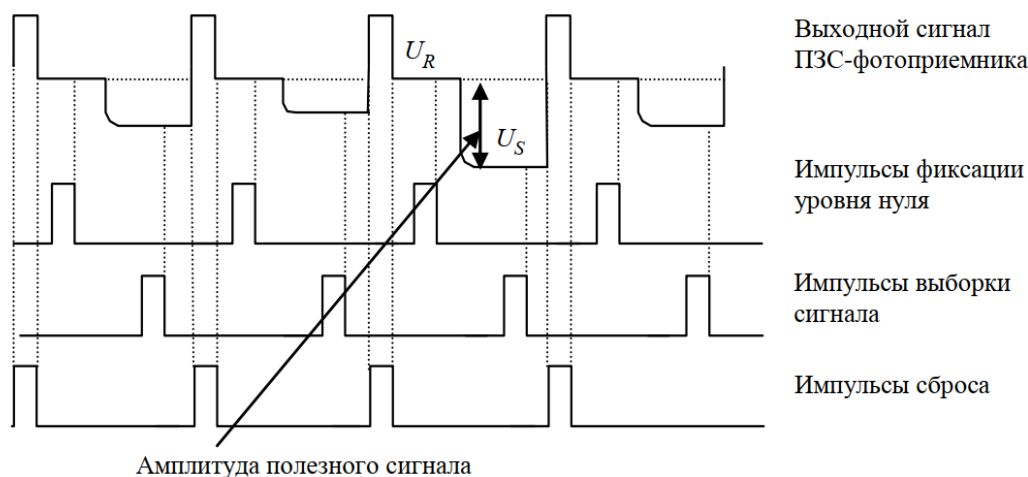


Рисунок 1 - Выборка сигнала для получения полезного сигнала [10]

Поэтому по ходу разработки ячейки ТОС, для реализации сигнала поступающего с ПЗС-матрицы, необходимо применять АЦП именно с функциональной особенностью в виде ДКВ.

Обосновывается это тем, что для получения и преобразования видеосигнала, поступающего с ПЗС-матриц, накладывается высокие требования к помехам, воздействующим на реальный сигнал. Использование архитектур с ДКВ способно существенно снижать низкочастотные шумы,  $1/f$  шумы и тепловые токи.

ДКВ способно повышать отношение сигнал-шум за счет устранения фоновых артефактов.

Увеличение динамического диапазона до 70-80 дБ, что является крайне важным для блоков ОЭП, так как съемка производится в условиях низкой освещенности.

### Обоснование выбора АЦП

В Таблице 2 представлен сравнительный анализ по некоторым основным характеристикам АЦП.

Таблица 2 - Сравнительный анализ некоторых АЦП [11-13]

Критерий оценки	Название		
	AD9944	5112HB035	1273ПА12Т
Максимальное разрешение	12 бит	14 бит	12 бит
Скорость преобразования	100 МГц	300 МГц	160 МГц
Динамический диапазон	85 дБ	80 дБ	80 дБ
Потребление энергии	умеренное	низкое	умеренное
Габариты	7 x 7 x 0.8 мм	12,7 x 12,7 x 2,1 мм	34,5 x 34,5 x 2 мм
Интерфейс	параллельный	параллельный	последовательный

Здесь стоит обозначить, что выбор аналогичных АЦП с функций ДКВ не представляется возможным из-за отсутствия их на Российском рынке.

В сравнении подбирались АЦП конвейерного типа, так как именно данный тип обладает ключевым рядом преимуществ, а именно: высокой скоростью преобразования и оптимальными параметрами по максимальному разрешению, которые позволят обеспечить успешную работу в устройствах на выходе.

Исходя из данных таблицы №2, выбор пал на АЦП AD9944 от Analog Devices.

Проводя сравнительный анализ между моделями, мы можем заметить исходя из данных Таблицы 2, что АЦП 5112HB035 превосходит выбранный AD9944 по показателям максимального разрешения и скорости преобразования. Но как говорилось ранее при

использовании АЦП для летной космической промышленности, накладывается требование по повышенной устойчивости к помехам. К сожалению, как упоминалось ранее, найти аналогичный АЦП с функцией ДКВ на Российском рынке не представляется возможным, поэтому выбор пал на АЦП AD9944 от Analog Devices. Соответственно преимущество 5112HB035 нивелируется отсутствием ДКВ.

Если же рассматривать АЦП 1273ПА12Т, то мы можем заметить, что он достаточно схож по своим параметрам с AD9944, но данный АЦП имеет последовательный интерфейс, который ограничивает скорость передачи данных, а крупные габариты делают модель непригодной для компактных решений. А также в данном АЦП отсутствует функция ДКВ.

Вследствие проведенного сравнительного анализа выбор сделан в сторону AD9944 – это 12-ти разрядный АЦП с параллельным интерфейсом выходных данных, который позволяет передавать все биты группы одновременно за один квант времени, а соответственно обеспечивает быструю передачу данных.

Параллельный интерфейс оптимален для систем с ПЗС-матрицами, где требуется быстрая передача данных.

Также преимуществом является усредненное значение максимального разрешения – 12 бит. Теперь мы знаем, что скорость преобразования и разрядность тесно связаны между собой, поэтому повышая разрядность преобразования, приходится жертвовать скоростью. Но в данном случае, имея наивысшую скорость преобразования, в отличие от представленных аналогов, мы также имеем средний показатель разрядности, что позволяет получать детализированное представление аналогового сигнала.

По параметрам динамического диапазона AD9944 демонстрирует лучший показатель (85 дБ) по сравнению с другими моделями, что позволяет проводить обработку сигналов с большей точностью, обеспечивает лучшее соотношение сигнал/шум, что критично для точной обработки изображений и измерений.

По габаритным показателям, АЦП AD9944, выигрывает у своих конкурентов, габаритные показатели составляют 7х7х0,8 мм (корпус LFCSP), что позволяет удобно размещать элементы АЦП на ячейке ТОС, соблюдая все необходимые требования по габаритным размерам платы.

Еще одним плюсом является тот факт, что при использовании АЦП AD9944, он имеет умеренные показатели по потреблению энергии (250 мВт, питание +3,3В), что положительно отражается на показателях надежности устройства. Также обладает функцией снижения мощности в режиме ожидания.

## **Выводы**

На основании всех вышеупомянутых плюсов и при сравнении АЦП AD9944 с его возможными аналогами, можно сделать вывод, что при разработке ячеек ТОС для ОЭП, следует применять данный АЦП. При сравнительном анализе он обладает оптимальными показателями по скорости преобразования, которая является ключевым фактором при подборе АЦП в сфере активной элементной базы, используемой в ячейках ТОС блоков ОЭП. А также главным преимуществом над аналогами, в виде функции ДКВ, которая позволит минимизировать тепловые токи и дрейфы, и тем самым повысить качество и надежность передаваемого и обрабатываемого сигнала.

Также АЦП AD9944 оптимизирован для работы с ПЗС-матрицами, что подходит под требования проектирования блоков ОЭП.

В заключение, следует заметить, что выбор конкретного АЦП требует тщательного анализа его характеристик и соответствия требований определенного проекта.

Необходимо учитывать параметры, такие как максимальное разрешение, скорость преобразования, интерфейсы, потребление энергии и габариты. После проведения сравнения и анализа характеристик, АЦП AD9944 соответствует необходимым требованиям к ячейке ТОС.

## Список литературы

1. Одинец А.И., Науменко А.П. Цифровые устройства: АЦП и ЦАП: учебное пособие. Омск: ИРСИД, 2006. 48 с.
2. Схемотехника // Хабр URL: [habr.com/ru/companies/milandr/articles/528164/](https://habr.com/ru/companies/milandr/articles/528164/) (дата обращения: 20.03.2025).
3. ИТМО. Аналого-цифровое и цифро-аналоговое преобразование. Лекция №3. 2018.
4. Типы АЦП преобразователей // dewesoft URL: [dewesoft.com/ru/blog/types-of-adc-converters/](https://dewesoft.com/ru/blog/types-of-adc-converters/) (дата обращения: 24.03.2025).
5. Колгин Е.А., Ухов А.А., Савушкин А.В. Спектрометры на основе полихрома и одномерной ПЗС-матрицы: опыт разработки и применения. СПб.: Российский научно-исследовательский институт "Электронстандарт", 2008. С. 120–126.
6. Колгин Е.А., Ухов А.А., Воронин А.А. Спектрометрическое устройство для идентификации пород древесины. СПб.: Российский научно-исследовательский институт "Электронстандарт", 2008. С. 116–119.
7. Воронин А.А., Герасимов В.А., Кострин Д.К. Модернизация приборов и методики спектральной идентификации пород древесины // Биотехносфера. 2013. №3. С. 16-20.
8. Василевский А. М., Коноплев Г. А., Светлов Д. А. Оптико-электронная информационно-измерительная система контроля дезинфицирующих средств на основе полигексаметиленгуанидина // Медицинская техника. 2014. № 1. С. 10–13.
9. Кострин Д. К., Ухов А. А. Метод контроля пространственного распределения световых и цветовых характеристик излучения светодиодов // Контроль. Диагностика. 2014. № 2. С. 65–68.
10. Пресс Ф.П. Фоточувствительные приборы с зарядовой связью. М.: Радио и связь, 1991. 264 с.
11. Комплектные 10-разрядные и 12-разрядные процессоры с частотой 25 МГц ПЗС-сигнальные процессоры // micro-semiconductor URL: [micro-semiconductor.com/datasheet/43-AD9943KCPZ.pdf](https://micro-semiconductor.com/datasheet/43-AD9943KCPZ.pdf) (дата обращения: 07.04.2025).
12. 5112HB035 14-ти разрядный АЦП с встроенной автокалибровкой и параллельным КМОП/LVDS интерфейсом выходных данных // dcsoyuz URL: [dcsoyuz.ru/products/ic-adc-dac/art/1655](https://dcsoyuz.ru/products/ic-adc-dac/art/1655) (дата обращения: 07.04.2025).
13. 1273ПА12Т быстродействующий двухканальный ЦАП повышенной спецстойкости // niiet URL: [niiet.ru/product/1273-па12т-2/](https://niiet.ru/product/1273-па12т-2/) (дата обращения: 07.04.2025).

## References

1. Odinets A.I., Naumenko A.P. Digital devices: ADC and DAC: a training manual. Omsk: IRSID, 2006. p. 48
  2. Circuit engineering // Habr URL: [habr.com/ru/companies/milandr/articles/528164/](https://habr.com/ru/companies/milandr/articles/528164/) (accessed: 03/20/2025).
  3. ITMO. Analog-to-digital and digital-to-analog conversion. Lecture No. 3. 2018.
  4. Types of ADC converters // dewesoft URL: [dewesoft.com/ru/blog/types-of-adc-converters/](https://dewesoft.com/ru/blog/types-of-adc-converters/) (date of access: 03/24/2025).
  5. Kolgin E.A., Ukhov A.A., Savushkin A.V. Spectrometers based on polychrome and one-dimensional CCD matrix: development and application experience. St. Petersburg: Russian Research Institute "Electronstandart", 2008. pp. 120-126.
  6. Kolgin E.A., Ukhov A.A., Voronin A.A. Spectrometric device for identification of wood species. Saint Petersburg: Russian Scientific Research Institute "Electronstandart", 2008. pp. 116-119.
  7. Voronin A.A., Gerasimov V.A., Kostrin D.K. Modernization of instruments and methods of spectral identification of wood species // Biotechnosphere. 2013. No. 3. pp. 16-20.
  8. Vasilevsky A.M., Konoplev G. A., Svetlov D. A. Optical-electronic information-measuring system for control of disinfectants based on polyhexamethylene guanidine // Medical equipment. 2014. No. 1. pp. 10-13.
  9. Kostrin D. K., Ukhov A. A. A method for controlling the spatial distribution of light and color characteristics of LED radiation. Diagnostics. 2014. No. 2. pp. 65-68.
  10. Press F.P. Photosensitive devices with charge coupling. Moscow: Radio and Communications, 1991. p.264
  11. Complete 10-bit and 12-bit processors with a frequency of 25 MHz CCD signal processors // micro-semiconductor URL: [micro-semiconductor.com/datasheet/43-AD9943KCPZ.pdf](https://micro-semiconductor.com/datasheet/43-AD9943KCPZ.pdf) (date of access: 04/07/2025).
  12. 5112NV035 14-bit ADC with integrated auto-calibration and parallel CMOS/LVDS output interface // dcsouyuz URL: [dcsouyuz.ru/products/ic-adc-dac/art/1655](https://dcsouyuz.ru/products/ic-adc-dac/art/1655) (date of issue: 04/07/2025).
  13. 1273PA12T high-speed dual-channel high-resistance DAC // niiet URL: [niiet.ru/product/1273-na12t-2/](https://niiet.ru/product/1273-na12t-2/) (date of access: 04/07/2025).
-





Международный журнал информационных технологий и энергоэффективности

Сайт журнала:

<http://www.openaccessscience.ru/index.php/ijcse/>



УДК 621.039:339.9

## ИНТЕГРАЦИЯ ВОДОРОДНЫХ КОМПЛЕКСОВ С АЭС: ИСПОЛЬЗОВАНИЕ ИЗБЫТОЧНОЙ МОЩНОСТИ НА ПРИМЕРЕ КОЛЬСКОЙ АЭС

**Роботко А.А.**

ФГАОУ ВО "НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ЯДЕРНЫЙ УНИВЕРСИТЕТ "МИФИ", Москва, Россия (115409, город Москва, Каширское ш., д.31), e-mail: [robotko.anna@gmail.com](mailto:robotko.anna@gmail.com)

В статье рассмотрена проблема неэффективного использования избыточной электроэнергии атомных электростанций (АЭС) в периоды низкого энергопотребления. В качестве решения предложена интеграция водородных комплексов, позволяющая преобразовывать избыток энергии в водород, который может использоваться как энергоноситель. На примере Кольской АЭС проанализированы технологические, экономические и экологические аспекты внедрения электролизных установок. Результаты исследования демонстрируют снижение потерь энергии, повышение гибкости работы АЭС и потенциал для декарбонизации энергетики. Экономическая оценка подтверждает целесообразность проекта при условии оптимизации стоимости производства водорода.

Ключевые слова: Атомная электростанция, водородные комплексы, избыточная мощность, электролиз, Кольская АЭС, энергоэффективность, декарбонизация, устойчивая энергетика.

## INTEGRATION OF HYDROGEN COMPLEXES WITH NUCLEAR POWER PLANTS: USING EXCESS CAPACITY ON THE EXAMPLE OF THE KOLA NPP

**Robotko A.A.**

"NATIONAL RESEARCH NUCLEAR UNIVERSITY "MEPHI", Moscow, Russia (115409, Moscow, Kashirskoye sh., 31 e-mail: [robotko.anna@gmail.com](mailto:robotko.anna@gmail.com)

The article addresses the issue of inefficient utilization of excess electricity generated by nuclear power plants (NPPs) during periods of low energy demand. A solution is proposed through the integration of hydrogen complexes, which convert surplus energy into hydrogen as an energy carrier. Using the example of the Kola NPP, the technological, economic, and environmental aspects of implementing electrolysis units are analyzed. The study results demonstrate reduced energy losses, increased operational flexibility of NPPs, and potential for decarbonization. The economic assessment confirms the feasibility of the project, provided the cost of hydrogen production is optimized.

Keywords: Nuclear power plant, hydrogen complexes, excess capacity, electrolysis, Kola NPP, energy efficiency, decarbonization, sustainable energy.

В последние десятилетия мир сталкивается с нарастающей проблемой изменения климата и истощения традиционных источников энергии. В этом контексте атомные электростанции (АЭС) представляют собой важный элемент энергетической инфраструктуры, обеспечивая значительные объемы электроэнергии с низким уровнем выбросов углерода. Однако, несмотря на их высокую производительность, АЭС часто сталкиваются с проблемой неэффективного использования избыточной электроэнергии, особенно в периоды низкого потребления. Это создает необходимость в поиске новых решений, которые позволят

максимально эффективно использовать генерируемую электроэнергию и одновременно способствовать переходу к более экологически чистым источникам энергии.

Одним из наиболее перспективных направлений является интеграция водородных комплексов с АЭС. Водород, как универсальный энергетический носитель, может быть произведен из избыточной электроэнергии, что позволит не только снизить потери энергии, но и создать новые возможности для хранения и транспортировки энергии. В рамках данной работы будет рассмотрен проект, посвященный исследованию интеграции атомных электростанций с водородными комплексами на примере Кольской АЭС. Этот проект предлагает новую схему, позволяющую эффективно использовать избыточную электроэнергию для производства водорода, что открывает новые горизонты для развития водородной энергетики.

Важным аспектом работы станет анализ существующих технологий водородного производства. На сегодняшний день существует несколько методов, включая электролиз воды, паровую реформу метана и термохимические циклы. Каждый из этих методов имеет свои преимущества и недостатки, и их оценка позволит выбрать наиболее подходящий для интеграции с АЭС. В рамках работы также будет разработана схема интеграции водородных комплексов с АЭС, что позволит оптимизировать процессы производства и использования водорода.

Кроме того, особое внимание будет уделено исследованию эффективности сжигания водорода. Водород может быть использован как чистое топливо для генерации электроэнергии, и его сжигание в газовых турбинах или котлах может значительно снизить выбросы углерода. Оценка эффективности этого процесса станет важным шагом в понимании потенциала водородной энергетики.

Не менее важным аспектом является экономическая целесообразность проекта. В условиях растущих цен на энергоносители и необходимости перехода к устойчивым источникам энергии, оценка затрат и выгод от интеграции водородных комплексов с АЭС станет ключевым элементом для принятия решений о реализации данного проекта.

В заключение, работа будет освещать перспективы дальнейшего развития водородной энергетики, включая возможные сценарии внедрения водородных технологий в энергетическую систему России и мира. Пример Кольской АЭС станет основой для анализа и разработки рекомендаций по эффективному использованию избыточной электроэнергии, что, в свою очередь, может способствовать более устойчивому и экологически чистому будущему.

### **Проблематика неэффективного использования избыточной электроэнергии**

Неэффективное использование избыточной электроэнергии на атомных электростанциях (АЭС) представляет собой одну из наиважнейших проблем, особенно в условиях растущего спроса на электроэнергию и ограниченной возможности АЭС быстро изменять свою мощность. Данная проблема становится более актуальной на фоне необходимости обеспечения стабильности энергосистем, где увеличение доли возобновляемых источников энергии (ВИЭ) заметно изменяет требования к электросетям и производителям электроэнергии [3].

Существующие технологии, предназначенные для хранения энергии, например низкотемпературный электролиз, могут оптимизировать процесс использования избыточной энергии, однако их внедрение требует как значительных капиталовложений, так и

переосмысления структуры управления на АЭС. Это включает в себя оптимизацию работы атомных станций, адаптацию их к условиям переменного спроса и необходимость в разработке новых подходов к управлению их мощностями [31].

Избыточная энергия может быть использована для производства водорода, что является интересным направлением в контексте декарбонизации энергетического сектора. В случае когда установленная мощность АЭС превышает потребности региона, созданный избыточный электрический ток может быть использован для генерации водорода [1]. Это не только оптимизирует эксплуатацию АЭС, но и срок службы установок, позволяя им работать более назидательно в условиях изменяющегося спроса [4].

Сравнение себестоимости электроэнергии от различных источников показывает, что АЭС остаются достаточно конкурентоспособными. Однако недостаточная гибкость в управлении электрическими нагрузками обостряет вопросы о целесообразности их использования в современных условиях. Зачастую избыточная энергия, производимая на АЭС, просто теряется, что создает дополнительные экономические потери и негативные экологические последствия [3].

В сценарии, где водород становится основным элементом в новых энергетических системах, возможности интеграции водородных комплексов с АЭС могут стать путём, способствующим более рациональному расходованию ресурсов и уменьшению устойчивого экологического ущерба [22]. Тем не менее, реализация этого потенциала потребует комплексного подхода к проектированию энергосетей и внедрения новых технологий, что само по себе является вызовом для атомной энергетики.

### **Текущие технологии водородного производства**

Водородные комплексы, обретающие всё большую популярность в контексте переработки избыточной электроэнергии, могут использовать различные методы производства водорода. К основным методам относятся паровой риформинг метана, газификация угля и электролиз воды.

Паровой риформинг метана является ключевым способом производства, составляя около 85% от общего объема. Этот процесс включает в себя нагревание метана водяным паром при наличии катализатора, что приводит к образованию водорода с высокой эффективностью, превышающей 80% [28]. Существует также метод газификации угля, который позволяет получать водород из угольного топлива через процесс термической обработки, превращающей уголь в синтетический газ [9].

Электролиз воды, в свою очередь, использует электрическую энергию для разложения воды на водород и кислород. Несмотря на свой потенциал для производства "зеленого" водорода, этот метод сталкивается с высокой стоимостью и требует большого количества электроэнергии, что делает его менее привлекательным, особенно в условиях избытка электроэнергии от атомных электростанций [14]. Разработка экономически эффективного оборудования для электролиза потребует значительных инвестиций и времени.

Среди других технологий можно упомянуть получение водорода из аммиака, которое также имеет свои преимущества и недостатки. В частности, когда аммиак разлагается, он позволяет получать чистый водород, но требует наличия сложных установок для обеспечения безопасности и эффективности процесса. Существуют и другие подходы, такие как

термохимические процессы, которые обещают расширить возможности производства водорода.

Современные вызовы в производстве водорода также связаны с его безопасностью, возможностями хранения и транспортировки. Эти аспекты труда и науки требуют особого внимания, так как эффективное создание инфраструктуры для водородной энергетики неразрывно связано с обеспечением безопасных условий для использования и хранения водорода [29]. Объем мирового производства водорода на сегодняшний день составляет более 70 миллионов тонн, с ожидаемым ростом в ближайшие годы, что открывает большие перспективы для водородных комплексов [16].

Таким образом, при интеграции водородных комплексов с АЭС возможно существенно снизить потерю избыточной электроэнергии. Использование имеющейся инфраструктуры и технологий может помочь достичь этого, однако необходимы дальнейшие усилия в области исследований и внедрения новинок для повышения эффективности всего процесса.

### **Схемы интеграции водородных комплексов с АЭС**

Интеграция водородных комплексов с атомными электростанциями (АЭС) открывает новые горизонты в использовании избыточной электроэнергии, особенно в условиях нестабильности спроса на электроэнергию. В частности, схемы комбинирования могут включать создание стендовых испытательных комплексов, которые служат для эффективного производства водорода и кислорода на базе существующих реакторов, таких как ВВЭР-1000 [12]. Одной из основных задач таких комплексов является необходимость оптимизации процессов перегрева пара в влажно-паровых циклах АЭС [32].

Кольская АЭС представляет собой яркий пример внедрения водородных комплексов благодаря ее географическому расположению и установленной мощности в 65,9%. Данная мощность предоставляет возможности для тестирования новых технологий в условиях нестабильного потребления энергии [26]. Использование водорода в паротурбинных циклах позволит значительно повысить производительность систем, однако важно учитывать вопросы надежности и стабильности данных технологий [20].

Разработка принципиальных схем, объединяющих АЭС с водородными комплексами, подразумевает создание систем электролиза, компримирования и хранения водорода. Эти технологии требуют серьезного подхода к минимизации рисков и отказов в работе оборудования [30]. Внедрение новых принципов комбинирования на основе существующих моделей АЭС позволяет учитывать внутренние и внешние изменения в энергетических рынках, что делает их более устойчивыми к долгосрочным изменениям [12].

Предложенные решения по комбинированию электроэнергетических установок с водородными системами помогут в реализации государственной стратегии по созданию адаптивных и высокоэффективных энергосистем, соответствующих требованиям современности. Важно, что подходы к интеграции будут учитывать не только эксплуатационные, но и экономические аспекты, что позволит снизить затраты и повысить общую эффективность системы [32].

Интерес к интеграции водородных комплексов с АЭС придает новый импульс разработкам в области получения и хранения чистой энергии. Испытания, проводимые на примере Кольской АЭС, демонстрируют высокую перспективность таких технологий, что может стать основой для масштабирования на другие атомные электростанции [26]. Таким

образом, дальнейшее развитие и оптимизация водородных комплексов в синергии с АЭС откроет новые пути обеспечения энергетической безопасности и устойчивости в условиях глобального перехода на чистые технологии.

### **Эффективность сжигания водорода**

Эффективность сжигания водорода зависит от ряда ключевых факторов, включая производственные процессы и технологии его применения. КПД водорода при производстве располагается в диапазоне 60-70%. Так, щелочные электролизеры обеспечивают около 60% эффективности, в то время как PEM-электролизеры могут достигать 70% при оптимальных условиях [11]. Этот уровень производственной эффективности имеет важное значение для оценки окончательной себестоимости зеленого водорода.

Сжигание водорода является одним из самых экологически чистых процессов, так как в результате его реакции с кислородом образуется только водяной пар, без выбросов углекислого газа. Удельная теплота сгорания составляет 140 МДж/кг, что в три раза превышает аналогичное значение для природного газа [21]. Однако объемная теплота сгорания водорода — примерно 10 МДж/м<sup>3</sup> — ограничивает его возможности использования в смешении с природным газом без изменения нормативной базы.

Применение водорода в различных сферах, от автомобильной до энергетической, активно растет. Например, технология водородных двигателей находит свое применение как в легковых машинах, так и в гоночных автомобилях, где компании, такие как BMW, демонстрируют значительные успехи [7]. Эти достижения подчеркивают, что водород не только предполагает будущее транспортной отрасли, но и открывает новые возможности для использования в коммерческих и промышленных энергетических установках.

Однако, чтобы достичь максимальной эффективности сжигания водорода, важно учитывать ряд критически значимых факторов, включая кинетику реакций, методы детонации и установку систем контроля выбросов, таких как оксиды азота (NO<sub>x</sub>). Несмотря на недостатки и текущие ограничения в утверждении нормативных документов для применения водорода в качестве топлива, его перспективы остаются весьма многообещающими. Водородные технологии могут стать важным элементом в стратегии перехода к более устойчивой и безопасной энергетической системе [8].

Совершенствование технологий сжигания водорода в газовых турбинах и двигателях внутреннего сгорания помогает увеличить общую эффективность и снизить воздействие на окружающую среду. Процессы, связанные с контролем выбросов, в том числе оптимизация рабочих параметров, действуют как стимул для дальнейших исследований и разработок в этой области [25]. Эффективное использование водорода в энергетических комплексах может значительно повысить производительность АЭС, обеспечивая таким образом поддержание устойчивого энергетического баланса при избытке электроэнергии.

### **Экономическая целесообразность проекта**

Анализ экономической целесообразности интеграции атомных электростанций (АЭС) с водородными комплексами демонстрирует несколько ключевых аспектов, способствующих успешной реализации данных проектов. В частности, методика оценки технико-экономических показателей, основанная на примере АЭС с реактором ВВЭР-1000, позволяет

установить связи между долей внепиковой мощности, используемой для производства водорода и кислорода, и общими экономическими выгодами от таких инвестиций [12].

При рассмотрении производственной стоимости водорода важно учитывать отпускную цену за электроэнергию. Если эта цена составляет около 70 \$/МВт·ч, а производственная стоимость водорода не превышает 5 \$/кг, то проект может потерять свою экономическую привлекательность [2]. Эффективность интеграции напрямую зависит от состояния сетевых ограничений, а также от существующих возможностей повышения коэффициента использования установленной мощности (КИУМ) АЭС [27].

Некоторые исследования показывают, что комбинирование АЭС с водородными комплексами может привести к повышению эффективности парогенераторов и к использованию сверхноминальной мощности во время пиковых нагрузок за счёт пароводородного перегрева [20]. В данном контексте реализация концепции водородного производства на базе Кольской АЭС, которая выбрана в качестве пилотного проекта, позволит определить дальнейшие стратегии в сфере использования атомной энергетики и возобновляемых источников с учётом растущего спроса на чистую энергию.

Ключевым моментом является умение адаптировать воду, использующуюся в процессах, под различные температуры, что прямо связано с производственной эффективностью [26]. Важно понимать, что только при условии значительного избытка мощностей и повышении цен на электроэнергию создание водородного производства становится оправданным. В условиях постоянного роста устойчивого производства электричества на АЭС шансы на успешную реализацию таких проектов в дальнейшем возрастают.

Следует отметить, что успешная интеграция и эффективность работы водородного комплекса во многом зависят от новых технологий и методов, направленных на снижение производственных затрат и повышение энергетической безопасности. Ожидается, что при помощи таких инициатив можно значительно улучшить общее состояние энергетической системы и сделать её более устойчивой к изменяющимся условиям.

### **Пример Кольской АЭС: реализация концепции**

Кольская АЭС демонстрирует пример успешного внедрения водородных технологий в российскую энергетику. На станции была запущена электролизная установка, которая произвела водород, необходимый для охлаждения турбогенераторов, обеспечивая тем самым эффективное использование избыточной электроэнергии. Система использует новейшие технологии и обеспечивает производство водорода с абсолютно высокой чистотой — 99,999% [19]. Это обеспечивается за счёт системы контроля безопасности, которая следит за работой установки, включая датчики для реакции на превышение установленных параметров [13].

Планируется создание стендового испытываемого комплекса для масштабного производства водорода, реализация которого запланирована на 2025 год. Кольская АЭС была выбрана для этого проекта благодаря наличию необходимой инфраструктуры и избытку электроэнергии, что позволяет не только производить водород, но и разрабатывать новые методы его эффективного применения [5]. Опыт работы с водородом на станции сформировал основу для дальнейших инноваций и расширения этого направления в России [17].

Использование водородных технологий на Кольской АЭС позволяет снизить углеродные выбросы, а также эффективнее управлять созданной электроэнергией. Этот процесс создает мост между атомной энергетикой и водородной экономикой, что открывает новые

возможности для устойчивого развития и обеспечивает выполнению экологических норм [18]. Таким образом, Кольская АЭС становится не только базовой платформой для производства водорода, но и пионером внедрения новых технологий, что способствует улучшению энергетической безопасности региона и страны в целом.

Кроме того, Кольская АЭС рассматривается как ключевой элемент в плане глобальной энергетической трансформации, предлагая не только гармоничное сочетание традиционной и возобновляемой энергетики, но и возможности для ее экспортирования [19]. Опыт, накопленный при использовании водорода, может служить примером для других атомных станций, что подтверждает ее статус пилотной площадки для дальнейшего внедрения подобных технологий [13].

В заключение, водородные технологии на Кольской АЭС не только способствуют более эффективному использованию избыточной мощности, но и создают платформу для будущих разработок в области водородной энергетики, что делает её образцовым объектом в рамках современных энергетических решений [17].

### **Перспективы дальнейшего развития водородной энергетики**

Водородная энергетика в России, согласно принятой в 2021 году Концепции, представляется важным направлением в рамках перехода на устойчивые источники энергии. В украинском контексте значительной является экологическая составляющая, так как водород, сгорая, образует лишь водяные пары, что делает его привлекательным для многих секторов [6]. Одним из ключевых аспектов также является высокая энергетическая плотность водорода, что позволяет использовать его в энергетических системах, транспорта и промышленности.

В последние годы наблюдается устойчивый рост интереса к водороду как источнику энергии, что подтверждается прогнозами международных организаций. Например, согласно МЭА, ожидается, что к 2050 году мировой спрос на водород может достигнуть 528 миллионов тонн, что создаёт новые экспортные возможности для России [24]. Уникальные экологические условия и запасы природного газа, которыми располагает страна, дают ей возможность быть конкурентоспособной на глобальных рынках водорода.

Для достижения успешных результатов России необходимо сосредоточиться на создании инфраструктуры, интегрированной с автомобильной промышленностью и исследовании международного опыта. Применение водорода может варьироваться от использования в качестве топлива для автомобилей до хранения избыточной электроэнергии в энергетических системах, что открывает новые горизонты для его применения [10].

Запуск пилотных проектов и развитие технологий, таких как улавливание углекислого газа и электролиз воды, также имеют большую значимость для расширения потенциала водорода [23]. Важно учесть, что развитие этих технологий может привести к снижению тарифов на «зеленый» водород и сделал бы его более доступным, что будет способствовать его массовому применению.

Наращивание экспортного потенциала к 2024 году до 200 тыс. тонн и до 12 млн тонн к 2035 году обозначает стратегический ориентир для страны [15]. Однако для достижения этих показателей нужно обеспечить активную кооперацию между государственными структурами и частным сектором, что создаст благоприятные условия для внедрения технологий и оптимизации избыточной мощности АЭС.

Таким образом, водородная энергетика, в контексте возможностей использования избыточной мощности АЭС, выглядит многообещающей как для реализации устойчивого энергетического будущего России, так и для ее интеграции в глобальную экономику.

#### **Выводы:**

Проанализировав полученные данные, можем сказать, что интеграция водородных комплексов с атомными электростанциями, в частности на примере Кольской АЭС, представляет собой многообещающий путь к более эффективному использованию избыточной электроэнергии, генерируемой в процессе работы АЭС. Проблема неэффективного использования этой электроэнергии становится все более актуальной в условиях глобального перехода к устойчивым и экологически чистым источникам энергии. Водород, как универсальный энергетический носитель, способен не только решить проблему избыточной генерации, но и стать важным элементом в структуре будущей энергетической системы.

Анализ существующих технологий водородного производства показал, что на сегодняшний день существует несколько подходов, включая электролиз, паровую реформу метана и термохимические циклы. Каждый из этих методов имеет свои преимущества и недостатки, однако именно электролиз, использующий избыточную электроэнергию, представляется наиболее перспективным в контексте интеграции с АЭС. Это позволяет не только производить водород, но и минимизировать потери энергии, что является ключевым аспектом для повышения общей эффективности работы атомных станций.

Разработка схем интеграции водородных комплексов с АЭС, предложенная в рамках данного проекта, открывает новые горизонты для использования атомной энергии. В частности, использование избыточной электроэнергии для подогрева питательной воды в парогенераторах может значительно повысить температуру пара, что, в свою очередь, улучшит эффективность сжигания водорода. Это создает возможность для более рационального использования ресурсов и увеличивает общую производительность АЭС.

Проведенные исследования по эффективности сжигания водорода также подтвердили его высокие энергетические характеристики и низкий уровень выбросов, что делает его идеальным кандидатом для замещения традиционных углеводородных источников энергии. В условиях глобального потепления и необходимости снижения углеродного следа, переход на водородные технологии становится не только целесообразным, но и необходимым.

Экономическая целесообразность проекта интеграции водородных комплексов с Кольской АЭС была оценена с учетом различных факторов, включая затраты на строительство и эксплуатацию, а также потенциальные доходы от продажи водорода. Результаты анализа показали, что проект может быть выгодным как для самой АЭС, так и для региона в целом, способствуя созданию новых рабочих мест и развитию инфраструктуры.

В заключение, перспективы дальнейшего развития водородной энергетики выглядят весьма обнадеживающе. С учетом глобальных трендов на декарбонизацию и переход к устойчивым источникам энергии, интеграция водородных комплексов с атомными электростанциями может стать важным шагом к созданию более устойчивой и эффективной энергетической системы. Кольская АЭС, как пилотный проект, может послужить примером для других атомных станций, стремящихся оптимизировать свои процессы и внести вклад в устойчивое развитие энергетики. Таким образом, работа, проведенная в рамках данного проекта, открывает новые горизонты для исследований и внедрения водородных технологий



в энергетический сектор, что, безусловно, будет способствовать решению актуальных проблем современности.

### Список литературы

1. Выгодно ли производить водород с помощью АЭС? [Электронный ресурс] // tenchat.ru - Режим доступа: <https://tenchat.ru/media/1596170-1-vygodno-li-proizvodit-vodorod-s-promoschu-aes>, свободный. - Загл. с экрана
2. (PDF) Оценка системной эффективности атомно-водородного... [Электронный ресурс] // [www.researchgate.net](http://www.researchgate.net) - Режим доступа: [https://www.researchgate.net/publication/330940325\\_ocenka\\_sistemnoj\\_effektivnosti\\_atomno-vodorodnogo\\_energeticeskogo\\_kompleksa](https://www.researchgate.net/publication/330940325_ocenka_sistemnoj_effektivnosti_atomno-vodorodnogo_energeticeskogo_kompleksa), свободный. - Загл. с экрана
3. «Куда девается "лишняя" электроэнергия...» — Яндекс Кью [Электронный ресурс] // [yandex.ru](http://yandex.ru) - Режим доступа: <https://yandex.ru/q/tech/8612442113/>, свободный. - Загл. с экрана
4. Будущее ядерной энергетики - Затраты - Безопасность... [Электронный ресурс] // [tr-page.yandex.ru](http://tr-page.yandex.ru) - Режим доступа: <https://tr-page.yandex.ru/translate?lang=en-ru&url=https://www.nuclear-power.com/future-of-nuclear-energy-costs-safety-sustainability/>, свободный. - Загл. с экрана
5. В Мурманской области впервые произвели уникальный... [Электронный ресурс] // [murmansk.rbc.ru](http://murmansk.rbc.ru) - Режим доступа: <https://murmansk.rbc.ru/murmansk/27/12/2022/63aaf64e9a79474bacad1943>, свободный. - Загл. с экрана
6. Водородная энергетика 2023: тренды и перспективы рынка... [Электронный ресурс] // [delprof.ru](http://delprof.ru) - Режим доступа: <https://delprof.ru/press-center/open-analytics/vodorodnaya-energetika-2023-trendy-i-perspektivy-rynka-chistoy-energetiki/>, свободный. - Загл. с экрана
7. Водородная энергетика — Википедия [Электронный ресурс] // [ru.wikipedia.org](http://ru.wikipedia.org) - Режим доступа: [https://ru.wikipedia.org/wiki/водородная\\_энергетика](https://ru.wikipedia.org/wiki/водородная_энергетика), свободный. - Загл. с экрана
8. Водородная энергетика: когда наступит будущее? | Кочетов... | Дзен [Электронный ресурс] // [dzen.ru](http://dzen.ru) - Режим доступа: <https://dzen.ru/a/xmz6cu6flt8buyls>, свободный. - Загл. с экрана
9. Водородная энергетика: методы получения водорода | Дзен [Электронный ресурс] // [dzen.ru](http://dzen.ru) - Режим доступа: <https://dzen.ru/a/xnttbefshghgi9f5>, свободный. - Загл. с экрана
10. Оразбердиева Э., Уссаев М., Уссаева А., Мяликулыева О. ВОДОРОДНАЯ ЭНЕРГЕТИКА: ПЕРСПЕКТИВЫ И ВЫЗОВЫ // Символ науки. 2024. №9-1-2. URL: <https://cyberleninka.ru/article/n/vodorodnaya-energetika-perspektivy-i-vyzovy> (25.03.2025).
11. Водородный транспорт — хорошая идея только в теории / Хабр [Электронный ресурс] // [habr.com](http://habr.com) - Режим доступа: <https://habr.com/ru/articles/575836/>, свободный. - Загл. с экрана
12. Диссертация на тему «Эффективность интеграции АЭС...» [Электронный ресурс] // [www.dissercat.com](http://www.dissercat.com) - Режим доступа: <https://www.dissercat.com/content/effektivnost-integratsii-aes-s-vodorodnym-energeticheskim-kompleksom>, свободный. - Загл. с экрана
13. Журналистам [Электронный ресурс] // [www.rosenergoatom.ru](http://www.rosenergoatom.ru) - Режим доступа: <https://www.rosenergoatom.ru/zhurnalistam/news/42683/>, свободный. - Загл. с экрана

14. Как получают водород в промышленности: методы, технологии... [Электронный ресурс] // [www.provita.ru](http://www.provita.ru) - Режим доступа: <https://www.provita.ru/articles/kak-poluchayut-vodorod-v-promyshlennosti-metody-tekhnologii-i-syre/>, свободный. - Загл. с экрана
15. Картинки по запросу "перспективы развития водородной энергетики" [Электронный ресурс] // [yandex.ru](http://yandex.ru) - Режим доступа: [https://yandex.ru/images/search?text=перспективы развития водородной энергетики](https://yandex.ru/images/search?text=перспективы+развития+водородной+энергетики), свободный. - Загл. с экрана
16. Картинки по запросу "технологии производства водорода" [Электронный ресурс] // [yandex.ru](http://yandex.ru) - Режим доступа: [https://yandex.ru/images/search?text=технологии производства водорода](https://yandex.ru/images/search?text=технологии+производства+водорода), свободный. - Загл. с экрана
17. Кольская АЭС планирует производить до 150 т чистого водорода... [Электронный ресурс] // [www.interfax.ru](http://www.interfax.ru) - Режим доступа: <https://www.interfax.ru/russia/939761>, свободный. - Загл. с экрана
18. На Кольской АЭС осваивают производство водорода... [Электронный ресурс] // [murman.tv](http://murman.tv) - Режим доступа: <https://murman.tv/news-n-12453--na-kolskoj-aes-osvaivayut-proizvodstvo-vodoroda-ekologicheskii-chistym-sposobom>, свободный. - Загл. с экрана
19. На Кольской АЭС произвели водород по новейшей российской... [Электронный ресурс] // [neftegaz.ru](http://neftegaz.ru) - Режим доступа: <https://neftegaz.ru/news/nuclear/764334-na-kolskoj-aes-proizveli-vodorod-po-noveyshey-rossiyskoj-tekhnologii/>, свободный. - Загл. с экрана
20. Аминов Р.З., Байрамов А.Н. ОЦЕНКА ЭФФЕКТИВНОСТИ КОМБИНИРОВАНИЯ АЭС С ВОДОРОДНЫМ КОМПЛЕКСОМ В УСЛОВИЯХ БЕЗОПАСНОГО ИСПОЛЬЗОВАНИЯ ВОДОРОДА В ПАРОТУРБИННОМ ЦИКЛЕ // Известия высших учебных заведений. Проблемы энергетики. 2021. №2. URL: <https://cyberleninka.ru/article/n/otsenka-effektivnosti-kombinirovaniya-aes-s-vodorodnym-kompleksom-v-usloviyah-bezopasnogo-ispolzovaniya-vodoroda-v-paroturbinnom> (14.12.2024).
21. Передовые технологии сжигания водорода: возможности и вызовы [Электронный ресурс] // [tr-page.yandex.ru](http://tr-page.yandex.ru) - Режим доступа: <https://tr-page.yandex.ru/translate?lang=en-ru&url=https://www.frontiersin.org/research-topics/64142/advanced-hydrogen-combustion-technology-opportunities-and-challenges/authors>, свободный. - Загл. с экрана
22. Перспективные методы преобразования излишков энергии... [Электронный ресурс] // [ppt-online.org](http://ppt-online.org) - Режим доступа: <https://ppt-online.org/369235>, свободный. - Загл. с экрана
23. Перспективы водородной энергетики — Новости — Институт... [Электронный ресурс] // [issek.hse.ru](http://issek.hse.ru) - Режим доступа: <https://issek.hse.ru/news/840275432.html>, свободный. - Загл. с экрана
24. Перспективы и недостатки водородной энергетики [Электронный ресурс] // [t-j.ru](http://t-j.ru) - Режим доступа: <https://t-j.ru/news/review-vodorod/>, свободный. - Загл. с экрана
25. Почему водородное топливо до сих пор не стало спасением... [Электронный ресурс] // [mobile-review.com](http://mobile-review.com) - Режим доступа: <https://mobile-review.com/all/articles/misc/pochemu-vodorodnoe-toplivo-do-sih-por-ne-stalo-spaseniem-chelovechestva/>, свободный. - Загл. с экрана
26. Применение водородных накопителей в комбинации с атомными... [Электронный ресурс] // [www.c-o-k.ru](http://www.c-o-k.ru) - Режим доступа: <https://www.c-o-k.ru/articles/primenenie-vodorodnyh-nakopiteley-v-kombinacii-s-atomnymi-elektrostanciyami>, свободный. - Загл. с экрана

27. Прогнозная экономическая эффективность комбинирования АЭС... [Электронный ресурс] // [www.isjaee.com](http://www.isjaee.com) - Режим доступа: <https://www.isjaee.com/jour/article/view/1699>, свободный. - Загл. с экрана
28. Производство водорода — Википедия [Электронный ресурс] // [ru.wikipedia.org](http://ru.wikipedia.org) - Режим доступа: [https://ru.wikipedia.org/wiki/производство\\_водорода](https://ru.wikipedia.org/wiki/производство_водорода), свободный. - Загл. с экрана
29. Производство водорода: как получают водородное топливо... [Электронный ресурс] // [electricalschool.info](http://electricalschool.info) - Режим доступа: <https://electricalschool.info/guides/2896-kak-proizvodyat-vodorod.html>, свободный. - Загл. с экрана
30. Разработка и обоснование нового принципа комбинирования АЭС... [Электронный ресурс] // [www.isjaee.com](http://www.isjaee.com) - Режим доступа: <https://www.isjaee.com/jour/article/view/2403>, свободный. - Загл. с экрана
31. Создание системы хранения лишней энергии... - Другое – Кампус [Электронный ресурс] // [kampus.ai](http://kampus.ai) - Режим доступа: <https://kampus.ai/referat/sozдание-sistemy-xraneniia-lisnei-energii-v-vide-ustroistv-dlia-upravleniia-nagruzko-na-atomnyx-stancii-50764/>, свободный. - Загл. с экрана

## References

1. Is it profitable to produce hydrogen using nuclear power plants? [Electronic resource] // [tenchat.ru](http://tenchat.ru) - Access mode: <https://tenchat.ru/media/1596170-1-vygodno-li-proizvodit-vodorod-s-pomoschyu-aes> , free. - Caption from the screen
2. (PDF) Evaluation of the system efficiency of atomic hydrogen... [Electronic resource] // [www.researchgate.net](http://www.researchgate.net) - Access mode: [https://www.researchgate.net/publication/330940325\\_ocenka\\_sistemnoj\\_effektivnosti\\_atomn-o-vodorodnogo\\_energeticeskogo\\_kompleksa](https://www.researchgate.net/publication/330940325_ocenka_sistemnoj_effektivnosti_atomn-o-vodorodnogo_energeticeskogo_kompleksa) , free. - Caption from the screen
3. "Where does the "extra" electricity go..." — Yandex Q [Electronic resource] // [yandex.ru](http://yandex.ru) - Access mode: <https://yandex.ru/q/tech/8612442113/> , free. - Caption from the screen
4. The future of nuclear energy - Costs - Safety... [Electronic resource] // [tr-page.yandex.ru](http://tr-page.yandex.ru) - Access mode: <https://tr-page.yandex.ru/translate?lang=en-ru&url=https://www.nuclear-power.com/future-of-nuclear-energy-costs-safety-sustainability/> , free. - Caption from the screen
5. For the first time, a unique product was produced in the Murmansk region... [Electronic resource] // [murmansk.rbc.ru](http://murmansk.rbc.ru) - Access mode: <https://murmansk.rbc.ru/murmansk/27/12/2022/63aaf64e9a79474bacad1943> , free. - Caption from the screen
6. Hydrogen energy 2023: market trends and prospects... [Electronic resource] // [delprof.ru](http://delprof.ru) - Access mode: <https://delprof.ru/press-center/open-analytics/vodorodnaya-energetika-2023-trendy-i-perspektivy-rynka-chistoy-energetiki/> , free. - Caption from the screen
7. Hydrogen energy — Wikipedia [Electronic resource] // [ru.wikipedia.org](http://ru.wikipedia.org) - Access mode: [https://ru.wikipedia.org/wiki/водородная\\_энергетика](https://ru.wikipedia.org/wiki/водородная_энергетика) , free. - Caption from the screen
8. Hydrogen energy: when will the future come? | Kochetov... | Zen [Electronic resource] // [dzen.ru](http://dzen.ru) - Access mode: <https://dzen.ru/a/xmz6cu6flt8buyls> , free. - Caption from the screen
9. Hydrogen energy: methods of hydrogen production | Zen [Electronic resource] // [dzen.ru](http://dzen.ru) - Access mode: <https://dzen.ru/a/xnttbefshghi9f5> , free. - Caption from the screen

10. Orazberdieva E., Ussaev M., Ussayeva A., Myalikgulyeva O. HYDROGEN ENERGY: PROSPECTS AND CHALLENGES // Symbol of Science. 2024. No. 9-1-2. URL: <https://cyberleninka.ru/article/n/vodorodnaya-energetika-perspektivy-i-vyzovy> (03/25/2025).
11. Hydrogen transport is a good idea only in theory / Habr [Electronic resource] // habr.com - Access mode: <https://habr.com/ru/articles/575836/>, free. - Caption from the screen
12. Dissertation on the topic "Efficiency of NPP integration ..." [Electronic resource] // [www.dissercat.com](http://www.dissercat.com) - Access mode: <https://www.dissercat.com/content/effektivnost-integratsii-aes-s-vodorodnym-energeticheskim-kompleksom>, free. - Caption from the screen
13. Journalists [Electronic resource] // [www.rosenergoatom.ru](http://www.rosenergoatom.ru) - Access mode: <https://www.rosenergoatom.ru/zhurnalistam/news/42683/>, free. - Caption from the screen
14. How hydrogen is produced in industry: methods, technologies... [Electronic resource] // [www.provita.ru](http://www.provita.ru) - Access mode: <https://www.provita.ru/articles/kak-poluchayut-vodorod-v-promyshlennosti-metody-tekhnologii-i-syre/>, free. - Caption from the screen
15. Pictures on request "prospects for the development of hydrogen energy" [Electronic resource] // [yandex.ru](http://yandex.ru) - Access mode: [https://yandex.ru/images/search?text=перспективы development of hydrogen energy](https://yandex.ru/images/search?text=перспективы+development+of+hydrogen+energy), free. - Caption from the screen
16. Pictures on request "hydrogen production technologies" [Electronic resource] // [yandex.ru](http://yandex.ru) - Access mode: [https://yandex.ru/images/search?text=технологии hydrogen production](https://yandex.ru/images/search?text=технологии+hydrogen+production), free. - Caption from the screen
17. The Kola NPP plans to produce up to 150 tons of pure hydrogen... [Electronic resource] // [www.interfax.ru](http://www.interfax.ru) - Access mode: <https://www.interfax.ru/russia/939761>, free. - Caption from the screen
18. Hydrogen production is being mastered at the Kola NPP... [Electronic resource] // [murman.tv](http://murman.tv) - Access mode: <https://murman.tv/news-n-12453--na-kolskoj-aes-osvaivayut-proizvodstvo-vodoroda-ekologicheski-chistym-sposobom>, free. - Caption from the screen
19. The Kola NPP produced hydrogen using the latest Russian technology... [Electronic resource] // [neftegaz.ru](http://neftegaz.ru) - Access mode: <https://neftegaz.ru/news/nuclear/764334-na-kolskoy-aes-proizveli-vodorod-po-noveyshey-rossiyskoy-tekhnologii/>, free. - Caption from the screen
20. Aminov R.Z., Bayramov A.N. EVALUATION OF THE EFFECTIVENESS OF COMBINING NUCLEAR POWER PLANTS WITH A HYDROGEN COMPLEX IN CONDITIONS OF SAFE USE OF HYDROGEN IN A STEAM TURBINE CYCLE // Izvestiya vysshikh uchebnykh zavedeniy. Energy problems. 2021. №2. URL: <https://cyberleninka.ru/article/n/otsenka-effektivnosti-kombinirovaniya-aes-s-vodorodnym-kompleksom-v-usloviyah-bezopasnogo-ispolzovaniya-vodoroda-v-paroturbinnom> (14.12.2024).
21. Advanced hydrogen combustion technologies: opportunities and challenges [Electronic resource] // [tr-page.yandex.ru](http://tr-page.yandex.ru) - Access mode: <https://tr-page.yandex.ru/translate?lang=en-ru&url=https://www.frontiersin.org/research-topics/64142/advanced-hydrogen-combustion-technology-opportunities-and-challenges/authors>, free. - Caption from the screen
22. Promising methods for converting excess energy... [Electronic resource] // [ppt-online.org](http://ppt-online.org) - Access mode: <https://ppt-online.org/369235>, free. - Caption from the screen
23. Prospects of hydrogen energy — News — Institute... [Electronic resource] // [issek.hse.ru](http://issek.hse.ru) - Access mode: <https://issek.hse.ru/news/840275432.html>, free. - Caption from the screen

24. Prospects and disadvantages of hydrogen energy [Electronic resource] // t-j.ru - Access mode: <https://t-j.ru/news/review-vodorod/> , free. - Caption from the screen
  25. Why hydrogen fuel has not yet become a salvation... [Electronic resource] // mobile-review.com - Access mode: <https://mobile-review.com/all/articles/misc/pochemu-vodorodnoe-toplivo-dosih-por-ne-stalo-spaseniem-chelovechestva/> , free. - Caption from the screen
  26. The use of hydrogen storage devices in combination with atomic ones... [Electronic resource] // www.c-o-k.ru - Access mode: <https://www.c-o-k.ru/articles/primenenie-vodorodnyh-nakopiteley-v-kombinacii-s-atomnymi-elektrostantsiyami> , free. - Caption from the screen
  27. Projected economic efficiency of combining nuclear power plants... [Electronic resource] // www.isjaee.com - Access mode: <https://www.isjaee.com/jour/article/view/1699> , free. - Caption from the screen
  28. Hydrogen production — Wikipedia [Electronic resource] // ru.wikipedia.org - Access mode: [https://ru.wikipedia.org/wiki/производство\\_водорода](https://ru.wikipedia.org/wiki/производство_водорода) , free. - Caption from the screen
  29. Hydrogen production: how hydrogen fuel is produced... [Electronic resource] // electricalschool.info - Access mode: <https://electricalschool.info/guides/2896-kak-proizvodyat-vodorod.html> , free. - Caption from the screen
  30. Development and justification of a new principle for combining nuclear power plants... [Electronic resource] // www.isjaee.com - Access mode: <https://www.isjaee.com/jour/article/view/2403> , free. - Caption from the screen
  31. Creation of an excess energy storage system... - Other – Campus [Electronic resource] // kampus.ai - Access mode: <https://kampus.ai/referat/sozdanie-sistemy-xraneniia-lisnei-energii-v-vide-ustroystv-dlia-upravleniia-nagruzkoi-na-atomnykh-stantsiakh-50764/> , free. - Caption from the screen
  32. Специальность 05.14.01 - Энергетические системы и комплексы [Электронный ресурс] // new-disser.ru - Режим доступа: [https://new-disser.ru/\\_avtoreferats/01004652675.pdf](https://new-disser.ru/_avtoreferats/01004652675.pdf), свободный. - Загл. с экрана
-



Международный журнал информационных технологий и  
энергоэффективности

Сайт журнала:

<http://www.openaccessscience.ru/index.php/ijcse/>



УДК 621.311.24: 338.24

## ENERGIEWENDE: ПАРАДОКСЫ НЕМЕЦКОГО ЭНЕРГОПЕРЕХОДА

Капланович Л.А.

ФГАОУ ВО "НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ЯДЕРНЫЙ УНИВЕРСИТЕТ  
"МИФИ", Москва, Россия (115409, город Москва, Каширское ш., д.31), e-mail:  
[kaplanovich21@gmail.com](mailto:kaplanovich21@gmail.com)

В статье проводится комплексный анализ реализации энергетического перехода (Energiewende) в Германии, выявляются ключевые противоречия и парадоксы данного процесса. Исследуется трансформация структуры немецкой электроэнергетики за последние три десятилетия, включая отказ от атомной энергетики, рост доли возобновляемых источников энергии и сохраняющуюся зависимость от угольной генерации. Показано, что несмотря на прогресс в развитии ВИЭ (более 50% в структуре производства электроэнергии к 2023 г.), энергетический переход сопровождается ростом цен на электроэнергию, технологическими ограничениями и институциональными противоречиями. Особое внимание уделено влиянию геополитических факторов, связанных с вынужденным отказом от российских энергоресурсов в 2022 году. Проанализированы перспективы развития международного сотрудничества в области офшорной ветроэнергетики, трансграничной торговли электроэнергией и водородных технологий. На основе результатов исследования сформулированы выводы о необходимости сбалансированного подхода к энергетическому переходу, учитывающего экономические, технологические и социальные факторы.

Ключевые слова: Немецкий энергопереход.

## ENERGIEWENDE: THE PARADOXES OF THE GERMAN ENERGY TRANSITION

Kaplanovich L.A.

"NATIONAL RESEARCH NUCLEAR UNIVERSITY "MEPHI", Moscow, Russia (115409, Moscow,  
Kashirskoye sh., 31 e-mail: [kaplanovich21@gmail.com](mailto:kaplanovich21@gmail.com)

The article provides a comprehensive analysis of the energy transition (Energiewende) implementation in Germany, identifying key contradictions and paradoxes of this process. The study examines the transformation of the German electricity sector structure over the past three decades, including the phase-out of nuclear power, the rise of renewable energy sources, and the persistent reliance on coal-fired generation. Despite progress in renewable energy development (over 50% in electricity generation structure by 2023), the energy transition is accompanied by rising electricity prices, technological constraints, and institutional contradictions. Special attention is given to the impact of geopolitical factors related to the forced abandonment of Russian energy resources in 2022. The prospects for developing international cooperation in offshore wind energy, cross-border electricity trading, and hydrogen technologies are analyzed. Based on the research results, conclusions are formulated about the need for a balanced approach to the energy transition that takes into account economic, technological, and social factors.

Keywords: German energy transition.

### Введение

Немецкая программа Energiewende ("энергетический поворот") представляет собой один из самых амбициозных проектов энергетической трансформации в мире, предполагающий

достижение доли ВИЭ в производстве электроэнергии на уровне 80% к 2030 году, полный отказ от угольной генерации к 2030-м годам и углеродную нейтральность к 2045 году.[1] События 2022 года, связанные с вынужденным отказом от российских энергоресурсов, обострили противоречия этого процесса и выявили системные проблемы немецкой модели энергетического перехода.

### **Современная структура электроэнергетики германии**

К 2023 году немецкая электроэнергетика претерпела радикальную трансформацию. Доля возобновляемых источников энергии превысила 50%, при этом на современные ВИЭ, прежде всего энергию ветра и солнца, приходится около 39% от общего объема производства электроэнергии.[2] Одновременно произошло существенное сокращение угольной генерации с 60% в 1990 году до 27% в 2023 году, а атомная энергетика была практически полностью выведена из эксплуатации к апрелю 2023 года.

По абсолютным объемам производства энергии из ВИЭ Германия занимает третье место в мире, уступая только Китаю и США.<sup>3</sup> В глобальном рейтинге по доле ветровой и солнечной энергии в структуре производства электроэнергии страна также находится на третьем месте с показателем 39,9%, опережая ее лишь Дания (67,4%) и Нидерланды (41,3%).<sup>4</sup>

Географически наблюдается смещение центра энергопроизводства на север страны, обусловленное благоприятными природно-климатическими условиями для ветровой энергетики. Северные федеральные земли, такие как Шлезвиг-Гольштейн и Нижняя Саксония, с их выходом к морю и устойчивыми ветрами, становятся центрами развития ВИЭ, в то время как промышленные центры юга страны испытывают дефицит энергии после закрытия атомных электростанций.[5]

### **Экономические и технологические ограничения**

Несмотря на впечатляющие достижения в развитии возобновляемых источников энергии, энергетический переход в Германии сопровождается серьезными экономическими проблемами. Стоимость электроэнергии в стране стабильно превышает средний уровень Европейского союза на 10-20%.[6] По относительной стоимости электроэнергии, рассчитанной по паритету покупательной способности, Германия занимает третье место в ЕС, уступая только Кипру и Чехии.[7] Значительную часть высокой стоимости составляют налоги и сборы, доля которых достигает 30% в конечной цене для потребителей.[8]

Технологические ограничения современных ВИЭ создают дополнительные вызовы для энергетической системы. Ветровые и солнечные электростанции существенно уступают традиционным источникам по коэффициенту использования установленной мощности: атомные электростанции работают около 7500 часов в год, угольные — около 4500 часов, в то время как ветровые электростанции на море функционируют примерно 3800 часов, на суше — лишь 1800 часов, а солнечные электростанции — около 900 часов в год.<sup>9</sup> Эта нестабильность генерации требует сохранения значительных резервных мощностей, что объясняет сохранение высокой доли угольной генерации несмотря на амбициозные планы декарбонизации.

### **Геополитические последствия**

Вынужденный отказ от российских энергоресурсов в 2022 году потребовал от Германии масштабной перестройки энергетической инфраструктуры. Страна была вынуждена в кратчайшие сроки развивать инфраструктуру для приема сжиженного природного газа, арендовав шесть плавучих регазификационных установок общей мощностью 30 млрд кубометров в год.[10] Одновременно были заключены долгосрочные контракты на поставку СПГ с Катаром объемом 2 млн тонн в год [11] и с Норвегией на поставку 10 млрд кубометров природного газа ежегодно.[12] В результате этих мер Норвегия стала крупнейшим поставщиком природного газа в Германию, обеспечивая 48% всего импорта.[13]

### **Международное сотрудничество**

В условиях энергетического перехода Германия активно развивает международное сотрудничество в сфере возобновляемой энергетики. Особое внимание уделяется совместным проектам в области офшорной ветроэнергетики, включая создание системы искусственных островов North Sea Wind Power Hub на пространстве Доггер-банка,<sup>14</sup> развитие интегрированной сетевой инфраструктуры Baltic Sea Offshore Grid в Балтийском море<sup>15</sup> и строительство энергетического хаба Bornholm Energy Island совместно с Данией стоимостью 5,5 млрд евро с планируемым завершением к 2033 году.<sup>16</sup>

Примечательно, что в результате энергетического перехода Германия трансформируется из традиционного нетто-экспортера в нетто-импортера электроэнергии. В 2024 году импорт электроэнергии из Дании составил 18,16 ТВт·ч, из Франции — 15,98 ТВт·ч, что отражает растущую зависимость от соседних стран для компенсации нестабильности собственных ВИЭ.[17]

Водородные технологии рассматриваются как стратегическое направление будущего развития. Обновленная в 2023 году Национальная водородная стратегия предусматривает увеличение мощности электролизеров до 10 ГВт к 2030 году и постепенный перевод газовых электростанций на использование водорода в период после 2030 года.<sup>18</sup>

### **Перспективы и вызовы**

Дальнейшее развитие немецкой электроэнергетики будет происходить по нескольким ключевым направлениям. Первостепенное значение имеет наращивание мощностей офшорной ветроэнергетики как наиболее эффективного сегмента возобновляемых источников энергии. Параллельно развиваются системы хранения энергии, мощность которых выросла на 50% только за 2024 год,<sup>19</sup> что критически важно для компенсации нестабильности ВИЭ. Модернизация сетевой инфраструктуры, включая реализацию проекта высоковольтной линии Südlink для передачи электроэнергии с севера на юг страны,[20] остается необходимым условием успешной интеграции растущих мощностей ВИЭ.

Однако путь к поставленным целям сопряжен с серьезными вызовами. Экономические ограничения становятся все более очевидными: расходы федерального бюджета на субсидирование ВИЭ могут вырасти с нынешних 15-20 млрд евро до 30 млрд евро к 2030 году.<sup>21</sup> Технологическая незрелость ключевых решений, особенно в области производства и использования "зеленого" водорода, создает неопределенность относительно возможности достижения углеродной нейтральности к 2045 году.[22] Институциональные барьеры и сложные бюрократические процедуры продолжают замедлять реализацию критически важных инфраструктурных проектов.



### **Заключение**

Опыт Германии в реализации энергетического перехода демонстрирует глубокую противоречивость современного подхода к декарбонизации электроэнергетики. Достигнув впечатляющих 50% доли ВИЭ в структуре производства электроэнергии, страна одновременно сохраняет 27% угольной генерации и сталкивается с устойчивым ростом цен для конечных потребителей. Анализ немецкого опыта позволяет сформулировать несколько ключевых выводов.

Прежде всего, необходим более сбалансированный подход, учитывающий не только климатические амбиции, но и экономическую реализуемость поставленных целей. Энергетический переход должен опираться на рыночные механизмы и технологические инновации, а не только на масштабное субсидирование, которое в конечном итоге перекладывает издержки на потребителей и снижает конкурентоспособность экономики. Важность развития инфраструктуры и систем хранения энергии нельзя недооценивать — без них интеграция нестабильных ВИЭ остается проблематичной.

Достижение поставленных Германией целей — 80% ВИЭ к 2030 году и углеродная нейтральность к 2045 году — остается под вопросом из-за технологических и экономических ограничений. Тем не менее, немецкий опыт представляет ценность для других стран, планирующих собственные программы энергетического перехода, демонстрируя как возможности, так и подводные камни масштабной трансформации энергетических систем.

### **Список литературы**

1. Энергетический переход Германии // Федеральное министерство экономики и борьбы с изменением климата. 2024.
2. Доля ветра и солнечной энергии в производстве электроэнергии // Enerdata – Ежегодник мировой энергетической и климатической статистики за 2024 год.
3. Рейтинг стран // Международное агентство по возобновляемым источникам энергии.
4. Доля ветра и солнечной энергии в производстве электроэнергии // Enerdata – Ежегодник мировой энергетической и климатической статистики за 2024 год.
5. Распределение мощности электростанций между отдельными землями в 2019 году // Федеральное министерство здравоохранения и охраны окружающей среды.
6. Статистика цен на электроэнергию // Евростат.
7. Цены на электроэнергию для бытовых потребителей // Евростат.
8. Статистика цен на электроэнергию // Евростат.
9. Jahresvolllaststunden 2021: Gesamte Elektrizitätswirtschaft // BDEW. 2022.
10. Германия рассматривает возможность передачи судов со сжиженным газом в субаренду после споров по контрактам // Bloomberg. 21 марта 2025 г.
11. QatarEnergy и ConocoPhillips подписали контракт на поставку СПГ в Германию // Aljazeera. 29 ноября 2022 г.
12. Немецкая Sefе и норвежская Equinor заключили сделку по поставкам газа на сумму 55 миллиардов долларов // Reuters. 19 декабря 2023 г.
13. Проблемы безопасности в центре внимания, поскольку Норвегия обеспечивает почти половину поставок газа в Германию // Clean Energy Wire. 9 января 2025 года.

14. Программа создания ветроэнергетического хаба в Северном море. URL: <https://northseawindpowerhub.eu/>
15. Хранилище Baltic InterGrid в морской электросети Балтийского моря // Европейская комиссия.
16. Энергетический остров Борнхольм. URL: <https://www.energiobornholm.dk/en>
17. Германия способствует переходу Европы к экологически чистой энергетике с помощью трансграничной торговли // Montel. 16 апреля 2025 г.
18. Национальная стратегия развития // Федеральное министерство труда и охраны окружающей среды.
19. Емкость аккумуляторных батарей в Германии увеличится на 50% в 2024 году – отчет // Clean Energy Wire. 31 января 2025 года.
20. Мера темпа жизни в Нетцаусбау: Начало строительства на Северной-Южной-Штроттрассе // Die Bundesregierung. 27 июля 2023 года.
21. Растущие расходы на субсидии в Германии свидетельствуют о трудностях перехода к "зеленой" экономике // Energy Connects. 30 июля 2024 г.
22. Перспективы энергетических технологий на 2020 год // МЭА. 2020.

## References

1. German Energy Transition // Federal Ministry for Economic Affairs and Climate Action. 2024.
2. Share of wind and solar in electricity production // Enerdata – World Energy & Climate Statistics Yearbook 2024.
3. Country Rankings // International Renewable Energy Agency.
4. Share of wind and solar in electricity production // Enerdata – World Energy & Climate Statistics Yearbook 2024.
5. Distribution of power plant capacity among the individual Länder in 2019 // Bundesministerium für Wirtschaft und Klimaschutz.
6. Electricity price statistics // Eurostat.
7. Electricity prices for household consumers // Eurostat.
8. Electricity price statistics // Eurostat.
9. Jahresvolllaststunden 2021: Gesamte Elektrizitätswirtschaft // BDEW. 2022.
10. Germany Looks to Sublet LNG Ships After Contractual Disputes // Bloomberg. March 21, 2025.
11. QatarEnergy, ConocoPhillips sign LNG deal for Germany // Aljazeera. November 29, 2022.
12. Germany's Sefo, Norway's Equinor strike \$55 billion gas supply deal // Reuters. December 19, 2023.
13. Security concerns in focus as Norway provides almost half of German gas supply // Clean Energy Wire. January 9, 2025.
14. North Sea Wind Power Hub Programme. URL: <https://northseawindpowerhub.eu/>
15. Baltic InterGrid Repository on Baltic Sea offshore electricity grid // European Commission.
16. Energy Island Bornholm. URL: <https://www.energiobornholm.dk/en>
17. Germany powers Europe's clean energy shift via cross-border trading // Montel. April 16, 2025.
18. Die Nationale Wasserstoffstrategie // Bundesministerium für Wirtschaft und Klimaschutz.
19. German battery storage capacity increases 50% in 2024 – report // Clean Energy Wire. January 31, 2025.

20. Mehr Tempo beim Netzausbau: Startschuss für wichtige Nord-Süd-Stromtrasse // Die Bundesregierung. July 27, 2023.
  21. Germany's Ballooning Subsidy Costs Show Challenge of Going Green // Energy Connects. July 30, 2024.
  22. Energy Technology Perspectives 2020 // IEA. 2020.
-



Международный журнал информационных технологий и  
энергоэффективности

Сайт журнала:

<http://www.openaccessscience.ru/index.php/ijcse/>



УДК 621.039.4

## ПРИНЦИПЫ И СЦЕНАРИИ ДВУХКОМПОНЕНТНОЙ ЯДЕРНОЙ ЭНЕРГЕТИКИ

**Мамаев Ю.А.**

ФГАОУ ВО "НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ЯДЕРНЫЙ УНИВЕРСИТЕТ  
"МИФИ", Москва, Россия (115409, город Москва, Каширское ш., д.31), e-mail:  
[yuram2001@mail.ru](mailto:yuram2001@mail.ru)

В статье рассматриваются принципы и сценарии развития двухкомпонентной ядерной энергетики России. Основное внимание уделяется анализу технико-экономических показателей АЭС с различными типами реакторов, включая ВВЭР и промышленные энергокомплексы с быстрыми реакторами. Исследуются вопросы создания замкнутого ядерного топливного цикла и перехода на новую технологическую платформу с доминированием быстрых реакторов естественной безопасности.

Проведен детальный анализ сценариев развития ядерной энергетики до конца XXI века, включая оценку необходимых ресурсов, затрат и интегральных показателей эффективности. Особое внимание уделяется вопросам переработки отработавшего ядерного топлива и оптимизации использования урановых ресурсов.

Ключевые слова: Двухкомпонентная ядерная энергетика, быстрые реакторы, ВВЭР, промышленный энергокомплекс, замкнутый ядерный топливный цикл, технико-экономические показатели, переработка ОЯТ, уран, модернизация, технологическая платформа.

## PRINCIPLES AND SCENARIOS OF TWO-COMPONENT NUCLEAR POWER

**Mamaev Yu.A.**

"NATIONAL RESEARCH NUCLEAR UNIVERSITY "MEPHI", Moscow, Russia (115409, Moscow,  
Kashirskoye sh., 31 e-mail: [yuram2001@mail.ru](mailto:yuram2001@mail.ru)

The article examines the principles and scenarios for the development of two-component nuclear energy in Russia. The main focus is on the analysis of technical and economic indicators of nuclear power plants with various types of reactors, including WWER and industrial power complexes with fast reactors. The issues of creating a closed nuclear fuel cycle and transition to a new technological platform with the dominance of fast reactors with natural safety are explored.

A detailed analysis of scenarios for the development of nuclear energy until the end of the 21st century is carried out, including an assessment of the necessary resources, costs and integral performance indicators. Special attention is paid to the issues of spent nuclear fuel reprocessing and optimization of uranium resource use.

Keywords: Two-component nuclear energy, fast reactors, WWER, industrial power complex, closed nuclear fuel cycle, technical and economic indicators, spent nuclear fuel reprocessing, uranium, modernization, technological platform.

### Введение

На конец 20 века, а именно, в 1990х годах, российскими учеными и специалистами академических институтов было разработано положение, о создании долгосрочной стратегии развития ядерной энергетики. Данная стратегия имеет актуальное значение и на данный этап времени. Что же побудило ученых разработать данное положение в конце прошлого века?

Одной из главных задач было – обеспечение безопасности АЭС. Как следствия, вытекают и следующие задачи, а именно:

- Предотвращение распространения оружейных материалов;
- Понижение стоимости строительства АЭС;
- Стремление к сохранению природного баланса при захоронении ОЯТ (Отработанное ядерное топливо);
- Реализация всего потенциала урановых запасов.

В данной статье мы рассмотрим проблематику экономики двух-компонентной ядерной энергетики России. Изучим выгодно ли это, насколько оно реализуемо, а также, сколько ресурсов и времени для этого необходимо.

Также, рассмотрим основные принципы и возможные сценарии развития двух-компонентной ядерной энергетики в России.

### **Принципы и сценарии двухкомпонентной ядерной энергетики»**

Как уже было сказано в введении, специалистами академических институтов и российскими учеными было разработано положение о создании долгосрочной стратегии развития ядерной энергетики. [1]

Данное положение нашло отражение и на уровне Правительства Российской Федерации в 2000 г. в утвержденной «Стратегии развития атомной энергетики России в первой половине XXI века».

Также, в 2011 г., с утверждением Федеральной целевой программы (ФЦП) «Ядерные энерготехнологии нового поколения» (ЯЭНП), была поставлена ключевая задача отрасли, а именно – разработка и реализация проекта «Прорыв», который смог бы объединить несколько проектов, нацеленных на создание технологий ядерной энергетики на основе быстрых реакторов, способных работать на быстрых нейтронах. А также, создание замкнутого ядерного топливного цикла (ЯТЦ).

Рассмотрим основные принципы двухкомпонентной ядерной энергетики:

- Отказ от теплоносителей на основе перегретой воды, пара или газа под высоким давлением, потенциально способных мобилизовать радиоактивность, накопленную в активной зоне, переход на инертный высококипящий свинцовый теплоноситель;
- Ввод самодостаточных быстрых реакторов, использующих для подпитки практически неограниченные ресурсы отвалного урана, с коэффициентом воспроизводства активной зоны (КВА) на уровне 1, в которых физика активной зоны ориентирована на достижение естественной безопасности, прежде всего благодаря работе равновесном плотном нитридном топливе с минимальным запасом реактивности, предотвращающим реактивностные аварии;
- Замыкание ядерного топливного цикла (ЯТЦ) быстрых реакторов (БР) и ядерной энергетики (ЯЭ) в целом с утилизацией в быстрых реакторах (БР) энергетически ценных продуктов переработки всех видов облученного ядерного топлива, с трансмутацией долгоживущих актинидов, без разделения урана (U) и плутония (Pu), отказ от наработки Pu оружейного качества в бланкете быстрых реакторов (БР), при экспорте в неядерные страны;
- Отказ от химически активных материалов (таких как: графит, цирконий, натрий), связанных с опасностью пожаров и взрывов при взаимодействии с воздухом и водой, сохраняя возможность ограниченного использования реакторов на быстрых

нейтронах на промежуточном этапе отработки технологий замкнутого ядерного топливного цикла;

- Реализация пристанционного ядерного топливного цикла в составе промышленных энергокомплексов (ПЭК) несколькими блоками быстрых реакторов, коротким временем выдержки отработавшего ядерного топлива (ОЯТ) минимальным накоплением ядерных материалов, без дальней транспортировки отработавшего ядерного топлива и ядерных материалов;[2]
- Экономически оправданная постепенная замена традиционных ВВЭР (Водоводяной энергетический реактор) на Быстрые Реакторы естественной безопасности, отказ в конечном итоге от технологии обогащения урана.

Перейдём к сценариям развития двухкомпонентной ядерной энергетики в России. Прежде всего, рассмотрим этапы ее развития по периодам:

1. Становление подсистемы быстрых реакторов и замыкания их ядерного топливного цикла в рамках существующей ядерной энергетики с продолжением развития подсистемы тепловых реакторов до прекращения их ввода;
2. Параллельного функционирования подсистем тепловых реакторов и быстрых реакторов с вводом новых мощностей только на быстрых реакторах;
3. Окончательно становление ядерной энергетики на новой технологической платформе с выводом из эксплуатации тепловых реакторов.

Суммарная продолжительность периодов, представленных выше, оценивается десятками лет.

Т.к. нам следует рассмотреть экономическую составляющую реализации данного проекта, то нам надо знать, с какой точки зрения нам следует её оценивать, например:

- Применительно к решению задач по удовлетворению долгосрочных энергетических потребностей;
- С позиции индивидуальных инвесторов или корпораций в отношении наиболее доходного проекта масштаба отдельно взятой АЭС.

### **Сценарии развития двухкомпонентной ядерной энергетики**

Для анализа возможных сценариев развития российской ядерной энергетики с переходом на двухкомпонентную составляющую, рассмотрен ряд возможных сценариев, с помощью данных ИНЭЙ, масштабы развития ядерной энергетики в целом до 2050 г. с выходом на уровень 70 ГВт, а при максимально возможном и оптимистичном варианте развития событий, к концу века – достижение ~120 ГВт.

Результаты анализа по каждому сценарию включают в себя динамику изменения структуры потребления и производства ядерного топлива коренным образом, а также, баланса продуктов переработки отработавшего ядерного топлива тепловых реакторов и быстрых реакторов потребления природного урана и объемов работы разделения, а также стоимостных показателей, определяющих топливную составляющую и себестоимость вырабатываемой электроэнергии. [3]

Таблица 1. – Техничко-экономические показатели АЭС с ВВЭР и ПЭК с БР

Удельные капитальные вложения	Единицы измерения	Стоимость
ВВЭР-ТОИ	долл./кВт(э)	2800
ПЭК с БР-1200		2300
Срок службы		
РУ ВВЭР-ТОИ, РУ БР-1200	лет	60
Удельные агрегированные эксплуатационные затраты (без топливных)		
АЭС с ВВЭР-ТОИ	долл./кВт (уст. э)	62
ПЭК с БР-1200		61
Стартовая загрузка		
РУ ВВЭР-ТОИ (УОХ, МОКС)	т ТМ	77,0
РУ БР-1200 (СНУП)		61,0
Выгорание		
РУ ВВЭР (ВВЭР-1000 – ВВЭР-ТОИ)	ГВт.сут/т ТМ	40-60
РУ БР-1200		62-115
Кампания (число перегрузок)		
РУ ВВЭР (ВВЭР-1000 – ВВЭР-ТОИ)	Эфф. суток	1200-1350 (3)
РУ БР-1200		1320-2640 (4-8)
Мощность годовой подпитки топливом (при КИУМ = 1)		
РУ ВВЭР (ВВЭР-1000 – ВВЭР-ТОИ)	т/год	27,4-20,6
РУ БР-1200		16,5-8,9

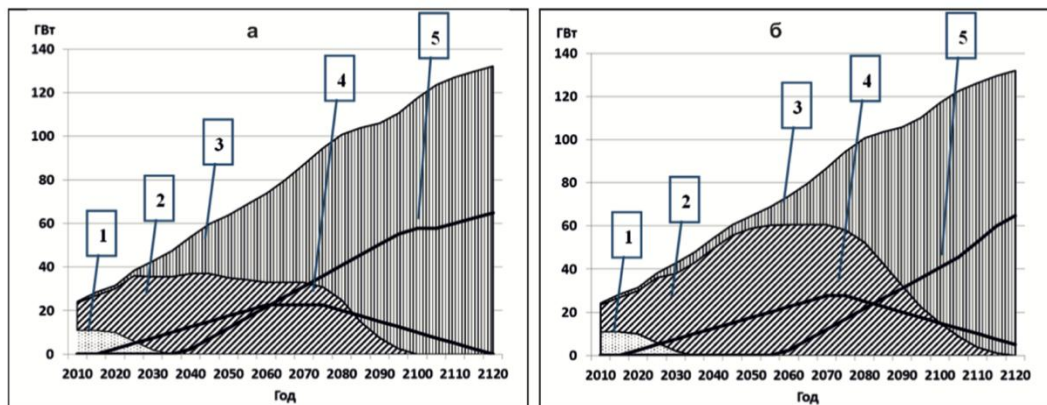
Таблица 2 - Техничко-экономические показатели ЯТЦ (цены 2014 года)

Пристанционный ЯТЦ в составе с ПЭК с БР	Единицы изм.	Стоимость
Удельные капитальные вложения	млн долл./ (т ТМ/год)	~40
Переработка ОЯТ БР + рефабрикация СНУП топлива	топлива млн долл./т ТМ	~6
Хранение ВАО от ОЯТ с выгоранием 7-12%	топлива млн долл./т ТМ	0,058-0,107
Захоронение ВАО от ОЯТ с выгоранием 7-12%	топлива млн долл./т ТМ	0,218-0,403
<b>Централизованный ЯТЦ БР</b>		
Удельные КВЛ, завод изготовления свежего СНУП-топлива, 100т/год	млн долл./ (т ТМ/год)	14,8
Фабрикация свежего СНУП-топлива, 100 т/год	млн долл./ (т ТМ/год)	2,5
Фабрикация свежего UN-топлива БР на действующем заводе масштаба, 1000 т/год	млн долл./ (т ТМ/год)	0,39
<b>Централизованный ЯТЦ ВВЭР</b>		
Исходная стоимость природного урана	долл./кг	100
Стоимость работы разделения, природный уран регенерат из ОЯТ ТР	долл./ЕРР	110 132
Удельные КВЛ, завод изготовления свежего UOX-топлива, 1000 т/год	млн долл./ (т ТМ/год)	1,68
Удельные КВЛ, завод переработки ОЯТ ВВЭР, 1000 т/год	млн долл./ (т ТМ/год)	1,91
Фабрикация свежего UOX-топлива ВВЭР, 1000 т/год	млн долл./т ТМ	0,32
Переработка ОЯТ ВВЭР, 1000 т/год	млн долл./т	0,24
Удельные КВЛ в хранилища ОЯТ: мокрое 6000 т Сухое 9000 т	млн долл./т емкости	0,060 0,044
Хранение ОЯТ во внестанционных хранилищах	млн долл./ (т ИТМ/год)	0,26 (0,008)

Рассмотрим теперь возможные сценарии развития двухкомпонентной ядерной энергетики.



1. Проанализируем сначала со стороны структуры генерирующих мощностей АЭС, которые формируются от двух факторов, а именно: общего масштаба развития и времени прекращения эксплуатации реакторов типа ВВЭР, как проиллюстрировано на Рисунках 1 и 2.

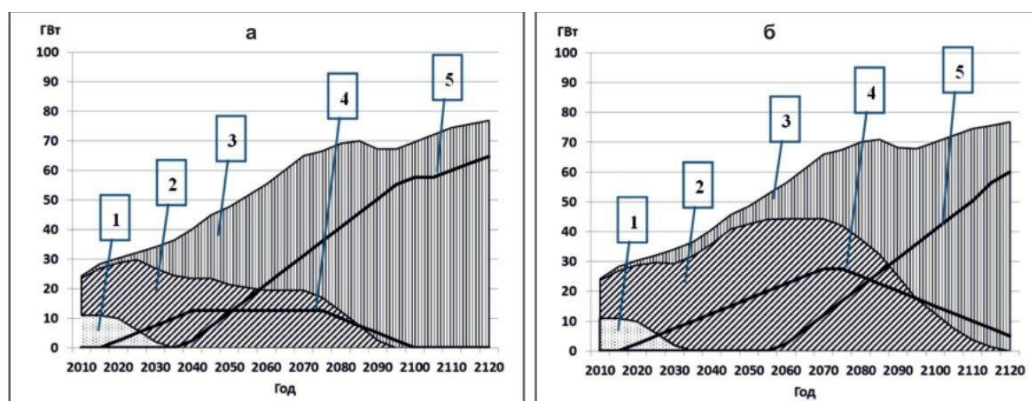


а) ввод ВВЭР до 2040 г.;

б) ввод ВВЭР до 2060 г.;

1 – РБМК; 2 – ВВЭР; 3 – БР; 4 – ВВЭР за рубежом; 5 – БР за рубежом

Рисунок 1 – Установленные мощности АЭС (оптимистичный масштаб развития)



а) ввод ВВЭР до 2035 г.;

б) ввод ВВЭР до 2060 г.;

1 – РБМК; 2 – ВВЭР; 3 – БР; 4 – ВВЭР за рубежом; 5 – БР за рубежом

Рисунок 2 – установленные мощности АЭС (вероятный масштаб развития)

На данных рисунках мы видим результат продолжения использования ВВЭР в задержке перехода ядерной энергетики на новой технологической платформе через двухкомпонентный этап, что отрицательно скажется на ряде ключевых показателей.

2. Если рассматривать со стороны топливного баланса, то развивающаяся система двухкомпонентной ядерной энергетики с замкнутым ядерным топливным циклом определяется следующими показателями:

- Использование продуктов переработки ОЯТ тепловых реакторов для получения, плутоний-содержащего ЯТ БР;
- Использованием СНУП-топлива БР с КВ ~1,05;
- Использованием UOX-топлива тепловых реакторов на основе обогащенного урана для реализации новых блоков;
- Использованием регенерата урана из ОЯТ тепловых реакторов в качестве сырья при разработке СНУП-топлива быстрых реакторов.[4]

3. Рассматривая сценарий со стороны переработки ОЯТ ТР(отработанное ядерное топливо тепловых реакторов) Переработка ОЯТ ТР. Влияние перечисленных факторов зависит, помимо роста генерирующих мощностей, от выбора времени начала массовой переработки, накопленного ОЯТ ТР с ожидаемым вводом завода РТ-2 (вместо либо в дополнение к действующему РТ-1 с относительно небольшой мощностью ~100 т/год). В качестве примера на рис. 3 представлены данные, относящиеся, в рамках оптимистического масштаба развития, к накоплению и переработке ОЯТ ВВЭР при наиболее раннем (2030 г) и наиболее позднем (2060 г.) сроке ввода РТ-2.

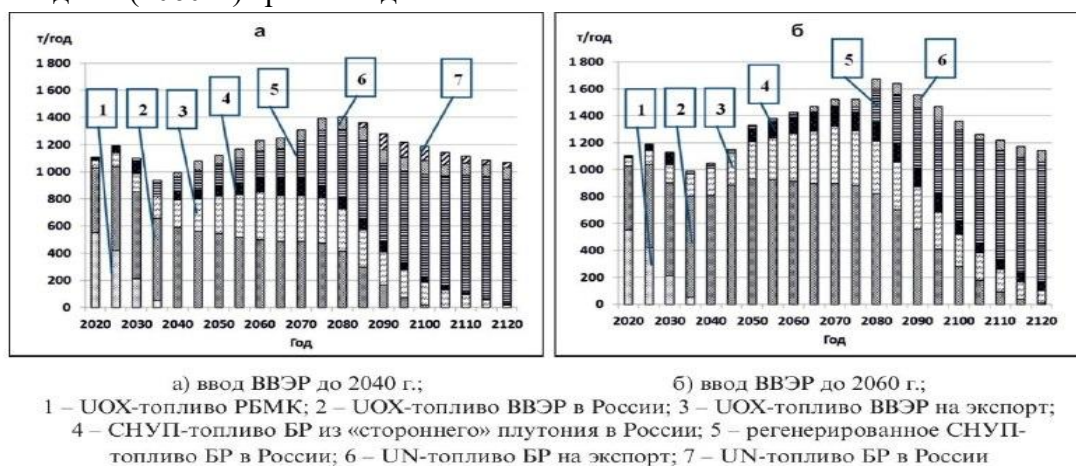
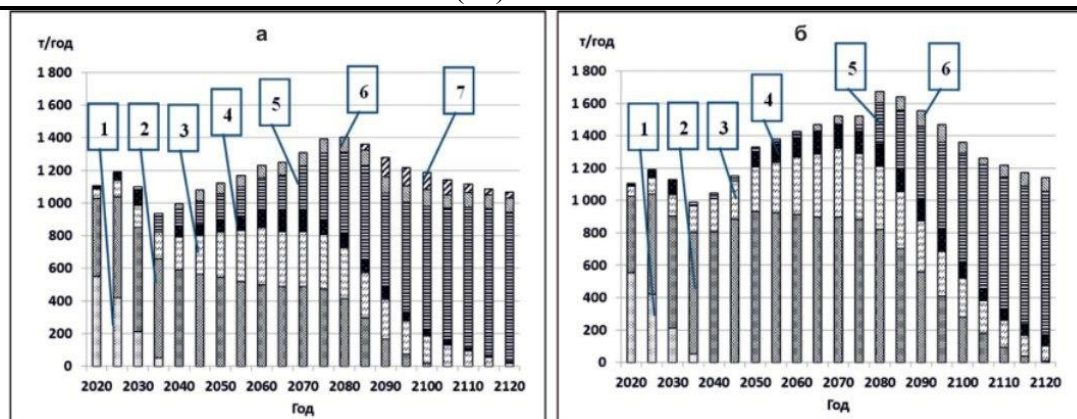


Рисунок 3 – Накопление и переработка ОЯТ ВВЭР (оптимистич. вар.)

Переработка ОЯТ РБМК (Реактор большой мощности канальный), имеющего пониженную по сравнению с ВВЭР (Водо-водяной энергетический реактор) концентрацию плутония (0,5%), рассматривается как дополнительная опция с возможной реализацией во второй половине века,

Сдвиг срока ввода РТ-2 (первая очередь мощностью 800 т/год) на 30 лет приводит к увеличению максимума накопления ОЯТ ВВЭР (с учетом возврата от экспортированных АЭС) в три раза — с 10 до 30 тыс. т, что потребует в районе 2040 г. ввода дополнительного хранилища, которое будет равняться существующему в 15000 т, а также увеличения во второй половине века скорости переработки. При учёте этих факторов утилизация ОЯТ отодвигается на 15 лет.[5]

4. Динамика и структура топливопотребления ЯЭ в целом при замыкании ЯТЦ зависят как от выхода продуктов переработки накопленного ОЯТ ТР, так и от изменения структуры генерирующих мощностей АЭС. Влияние последнего фактора иллюстрируется рис. 4, где показаны полный объем топливопотребления АЭС России с его составляющими, а также поставки топлива для экспортируемых АЭС (но без учета регенерированного топлива экспортированных БР, производимого в пристанционном ЯТЦ).



а) ввод ВВЭР до 2040 г.; б) ввод ВВЭР до 2060 г.;  
 1 – UOX-топливо РБМК; 2 – UOX-топливо ВВЭР в России; 3 – UOX-топливо ВВЭР на экспорт;  
 4 – СНУП-топливо БР из «стороннего» плутония в России; 5 – регенерированное СНУП-топливо БР в России; 6 – UN-топливо БР на экспорт; 7 – UN-топливо БР в России

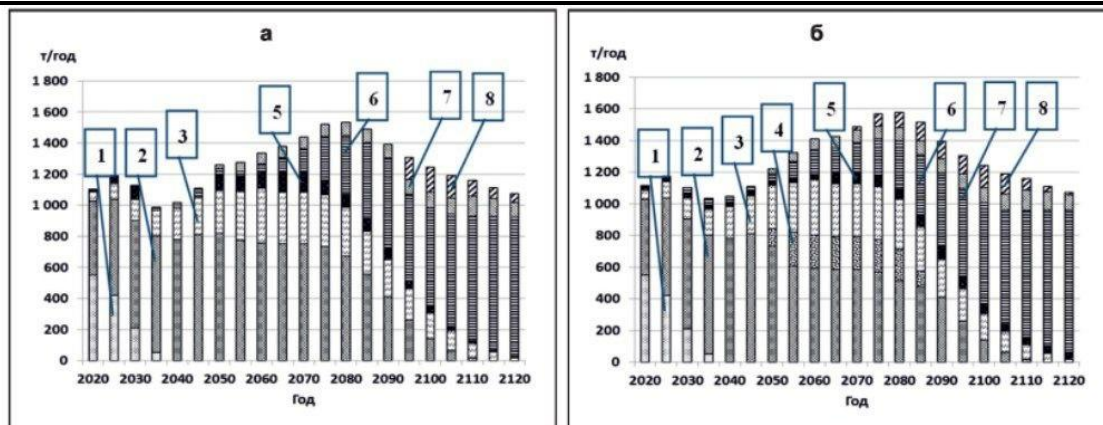
Рисунок 4 – Потребление топлива АЭС (оптимистич. вар)

Сразу следует обратить внимание, что общий объем топливопотребления к концу века оказывается примерно равным современному, хотя суммарная мощность АЭС в приведенном примере оптимистического масштаба развития возрастает в 4 раза (Рисунок 1). Это объясняется отчасти предполагаемым замедлением темпов наращивания мощностей АЭС (с соответствующим уменьшением затрат топлива на первые загрузки вводимых блоков) по завершении развертывания крупномасштабной ЯЭ, но главным фактором здесь является переход ЯЭ на НТП (Новая технологическая платформа) с доминированием БР (Быстрые реакторы), которые потребляют меньше топлива благодаря повышенной средней глубины выгорания.

Эффект от перестройки ЯЭ при продолжении использования ВВЭР (Рисунок 4б) снижается, а общий уровень потребления возрастает (Рисунок 4а).

5. Существует, так же, сценарий с использованием опции МОКС-топлива. Это означает, что при продолжении ввода ВВЭР существует сценарий с расширением их топливного ресурса и использованием МОКС-топлива.

В данном сценарии имеющиеся запасы плутония направляются как раз-таки на создание МОКС-топлива ВВЭР, «вторичный» плутоний из МОКС ОЯТ передается на производство топлива БР, а «улучшенный» плутоний из ОЯТ БР – для нового МОКС-топлива ВВЭР. Динамика и структура топливопотребления в сценариях без и с использованием МОКС-топлива ВВЭР отображены на Рисунке 5.



а) без МОКС-топлива;  
 б) с МОКС-топливом;  
 1 – UOX-топливо РБМК; 2 – UOX-топливо ВВЭР в России; 3 – UOX-топливо ВВЭР на экспорт;  
 4 – МОКС-топливо ВВЭР в России; 5 – СНУП-топливо БР из «стороннего» плутония в России;  
 6 – регенерированное СНУП-топливо БР в России; 7 – UN-топливо БР на экспорт;  
 8 – UN-топливо БР в России

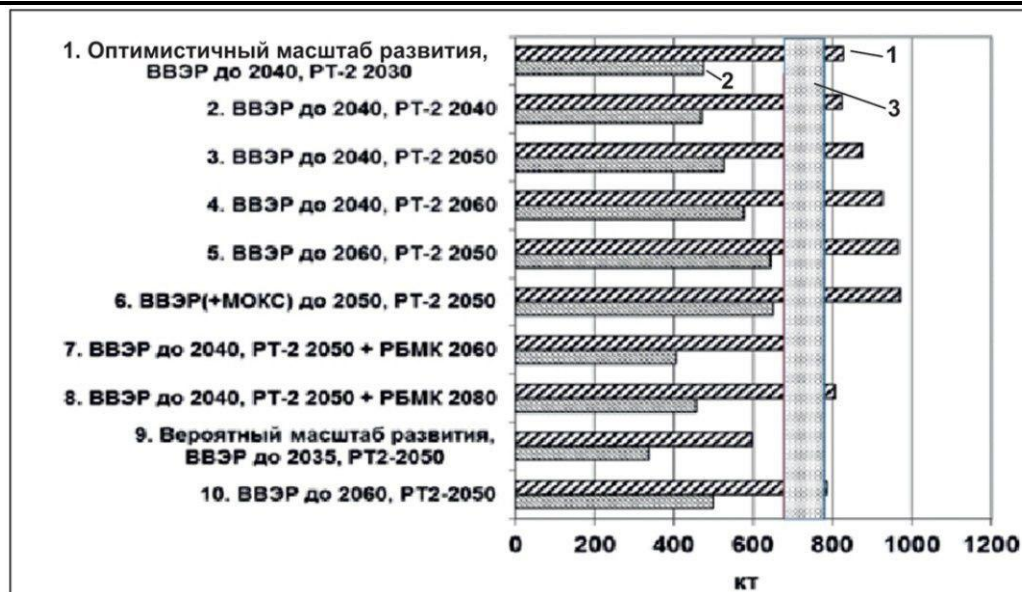
Рисунок 5 – Потребление топлива АЭС без и с МОКС-топливом ВВЭР (оптимист. масштаб развития, ввод ВВЭР до 2050 г.)

При использовании МОКС-топлива потребление топлива ВВЭР несколько возрастает из-за ограничения глубины выгорания, связанного с деградацией изотопного состава при рециклировании (принято 50 ГВт.сут/т против 60 ГВт.сут/т для UOX). Для БР переход на использование плутония из ОЯТ МОКС ВВЭР вместо ОЯТ UOX сокращает ресурс плутония из-за ухудшения его качества после облучения в ВВЭР — концентрация плутония в первой загрузке требуется на 22% больше. Компенсация данного эффекта происходит с помощью увеличения потребления замыкающего уранового топлива (сравнение Рисунки 5а, 5б), что влияет на общий баланс потребления природного урана.

6. Также, существует сценарий интегрального потребления урана.

По внутреннему потреблению урана в России (Рисунок 6) наименее экономными, с интегральным потреблением 630-650 кт, оказываются сценарии с продлением ввода ВВЭР до 2050-60 гг. и с использованием МОКС-топлива. Прекращение ввода ВВЭР после 2040 г. и пуск РТ-2 в это же время с отказом от использования МОКС-топлива ВВЭР позволяют снизить интегральное потребление до 470 кт.





1 – интегральное потребление с учетом экспорта ядерного топлива;  
 2 – в том числе для России; 3 – ограничение по национальным запасам (включая зарубежные активы)

Рисунок 6 – Интегральное потребление урана до конца века.

Интегральное внутреннее потребление урана в России по мере перехода ЯЭ на двухкомпонентный тип близится к концу 21 века к насыщению, в следствие чего, решается проблема ресурсов для национальной ядерной энергетики.

7. Интегральные затраты. На следующем рисунке представим сравнение сценариев по интегральным затратам развития системы ядерной энергетики до конца 21 века.

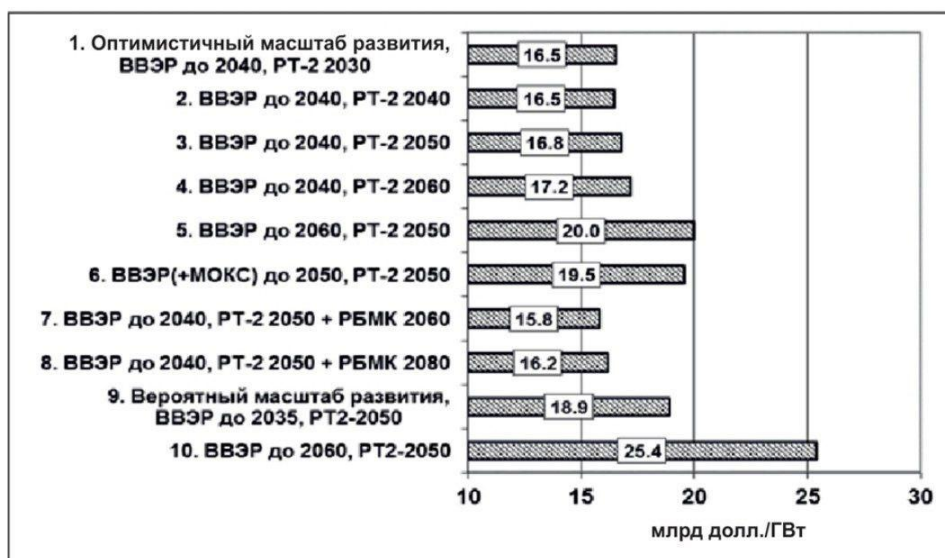


Рисунок 7 – относительные затраты на двухкомпонентную систему ЯЭ в России.

Проанализировав рисунок, мы можем сделать вывод о том, что продолжение ввода ВВЭР неэффективно. Но есть и положительные стороны. Реализация переработки накопленного ОЯТ РБМК может способствовать снижению затрат на развитие двухкомпонентной системы ЯЭ (из-за экономии урана).

8. И рассмотрим ещё один возможный сценарий развития ЯЭ в России – Общесистемный тариф безубыточности (Рисунок 8).

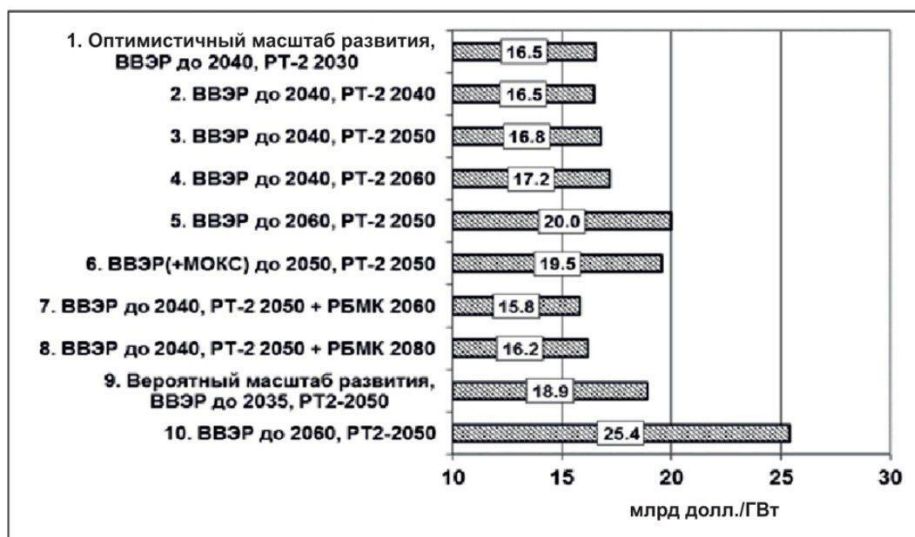


Рисунок 8. – Общесистемный тариф безубыточности (SLCOE).

Общесистемный тариф безубыточности (SLCOE — Рисунок 8) в данном исследовании, при заданном одинаковом для всех сценариев росте генерирующих мощностей, является одновременно и формой выражения приведенных затрат на развитие системы ЯЭ.

По критерию достижения минимальной SLCOE сценарии 5 и 6 с продлением ввода ВВЭР и использованием в них МОКС-топлива выглядят наихудшим образом. В отношении срока пуска завода РТ-2 для массовой переработки ОЯТ ВВЭР можно отметить, что выбор 2030 г. по сценарию 1 не является необходимым, минимум SLCOE приходится на 2040 г. (сценарий 2)

Следует указать также, что снижение SLCOE, относящихся к вероятному масштабу развития, по отношению к аналогичным сценариям 3 и 5 оптимистичного масштаба развития отнюдь не свидетельствует об оптимальности первых. Указанные пары сценариев относятся к решению задач разного масштаба в части удовлетворения потребностей страны в электроэнергии, и каждая из них имеет свою «цену», которая может быть минимизирована.

### Заключение

На основе сценарных системных исследований развития ЯЭ России показано преимущество скорейшего перехода на НТП с доминированием БР естественной безопасности и ЗЯТЦ (проект «Прорыв»), исходя из критериев:

- общей безопасности системы ЯЭ;
- энергобезопасности;
- минимизации абсолютных затрат на единицу мощностей НТП;
- минимизации общесистемного тарифа безубыточности (SLCOE)

При условии подтверждения работоспособности и ожидаемых характеристик головных блоков БР-1200 на рубеже 2030 г. целесообразно прекратить ввод ВВЭР к 2040 году. Топливный баланс замкнутого ЯТЦ следует ориентировать на поступление продуктов массовой переработки ОЯТ ВВЭР не ранее 2040 года.

Концепцию использования МОКС-топлива в реакторах ВВЭР с передачей плутония из ОЯТ МОКС для получения топлива БР необходимо признать неэффективной; выигрыши от использования МОКС- и РЕМИКС-технологий, дающие до 30% экономии урана в однокомпонентной ЯЭ на ТР, в двухкомпонентной ЯЭ с БР теряют свое значение, а главным фактором становится быстрее́шая замена ТР на БР с полным замыканием ЯТЦ. До начала экспорта технологий БР и ЗЯТЦ должна быть определена политика использования национальных ресурсов урана с учетом их ограниченности.

### Список литературы

1. А.Ю. Петров, А.В. Шутиков, Н.Н. Пономарев-Степной, В.С. Беззубцев, М.В. Баканов, В.М. Троянов. Перспективы создания двухкомпонентной ядерной энергетической системы. Известия вузов. Ядерная энергетика, 2019, №2, с.5-15.
2. А.А. Андрианов, И.С. Купцов, Т.А. Осипова, О.Н. Андрианова, Т.В. Утянская. Оптимизационные модели двухкомпонентной ядерной энергетики с тепловыми и быстрыми реакторами в замкнутом ядерном топливном цикле. Известия вузов. Ядерная энергетика, 2018, №3, с.100-112
3. Карелин В.А. Технология переработки облученного ядерного топлива: учебное пособие / В.А. Карелин, А.Н. Страшко; Томский политехнический университет. – Томск: Изд-во Томского политехнического университета, 2018. – 89 с. ISBN 978-5-4387-0822-3
4. Толстоухов Д.А. Конкурентоспособность быстрых реакторов с ЗЯТЦ. Научно-практическая конференция «Проектное направление «ПРОРЫВ». Результаты реализации новой технологической платформы», 2015.
5. Прогноз развития энергетики мира и России 2016. М.: ИНЭИ РАН, Аналитический центр при Правительстве РФ. 2016.

### References

1. A.Yu. Petrov, A.V. Shutikov, N.N. Ponomarev-Stepnoy, V.S. Bezzubtsev, M.V. Bakanov, V.M. Troyanov. Prospects for the creation of a two-component nuclear energy system. Izvestiya vuzov. Nuclear Power Engineering, 2019, No. 2, pp.5-15.
  2. A.A. Andrianov, I.S. Kuptsov, T.A. Osipova, O.N. Andrianova, T.V. Utyanskaya. Optimization models of two-component nuclear power engineering with thermal and fast reactors in a closed nuclear fuel cycle. Izvestiya vuzov. Nuclear Power Engineering, 2018, No. 3, pp.100-111
  3. Karelin V.A. Technology of processing irradiated nuclear fuel: a textbook / V.A. Karelin, A.N. Strashko; Tomsk Polytechnic University. Tomsk: Publishing House of Tomsk Polytechnic University, 2018. 89 p. ISBN 978-5-4387-0822-3
  4. Tolstoukhov D.A. Competitiveness of fast reactors with nuclear fuel. Scientific and practical conference "Project direction "BREAKTHROUGH". The results of the implementation of the new technological platform", 2015.
  5. World and Russian Energy Development Forecast 2016. Moscow: INEI RAS, Analytical Center under the Government of the Russian Federation. 2016.
-



Международный журнал информационных технологий и  
энергоэффективности

Сайт журнала: <http://www.openaccessscience.ru/index.php/ijcse/>



УДК 621.3.049.774

## РАЗРАБОТКА СХЕМЫ СБРОСА ПО ТЕХНОЛОГИИ КМОП 180 НМ

<sup>1</sup> Калёнов А.Д., <sup>2</sup>Сурков А.И.

<sup>1</sup>ФГАОУ ВО "НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ "МОСКОВСКИЙ ИНСТИТУТ ЭЛЕКТРОННОЙ ТЕХНИКИ", Москва, Россия, (124498, город Москва, город Зеленоград, пл. Шокина, д. 1), e-mail: [kalyonov.alex@yandex.ru](mailto:kalyonov.alex@yandex.ru)

<sup>2</sup>ООО «Сенсарт», Москва, Россия (124498, город Москва, город Зеленоград, ул. Юности, д. 8)

В работа представлена разработка схемы сброса при включении питания, выполненный по технологии КМОП с технологической нормой 0,18 мкм. При подаче напряжение питания на интегральную схему (ИС), необходимо сначала инициализировать работу ИС путем первоначального сброса в определенное состояние. Схема сброса при включении питания (POR) с функцией сброса при отключении питания (BOR) выполняет генерацию сброса в соответствии с поведением источника питания.

Ключевые слова. POR, ИС, КМОП.

## DEVELOPMENT OF A POWER ON RESET SCHEME 180 NM CMOS TECHNOLOGY

<sup>1</sup> Kalenov A.D., Surkov A.I.

<sup>1</sup>"NATIONAL RESEARCH UNIVERSITY "MOSCOW INSTITUTE OF ELECTRONIC TECHNOLOGY", Moscow, Russia, (124498, Moscow, Zelenograd, Shokina Square, 1), e-mail: [kalyonov.alex@yandex.ru](mailto:kalyonov.alex@yandex.ru)

<sup>2</sup>Sensart LLC, Moscow, Russia (124365, Moscow, Zelenograd, Yunosti Street, 8)

The paper presents the development of a power-on reset scheme, made using CMOS technology with a technological norm of 0.18 microns. When applying the power supply voltage to the integrated circuit (IC), it is necessary to first initialize the operation and reset it to a certain state. A power-on reset (POR) circuit with a power-off reset (BOR) function generates a reset according to the behavior of the power supply.

Keywords. POR, IC, CMOS.

Существует несколько подходов к реализации схемы сброса, в зависимости от типа и сложности (масштаба) микросхемы. Для простых маломощных устройств требуется элементарная схема с низким энергопотреблением и базовой функцией POR. Микросхемы с источником питания или без него, например, микросхемы радиочастотной идентификации [5], [6], [7]. Современные цифровые микросхемы могут работать при напряжении VSUP ниже 0,5 В, что приводит к подпороговому срабатыванию модуля POR и невозможности реализации опорного напряжения [8].

Для сложных микросхем и SOC, работающих постоянно в течение длительного времени, сбой в работе VSUP являются обычным явлением. Поэтому для дополнительного сброса необходима функция BOR. Сбой в работе связан с постоянным мониторингом VSUP, что приводит к использованию различных схемотехнических решений. Это может быть сделано с



помощью схемы с простым компаратором напряжения, который сравнивает напряжение на резистивный делитель с некоторым опорным напряжением, например, пороговым напряжением МОП-транзистора [1], [2]. Эти простые конструкции имеют недостатки, связанные с резисторами и температурной зависимостью порогового напряжения. Более сложным решением, которое оказывает меньшее влияние на температуру, является датчик уровня напряжения со стабильным опорным напряжением, основанный на задании ширины запрещенной зоны (BOR) [9]. Постоянная активность определяет статическое потребление тока схемой, которым нельзя пренебречь; следовательно, необходим компромисс между энергопотреблением и увеличивается площадь модуля. В случае точного переключения требуется дополнительная регулировка пороговых значений [6].

Уменьшение площади и статического энергопотребления может быть достигнуто несколькими способами. Первый способ заключается в отключении схемы датчика напряжения и физическом разделении цепей POR и BGR, используя технологию накопления заряда в последней [7]. Второй способ заключается в использовании МОП-транзистора в качестве генератора опорного напряжения [4]. Например, для схемы с накопителем заряда [5] предлагается использовать BGR вместо простого датчика напряжения, а после срабатывания POR и до того, как произойдет отключение, отключить питание BGR [8].

Рекомендуемое напряжение питания превышает HSP, и этот уровень напряжения является пороговым для POR. Абсолютный минимальный достаточный уровень VSUP соответствует низкой точке переключения (LSP) и является пороговым напряжением для BOR. Для обеспечения надежной работы HSP и LSP имеют гистерезис напряжения (HYST) между собой.

Длительность импульса POR выражается во времени задержки сброса при включении питания. Кроме того, существует эффект задержки распространения VSUP для больших и сложных микросхем [систем на кристалле (SOC)] в случае быстрого повышения напряжения питания (короткого замыкания). Сигнал сброса RST может быть сгенерирован до того, как будет достигнут требуемый уровень VSUP для всех внутренних модулей микросхемы. Эта особенность требует определенной длительности импульса POR (или задержки RST) после того, как значение VSUP превысит HSP. На Рисунке 1 представлен принцип работы POR и BOR.

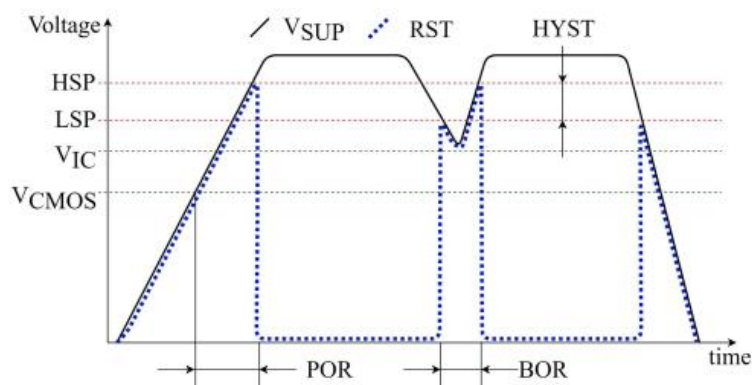
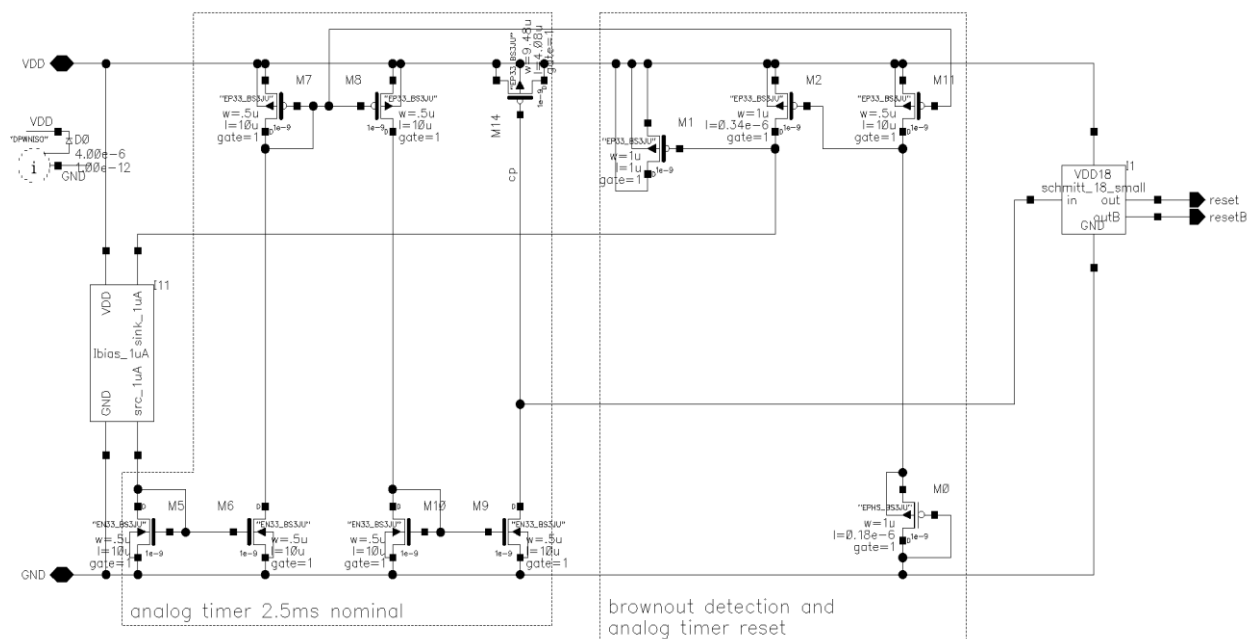


Рисунок 1 – Принцип работы POR и BOR

RST генерирует сигнал следующим образом. Сначала детектор напряжения генерирует сигнал RST\_A, в зависимости от того, пересекает ли VSUP HSP или LSP. Затем первый блок

задержки генерирует асимметричную задержку (в зависимости от повышения/понижения напряжения).

На Рисунке 2 показан блок детектора напряжения модуля POR (генератор RST\_A). Используется базовая концепция детектирующих схем и компаратора с дополнительным генератором смещения [9].



Поэтому введен дополнительный блок с возможностью фильтрации быстрых событий RST\_A. Функция дополнительного блока генерирует соответствующий сигнал. Сигнал RST основан на входном сигнале RST\_A в соответствии с требованиями к синхронизации всего проекта. Эта функция была реализуется с помощью блока задержки основанном на триггере Шмидта представленная на Рисунке 4.

Большая длительность первого импульса в сочетании с требованиями к стабильности, связанными со временем нарастания импульса VSUP, диктуют необходимость использования блока задержки, основанного на источнике слабого тока.

Из-за упомянутой выше задержки между запуском источника тока и быстрым увеличением или восстановлением VSUP после аварийных сбоев была введена дополнительная задержка примерно на 5 мкс. Эта задержка была создана текущим блоком.

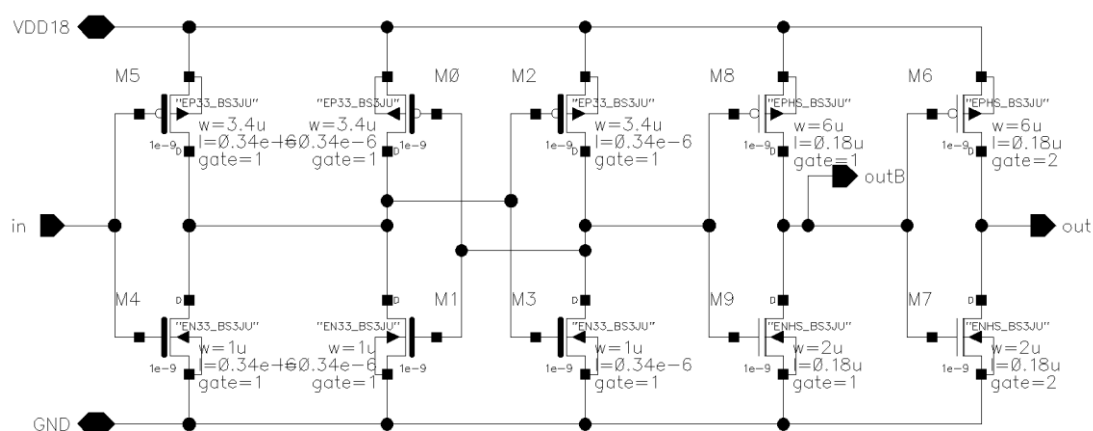


Рисунок 4 – Электрическая схема триггера Шмидта

Данная схема позволяет получить гистерезис и выронить времена фронта и среза сигнала сброса. Гистерезис получен на основе бистабильной ячейки двух инверторов. Далее инверторы выравнивают время фронта сигнала сброса.

Энергопотребление схемы сброса в режиме покоя полностью определяется датчиком напряжения и схемой смещения. Энергопотребление блока задержки в режиме покоя равно нулю. Динамическое потребление определяется переключением инверторов, буферов и триггеров (пиковое значение ниже 300 мкА), а также ячейки задержки переключения в блоке задержки <5 мкА среднего тока во время первой задержки.

При скорости нарастания/спада VSUP в 10 мс (медленный режим) и граничных напряжениях питания 1,6 и 2 В схема сброса демонстрирует постоянство своих параметров, а именно: постоянное напряжение HSP 1,5 В, напряжение LSP 1,4 В и длительность первого импульса 0,4 мс. Зависимости от VSUP нет.

Схема сброса POR разработана с использованием технологии КМОП HCMOS8D 180нм. На Рисунке 5 показана топологическая схема сброса с блоком задержки. Размеры схемы сброса 45 мкм×70 мкм.

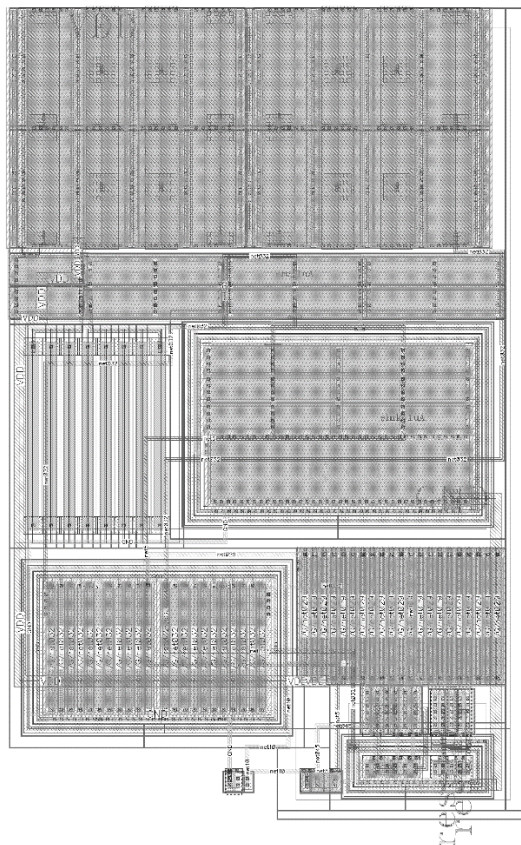


Рисунок 5 – Топологическое представление схемы сброса POR

#### Основные технические характеристики схемы сброса

Значения электрических параметров схемы сброса при приемке (поставке), эксплуатации (в течение наработки) и хранении (в течение срока сохраняемости) в режимах и условиях, установленных настоящими техническими требованиями, должны соответствовать нормам, приведенным в Таблице 1.

В таблице 1 приведены электрические параметры разрабатываемой схемы сброса.

Таблица 1 – Электрические параметры при приемке и поставке схемы сброса

Параметр	Описание	Значение			Температура окружающей среды, °C
		Мин	Макс	Ед.изм	
HSP	Верхняя граница переключения напряжения	1,45	1,55	В	25 ± 10, –60, 85
LSP	Нижняя граница переключения напряжения	1,35	1,45	В	
HYST	Гистерезис напряжения	100	200	мВ	
T	Время сброса	2.4	2.6	мс	
I	Ток потребления схемы сброса	1,5	3,5	мА	

Напряжение питания для приемника и передатчика 1.8В ±5%.

Результат моделирования во временной области схемы сброса, спроектированного на отечественной технологии КМОП HCMOS8D 180нм показан на Рисунке 6.

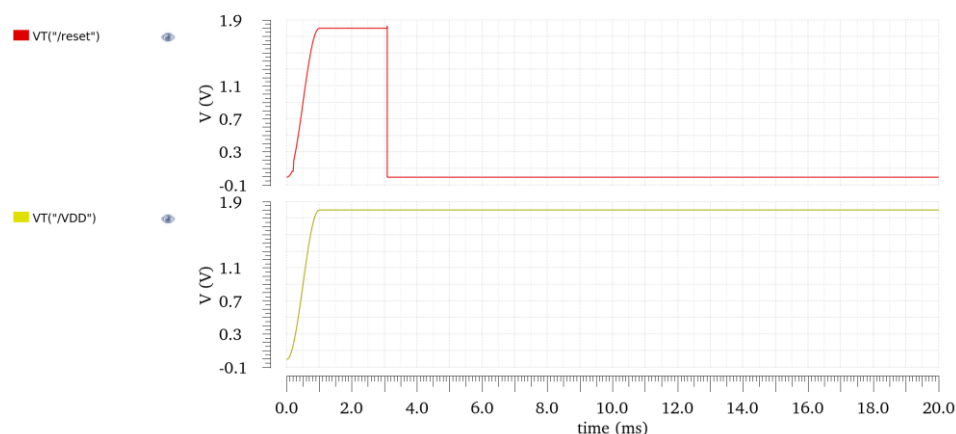


Рисунок 6 – Результаты моделирования схемы сброса

*Исследования и разработки выполнены в рамках соглашения с Минобрнауки №075-03-2025-266 от 16.01.2025г. FSMR-2023-0002.*

*Research and development were carried out within the framework of the agreement with the Ministry of Education and Science No075-03-2025-266 dated 01/16/2025. FSMR-2023-0002.*

### Список литературы

1. Б. Чжоу, Ю. Чжан, З. Лю и Д. Лю, “Надежная схема сброса при включении питания с обнаружением отключения”, J. Beijing Inst. Технология, том 23, № 1, С. 53-57, 2014.
2. Б. Чжоу, С. Лю и П. Чيانг, “Гибридная схема с опорной шириной запрещенной зоны 0,55 В и 2,5 мкВт низкой сложности и сбросом напряжения при включении”, Электрон. Литература, том 52, № 5, с. 346-348, март 2016 г., doi: 10.1049/EL.2015.2637.
3. Г. Хилбер, Д. Грубер, М. Сэмс и Т. Остерманн, “Калибровка гибкого высокоточного сброса при включении питания во время производственных испытаний”, в Proc. IEEE Int. Тестовая конференция, ноябрь 2012 г., С. 1-7.

4. С. К. Вадхва, Г. К. Сиддхартха и А. Гаурав, “Схема включения питания с нулевым постоянным током при включении и сбросе с детектором отключения”, в 19-й главе. Конф. VLSI Design Совместно провели 5-ю международную конференцию Conf. Встраиваемая система. Дизайн (VLSID), 2006, 6 с.
5. А. Диегез, А. Арбат, А. Сануй, Р. Казанова, М. Россиньоль и Ж. Самитье, “Схема пробуждения с тактовой частотой с температурной компенсацией в КМОП-технологии 1,2 В-0,13 мкм”, в 14-м выпуске IEEE Int. Конф. Электрон., Circuits System, декабрь 2007, С. 367-370.
6. У. Шан, Х. Ванг, Х. Лю и Х. Сун, “Схема включения-сброса при сверхнизком постоянном токе в 65-нм КМОП-технологии”, Chin. J. Electron, том 23, № 4, С. 678-681, октябрь 2014 г.
7. Р. Се, К. Чжао, Ю. Ма, Ф. Се, Ф. Лин и С. Чжан, “Схема сброса при включении питания с точно срабатывающими пороговыми напряжениями”, в Proc. Int. Conf. Твердотельные схемы электронных устройств (EDSSC), октябрь 2017 г., С. 1-2.
8. Дж. Чжан, Л. Цзян и З. Цзэн, “Разработка новой схемы сброса питания при включении на основе детектора источника питания”, в 8-м выпуске. Вступ. ст. Сост., внутр. Конф. Масштабируемые вычисления. Коммуна, 2009, С. 355-359.
9. Разави Б., "Проблемы при проектировании высокоскоростных схем синхронизации и восстановления данных", журнал IEEE Communications, том 40, № 8, С. 94-101, август 2002 г.

## References

1. B. Zhou, Y. Zhang, Z. Liu, and D. Liu, “Robust power-on reset circuit with brown-out detection,” J. Beijing Inst. Technol., vol. 23, no. 1, pp. 53–57, 2014.
2. B. Zhou, S. Liu, and P. Chiang, “Low-complexity 0.55-V 2.5-μW bandgap reference and power-on reset hybrid circuit,” Electron. Lett., vol. 52, no. 5, pp. 346–348, Mar. 2016, doi: 10.1049/EL.2015.2637.
3. G. Hilber, D. Gruber, M. Sams, and T. Ostermann, “Calibration of a flexible high precision power-on reset during production test,” in Proc. IEEE Int. Test Conf., Nov. 2012, pp. 1–7.
4. S. K. Wadhwa, G. K. Siddhartha, and A. Gaurav, “Zero steady state current power-on-reset circuit with brown-out detector,” in Proc. 19th Int. Conf. VLSI Design Held Jointly 5th Int. Conf. Embedded Syst. Design (VLSID), 2006, p. 6.
5. A. Dieguez, A. Arbat, A. Sanuy, R. Casanova, M. Rossinyol, and J. Samitier, “A wake-up circuit with temperature compensated clock in 1.2 V-0.13 μm CMOS technology,” in Proc. 14th IEEE Int. Conf. Electron., Circuits Syst., Dec. 2007, pp. 367–370.
6. W. Shan, X. Wang, X. Liu, and H. Sun, “An ultra low steady-state current power-on-reset circuit in 65 nm CMOS technology,” Chin. J. Electron., vol. 23, no. 4, pp. 678–681, Oct. 2014.
7. R. Xie, Q. Zhao, Y. Ma, F. Xie, F. Lin, and S. Zhang, “A power-on-reset circuit with precisely triggered threshold voltages,” in Proc. Int. Conf. Electron Devices Solid-State Circuits (EDSSC), Oct. 2017, pp. 1–2.
8. J. Zhang, L. Jiang, and Z. Zeng, “Design of a novel power-on-reset circuit based on power supply detector,” in Proc. 8th Int. Conf. Emb. Comp., Int. Conf. Scalable Comput. Commun., 2009, pp. 355–359.

9. Razavi B., "Challenges in the design high-speed clock and data recovery circuits," IEEE Communications Magazine, vol.40, no.8, pp. 94-101, Aug. 2002.
-



Международный журнал информационных технологий и энергоэффективности

Сайт журнала:

<http://www.openaccessscience.ru/index.php/ijcse/>



УДК 629.127: 627.36

## **ПРОБЛЕМЫ КОММУТАЦИИ И ПРОЕКТИРОВАНИЯ СИСТЕМЫ УПРАВЛЕНИЯ ПОГРУЖНЫМ ПОДВОДНЫМ МОБИЛЬНЫМ РОБОТОМ, КОНФИГУРАЦИЯ АДАПТИВНОГО УПРАВЛЕНИЯ ПОД ЗАДАЧИ ИНСПЕКЦИИ ТРУДНОДОСТУПНЫХ ПОДВОДНЫХ РАЙОНОВ**

**Пасечник В.С.**

*ФГАОУ ВО "МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ "СТАНКИН", Москва, Россия (127055, город Москва, Вадковский пер., д.3а), e-mail: pasechnik-v@list.ru*

В статье анализируются ключевые проблемы проектирования и построения схемы коммутации исполнительных механизмов подводного мобильного робота. Основное внимание уделяется вопросам формирования адаптивной структуры системы управления, обеспечивающей устойчивую работу в условиях изменяющейся подводной среды.

Представлены основные подходы к реализации модулей распределённого управления, кратко описаны типовые трудности реализации аппаратных решений для адаптивных алгоритмов в реальной конструкции робота. Описан выбор интегрируемых модулей, плат и датчиков. Дано краткое описание решений, встречающихся в современной научной литературе, и указаны примеры реализации таких систем в существующих прототипах.

В выводах к статье приводится краткий анализ ожидаемой эффективности и надёжности предлагаемых технических решений.

Ключевые слова: Погружные роботы, адаптивное управление, разработка прототипа, альтернативные подходы, системы компьютерного анализа, САПР, CAE, CAM.

## **CHALLENGES OF CONTROL SYSTEM DESIGN AND SWITCHING FOR AN UNDERWATER MOBILE SUBMERSIBLE ROBOT: ADAPTIVE CONTROL CONFIGURATION FOR INSPECTION OF HARD-TO-REACH SUBAQUATIC AREAS**

**Pasechnik V.S.**

*MOSCOW STATE TECHNOLOGICAL UNIVERSITY "STANKIN", Moscow, Russia (127055, Moscow, Vadkovsky per., 3a), e-mail: pasechnik-v@list.ru*

The article analyzes the key challenges in designing and constructing the commutation scheme for the actuators of an underwater mobile robot. Particular attention is given to the development of an adaptive control system architecture that ensures stable operation in a dynamically changing underwater environment.

The main approaches to implementing distributed control modules are presented, along with a brief overview of typical hardware implementation difficulties for adaptive algorithms in a real robotic system. The selection of integrated modules, boards, and sensors is also described.

A concise review of existing solutions found in current scientific literature is provided, along with examples of their implementation in existing prototypes.

The conclusion of the article includes a brief analysis of the expected efficiency and reliability of the proposed technical solutions.

Keywords: submersible robots, adaptive control, prototype development, alternative approaches, computer analysis systems, CAD, CAE, CAM.



**Проблемы коммутации и проектирования системы управления погружным подводным мобильным роботом, конфигурация адаптивного управления под задачи инспекции труднодоступных подводных районов.**

**1. Проектирование системы управления.**

В процессе изучения современного состояния российского и международного рынков подводных дронов и автономных погружных систем были выявлены целые сегменты, остающиеся в тени научного внимания, а также ряд технических барьеров, тормозящих развитие отрасли. Подавляющее большинство существующих моделей работают с кабельным подключением длиной от 50 до 200 метров, что влечёт за собой ряд серьёзных ограничений:

1. Невозможность эксплуатации в узких каналах подводных инфраструктур, среди густой водной растительности, в зонах с плотной застройкой балками и опорами, а также в сложных рельефах, таких как подводные каньоны и рифы, где кабель ограничивает манёвренность; [3, с. 7]

2. Работа в режиме нейтральной плавучести, что исключает транспортировку дополнительного оборудования или грузов, включая спасательные средства и дистанционно управляемые устройства;

3. Отсутствие эффективной системы стабилизации и защиты от течений, способных сносить аппарат с курса.

Появление мобильных подводных роботов и погружных платформ является ответом на потребности в эффективной работе в сложных и переменчивых условиях — от морских и озёрных исследований до спасательных операций, инженерных задач, обслуживания флота и морского картографирования. Внедрение инноваций в области ИИ, биоинспирированных решений и энергоэффективных систем открывает новые горизонты для создания высокофункциональных роботов следующего поколения. [1, с. 16]

В ходе исследования были выявлены такие проблемы: проблема передачи данных в толще воды, сложность перехода между средами; ограниченность энергопотребления и автономность; ограниченность сенсоров и трудности в позиционировании и управлении; а также недерменированность среды. Была разработана первичная блок-схема функционирования комплекса (Рисунок 1).

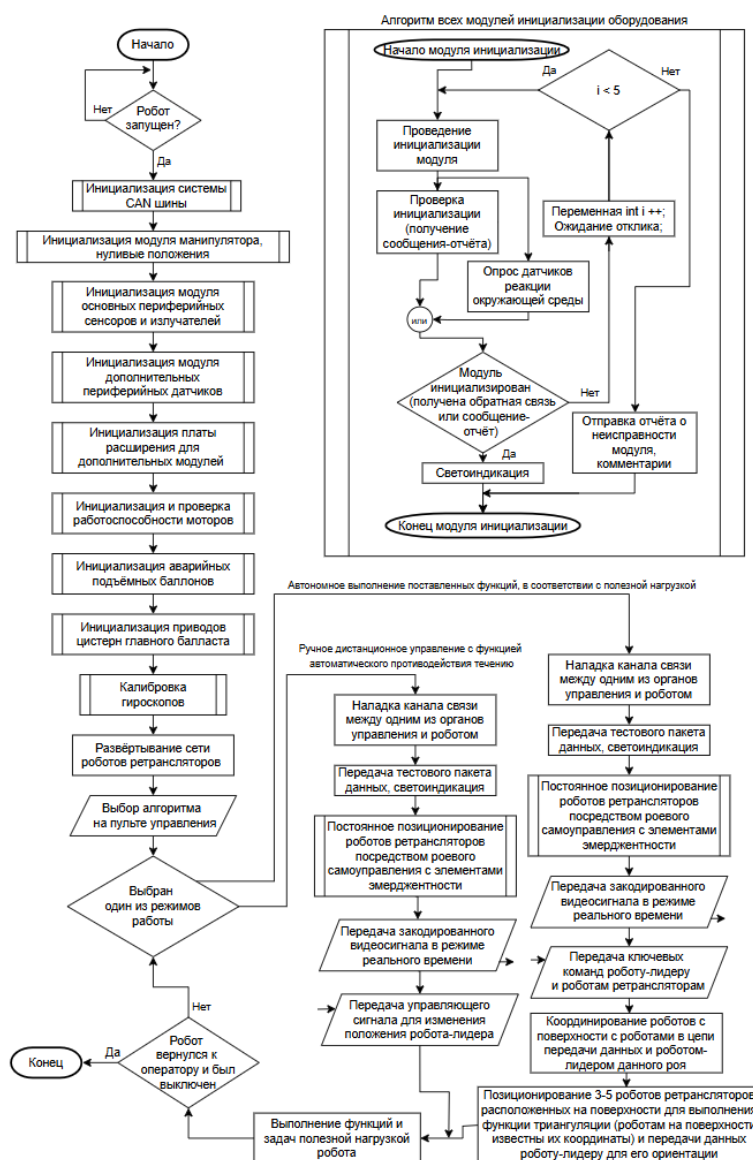


Рисунок 1 - Первичная блок-схема функционирования комплекса

В ходе анализа были выявлены перспективные инженерные решения, научные разработки и концептуальные модели, созданные исследовательскими группами и авторитетными научными учреждениями. Одним из ключевых вызовов при проектировании подобных роботов является обеспечение стабильного перехода между подводной и надводной средами. Наиболее сложной и до конца не решённой задачей остаётся точное позиционирование под водой. Эта проблема требует либо значительных вычислительных ресурсов, что малореализуемо для автономных систем, либо применения нестандартных методов управления. Среди них — использование картографирования в связке с системой гидролокаторов и тросовых буёв, которые периодически поднимаются на поверхность для GPS-корректировки построенной модели дна. [2, с. 44]

## 2. Этапы выполнения работы с иллюстрациями.

### 2.1 Коммутация в корпус

Проектирование нового корпуса робота велось с учётом интеграции всех ключевых компонентов — сенсорных систем, приводов, функциональных модулей и подсистем, — на основе предварительных инженерных расчётов. В процессе использовались инструменты: Компас-Чертежи и Компас-3D для разработки КД, Fusion360 и Blender для создания фотореалистичных моделей и анимации, а также SolidWorks Simulation и Компас-CAE (APM FEM) для анализа прочности и оценки гидроаэродинамических характеристик. Важной частью этапа компоновки было проектирование внутренней архитектуры, включая размещение кабельных каналов, шин и элементов гидроизоляции, с последующим изготовлением полноразмерного прототипа методом 3D-печати. (Рисунок 1)

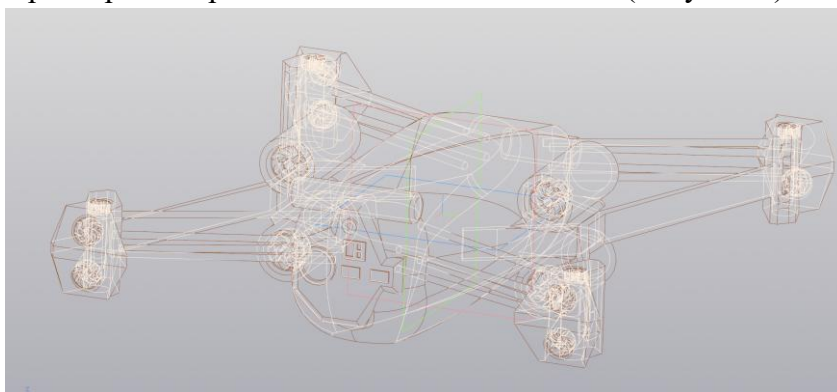


Рисунок 2 - Изометрический вид робота (прозрачность текстур)

Для снижения гидростатических нагрузок при проектировании первой функциональной модели корпуса робота были использованы CAE-системы, исключены герметичные полости (кроме модулей плавучести), а корпус преднамеренно выполнен негерметичным, что позволило уменьшить давление на него в 2,25 раза. [6, с. 24]

Ниже приведены этапы расчёта в CAE-модуле САПР Компас-3D, где сначала геометрия детали дискретизируется на тетраэдрические конечные элементы, после чего проводится анализ нагрузок, действующих на корпус. (Рисунок 3 и 4) [9, с. 41]

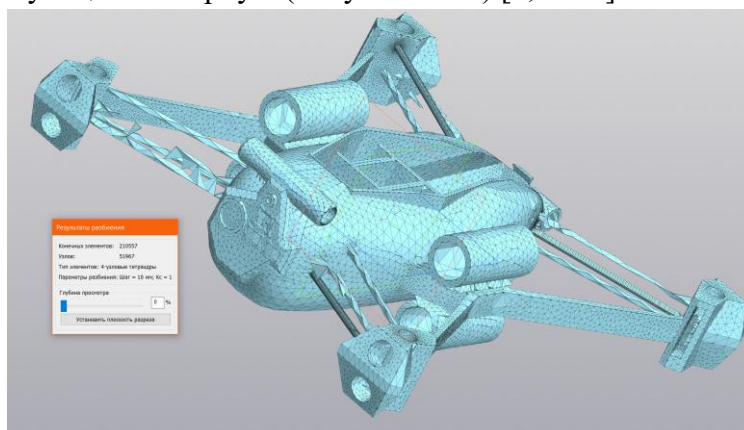


Рисунок 3 – Деталь, разбитая на конечные элементы

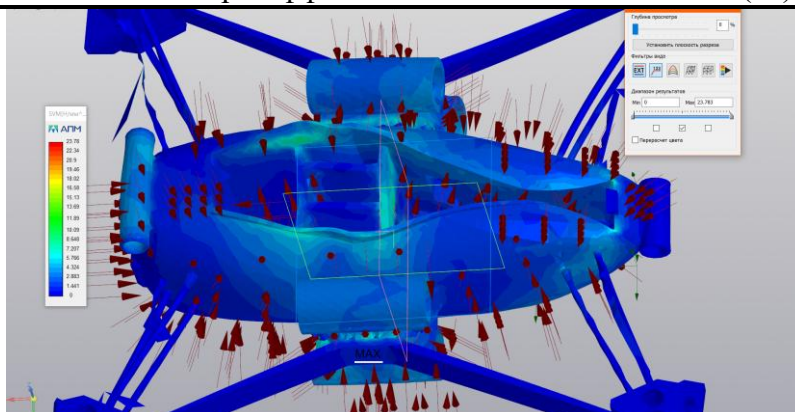


Рисунок 4 – Карта результатов в виде эпюры напряжённости.

## 2.2 Сопутствующие расчёты для выбора комплектующих, и расчёта корпуса.

Для определения нагрузок, направленных в глубь корпуса и прикладываемых к его поверхностям – можем принять глубину испытания робота на отметке в 100 метров. Тогда рассчитаем согласно выражению  $P = \rho_0 * g * h = 1030 * 9,8 * 100 = 10094 * 100 = 1009400 \text{ Па}$ . Тогда в пересчёте на  $\text{Н/мм}^2$  – это будет 1.0094 МПа. [11, с. 61]

2.3 Новый алгоритм управления. (Создание внутренней модели в Windows – Unity (симуляция для отработки всех модулей без работы в режиме реального времени), и иная, на основе Linux и языка ROS2, к момента полноценной отладки прототипа) (Рисунок 5)

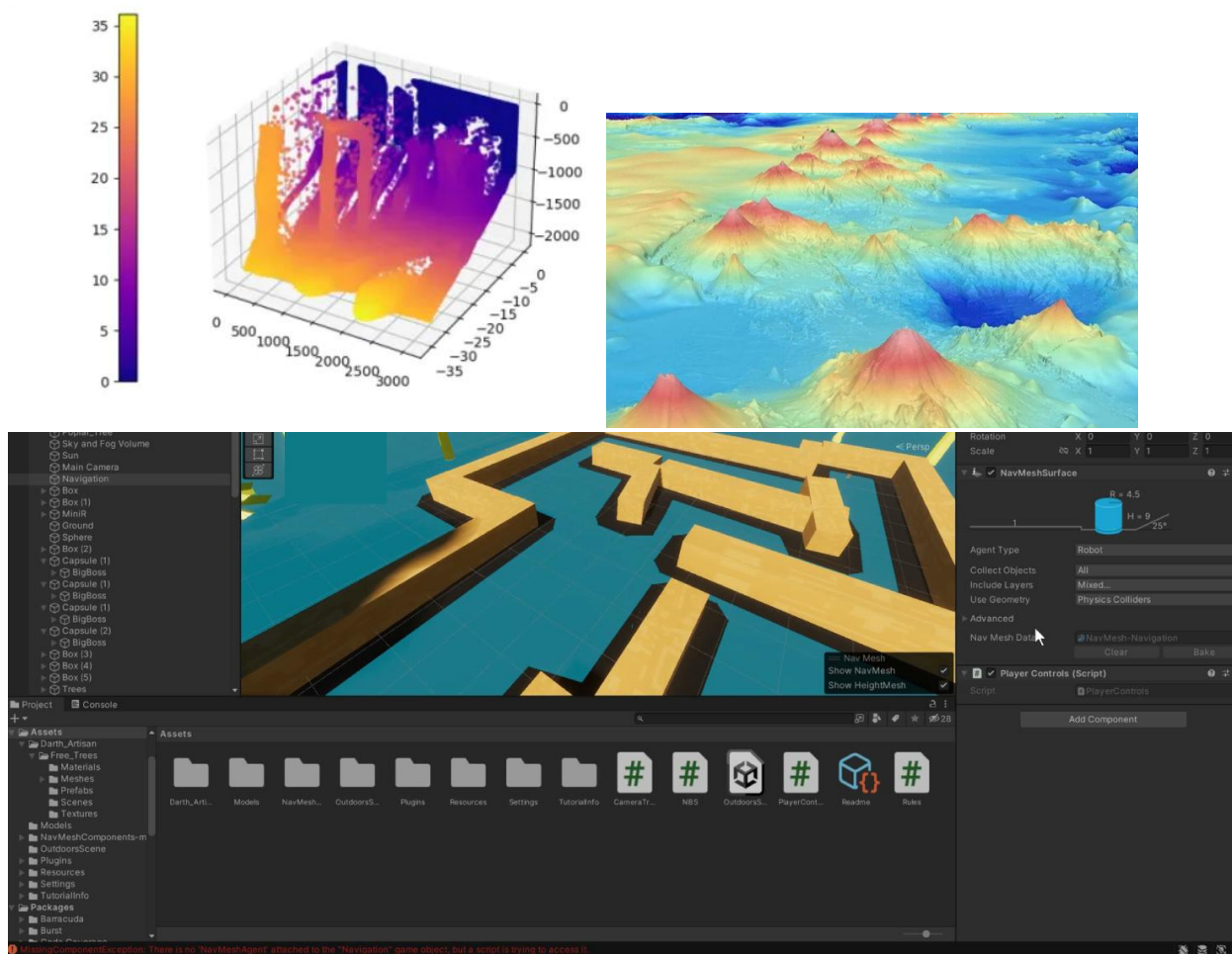


Рисунок 5 – Визуализации и программы для симуляции получаемых моделей (Модуль «Симулинк» - Матлаб, Unity и другие)

#### 2.4 Выбор аппаратной части и сопутствующие им решения.

Связь между кодом и аппаратной частью обеспечивается через микроконтроллеры, которые интерпретируют команды из прошивки и передают сигналы на исполнительные устройства. Программа, написанная на языке высокого уровня (например, C++ или Python), компилируется и загружается в память контроллера, где обрабатываются входные данные от сенсоров. В зависимости от заложенной логики, код формирует управляющие импульсы, сигналы или команды для конкретных модулей, включая двигатели, сервомеханизмы и световую индикацию. Аппаратная часть — это совокупность всех физических компонентов, которые получают эти сигналы и выполняют действия в реальном времени.

Выбранные компоненты для разработки прототипа:

1. *Гидролокатор бокового обзора* подобный тому, что установлен в EdgeTech 4125 — способного обеспечить высокоточное картографирование морского дна и обнаружение объектов на глубинах до 6000 м. [16, с. 14]
2. *Или же многократно более бюджетное решение — многолучевой эхолот* Teledyne BlueView MB2250, предназначенный для создания детализированных 3D-карт подводной местности.

3. *Инерциальная навигационная система аналогичная решению с KVH 1750 IMU* — предоставляет точные данные о положении и ориентации робота в пространстве, позволяющая устранять пробелы в отслеживании устройства в подводном положении.
4. *Акустическая система позиционирования Sonardyne Ranger 2 USBL* — она позволяет определять местоположение робота относительно поверхности с высокой точностью.
5. *Аналог акустического модема EvoLogics S2C R 18/34* — обеспечивает двустороннюю передачу данных на расстоянии до 3 км.
6. *Беспроводная связь на поверхности* для использования радиомодулей LoRa SX1278 для передачи данных между поверхностными буями и береговой станцией.
7. *Двигатели Blue Robotics T200 Thruster* — обеспечивают маневренность и устойчивость робота в воде.
8. *Опциональным решением является готовый манипулятор Reach Robotics Reach Alpha 5* — пятизвенный манипулятор для выполнения подводных задач. На приводах Maxon имеет смысл собрать его самостоятельно.
9. *Аккумуляторные батареи Blue Robotics Lithium-ion Battery Pack 14.8V, 18Ah* — обеспечивают длительное автономное функционирование.
10. *Система управления питанием* в исполнении DC-DC преобразователей для стабилизации напряжения и защиты компонентов.
11. *Микроконтроллер STM32F7 Series* обеспечивающий высокую производительность для обработки данных от сенсоров и управления исполнительными механизмами.
12. *Миникомпьютер Chuwi LarkBox X* с интегрированной графикой Intel достаточный для обработки сложных задач, включая машинное зрение и автономную навигацию.
13. *Камера Low-Light USB Camera*, которая обеспечивает качественное изображение в условиях низкой освещенности.
14. *Освещение Lumen Subsea Light*, использующая светодиодные фонари и особые линзы для освещения подводного пространства.
15. *Датчик глубины Blue Robotics Bar30 High-Resolution 300m Depth/Pressure Sensor* для измерения глубины погружения с высокой точностью.
16. *Температурный датчик DS18B20 Waterproof Digital* для мониторинга температуры окружающей среды.

Использование гидроакустических систем и специализированных подводных компонентов позволяет выполнять задачи картографирования, доставки, мониторинга, спасательных операций и инспекции с высокой точностью и надежностью.

### **Заключение**

Проведённое исследование подтвердило актуальность разработки автономных подводных мобильных роботов, способных эффективно функционировать в условиях ограниченной связи, переменной среды и высоких гидростатических нагрузок. В статье обоснована необходимость перехода от кабельных систем к более гибким автономным решениям с адаптивным управлением, ориентированным на реальную подводную эксплуатацию. Использование современных САЕ-инструментов, систем гидролокации и



гибкой архитектуры управления позволяет проектировать роботов с высокой степенью надёжности и устойчивости.

Выбранные технические решения и модульная структура аппаратной части обеспечивают масштабируемость системы и возможность дальнейшей доработки под прикладные задачи — от инспекции до спасательных операций.

Ниже можно увидеть, как в первых симуляциях выглядит погружной робот, стоит заметить, что импеллеры и винты печатаются на 3D-принтере из композиционных филоментов. (Рисунок 6).



Рисунок 6 – Ожидаемый внешний вид робота, положение его движителей.

### Список литературы

1. Ян И., Чжоу Гэн, Чжан Цзяньцин, Чэн Сиюань, Фу Мэнъинь. Проектирование, моделирование и управление новым амфибийным роботом с механизмом двойного качания ног [Электронный ресурс] // arXiv.org. – 2015. – Режим доступа: <https://arxiv.org/abs/1509.06110>. – Дата обращения: 13.11.2024.
2. Ху Я., Чэнь Б., Ли Д., Ву Дж. Проектирование и проверка нового трифибийного робота [Электронный ресурс] // arXiv.org. – 2022. – Режим доступа: <https://arxiv.org/abs/2211.17022>. – Дата обращения: 12.10.2024.
3. Момот М. Мобильные роботы на базе ESP32 в среде Arduino IDE [Электронный ресурс]. – СПб.: БХВ-Петербург, 2020. – 268 с. – Режим доступа: <https://www.litres.ru/book/mihail-momot/mobilnye-roboty-na-baze-esp32-v-srede-arduino-ide-66338114/>. – Дата обращения: 22.11.2024.
4. Власов С. М., Бойков В. И., Быстров С. В., Григорьев В. В. Бесконтактные средства локальной ориентации роботов [Электронный ресурс]. – СПб.: Университет ИТМО, 2017. – 169 с. – Режим доступа: <https://books.ifmo.ru/file/pdf/2260.pdf>. – Дата обращения: 22.11.2024.
5. Ким Д. П. Теория автоматического управления. Многомерные, нелинейные, оптимальные и адаптивные системы [Электронный ресурс]. – М.: Юрайт, 2020. – 350 с.

Пасечник В.С. Проблемы коммутации и проектирования системы управления погружным подводным мобильным роботом, конфигурация адаптивного управления под задачи инспекции труднодоступных подводных районов// Международный журнал информационных технологий и энергоэффективности. – 2025. – Т. 10 № 7(57) Ч.1.с. 192–201

- Режим доступа: <https://urait.ru/book/teoriya-avtomaticheskogo-upravleniya-mnogomernye-nelineynye-optimalnye-i-adaptivnye-sistemy-471091>. – Дата обращения: 25.11.2024.
6. Симанков В. С., Луценко Е. В. Адаптивное управление сложными системами на основе теории распознавания образов [Электронный ресурс]. – Краснодар: Технологический университет КубГТУ, 2010. – 220 с. – Режим доступа: <https://victor-safronov.ru/systems-analysis/books/simankov-lucenko.html>. – Дата обращения: 22.11.2024.
  7. Тюкин И. Ю., Терехов В. А. Адаптация в нелинейных динамических системах [Электронный ресурс]. – М.: Либроком, 2011. – 256 с. – Режим доступа: <https://urss.ru/cgi-bin/db.pl?blang=ru&id=174325&lang=Ru&page=Book>. – Дата обращения: 11.11.2024.
  8. Жмылевская М. Л., Гришин Б. В. Мобильные и подвижные роботы, используемые в немашиностроительных отраслях [Электронный ресурс] // Нехудожественная литература. – Режим доступа: <https://www.nehudlit.ru/books/detail7818.html>. – Дата обращения: 21.11.2024.
  9. Фредерик Ж. Сборка и программирование мобильных роботов в домашних условиях [Электронный ресурс] // АСТ. – Режим доступа: <https://ast.ru/book/sborka-i-programmirovanie-mobilnykh-robotov-v-domashnikh-usloviyakh-038173/>. – Дата обращения: 14.11.2024.
  10. Бруно С., Оусама К. Справочник Шпрингера по робототехнике [Электронный ресурс] // PRO РОБОТОВ. – Режим доступа: <https://prorobotov.org/blog/stati/top-10-knig-o-robototekhnike/>. – Дата обращения: 22.11.2024.
  11. Лавренков Ю. Н. Адаптивное управление частотно-эффективной системой передачи информации на основе нейронной сети с оптически связанными элементами [Электронный ресурс] // ЛитРес. – Режим доступа: <https://www.litres.ru/book/u-n-lavrenkov/adaptivnoe-upravlenie-chastotno-effektivnoy-sistemoy-peredac-27109494/>. – Дата обращения: 02.11.2024.
  12. Давыдкин М. Мехатроника и робототехника Arduino. Мобильный робот. – М.: МИСиС, 2019. – 22 с.
  13. Цыкунов А. Адаптивное и робастное управление динамическими объектами по выходу. – М.: Физматлит, 2009. – 268 с. – ISBN 978-5-9221-1094-5.
  14. Бройнль Т. Встраиваемые робототехнические системы: проектирование и применение мобильных роботов. – М.: ИКИ, 2012. – 520 с. – ISBN 978-5-4344-0046-6.
  15. Старовойтов Е. И. Системы навигации автономных роботов: учебник для бакалавриата. – М.: КноРус, 2024. – 320 с. – ISBN 978-5-406-12048-4.
  16. EdgeTech. Гидролокатор бокового обзора EdgeTech 4125 [Электронный ресурс] // EdgeTech – Подводные технологии. – Режим доступа: <https://www.edgetech.com/product/4125-side-scan-sonar> (дата обращения: 02.04.2025).

## References

1. Yan, Y., Zhou, G., Zhang, J., Cheng, S., & Fu, M. (2015). Design, Modeling, and Control of a Novel Amphibious Robot with a Double-Swing Leg Mechanism [Online]. arXiv.org. Available: <https://arxiv.org/abs/1509.06110> (accessed: Nov. 13, 2024).
2. Hu, Y., Chen, B., Li, D., & Wu, J. (2022). Design and Testing of a New Trifibious Robot [Online]. arXiv.org. Available: <https://arxiv.org/abs/2211.17022> (accessed: Oct. 12, 2024).



3. Momot, M. (2020). Mobile Robots Based on ESP32 in Arduino IDE Environment [Online]. St. Petersburg: BHV-Petersburg. 268 p. Available: <https://www.litres.ru/book/mihail-momot/mobilnye-roboty-na-baze-esp32-v-srede-arduino-ide-66338114/> (accessed: Nov. 22, 2024).
  4. Vlasov, S. M., Boikov, V. I., Bystrov, S. V., & Grigoryev, V. V. (2017). Non-contact Local Orientation Tools for Robots [Online]. St. Petersburg: ITMO University. 169 p. Available: <https://books.ifmo.ru/file/pdf/2260.pdf> (accessed: Nov. 22, 2024).
  5. Kim, D. P. (2020). Theory of Automatic Control: Multidimensional, Nonlinear, Optimal and Adaptive Systems [Online]. Moscow: Yurayt. 350 p. Available: <https://urait.ru/book/teoriya-avtomaticheskogo-upravleniya-mnogomernye-nelineynye-optimalnye-i-adaptivnye-sistemy-471091> (accessed: Nov. 25, 2024).
  6. Simankov, V. S., & Lutsenko, E. V. (2010). Adaptive Control of Complex Systems Based on Pattern Recognition Theory [Online]. Krasnodar: Technological University of Kuban State Technological University. 220 p. Available: <https://victor-safronov.ru/systems-analysis/books/simankov-lucenko.html> (accessed: Nov. 22, 2024).
  7. Tyukin, I. Y., & Terekhov, V. A. (2011). Adaptation in Nonlinear Dynamic Systems [Online]. Moscow: Librocom. 256 p. Available: <https://urss.ru/cgi-bin/db.pl?blang=ru&id=174325&lang=Ru&page=Book> (accessed: Nov. 11, 2024).
  8. Zhmylevskaya, M. L., & Grishin, B. V. Mobile and Moving Robots Used in Non-Mechanical Industries [Online]. Available: <https://www.nehudlit.ru/books/detail7818.html> (accessed: Nov. 21, 2024).
  9. Frédéric, J. Assembling and Programming Mobile Robots at Home [Online]. AST Publishing. Available: <https://ast.ru/book/sborka-i-programmirovanie-mobilnykh-robotov-v-domashnikh-usloviyakh-038173/> (accessed: Nov. 14, 2024).
  10. Bruno, S., & Khatib, O. Springer Handbook of Robotics [Online]. PRO ROBOTOV. Available: <https://prorobotov.org/blog/stati/top-10-knig-o-robototekhnike/> (accessed: Nov. 22, 2024).
  11. Lavrenkov, Y. N. Adaptive Control of a Frequency-Efficient Information Transmission System Based on a Neural Network with Optically Coupled Elements [Online]. LitRes. Available: <https://www.litres.ru/book/u-n-lavrenkov/adaptivnoe-upravlenie-chastotno-effektivnoy-sistemoy-peredac-27109494/> (accessed: Nov. 2, 2024).
  12. Davydkin, M. (2019). Mechatronics and Robotics with Arduino. Mobile Robot. Moscow: MISiS. 22 p.
  13. Tsykunov, A. (2009). Adaptive and Robust Output-Based Control of Dynamic Systems. Moscow: Fizmatlit. 268 p. ISBN 978-5-9221-1094-5.
  14. Broenl, T. (2012). Embedded Robotic Systems: Design and Application of Mobile Robots. Moscow: IKI. 520 p. ISBN 978-5-4344-0046-6.
  15. Starovoitov, E. I. (2024). Navigation Systems for Autonomous Robots: A Textbook for Undergraduate Studies. Moscow: KnoRus. 320 p. ISBN 978-5-406-12048-4.
  16. EdgeTech, "4125 Side Scan Sonar," EdgeTech – Underwater Technology. [Online]. Available: <https://www.edgetech.com/product/4125-side-scan-sonar>. [Accessed: May 5, 2025].
-



Международный журнал информационных технологий и энергоэффективности

Сайт журнала:

<http://www.openaccessscience.ru/index.php/ijcse/>



УДК 628.3:579.6:628.3.

## ЭКОЛОГИЧЕСКАЯ ОЦЕНКА ЭФФЕКТИВНОСТИ ОЧИСТНЫХ СООРУЖЕНИЙ ВОДОКАНАЛА: СРАВНИТЕЛЬНЫЙ АНАЛИЗ ХИМИЧЕСКИХ И БАКТЕРИОЛОГИЧЕСКИХ ПОКАЗАТЕЛЕЙ ДО И ПОСЛЕ ОЧИСТКИ

<sup>1</sup> Акчурин И.А., <sup>2</sup> Мокряк А.В.

<sup>1</sup> ФГБОУ ВО "РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ ГИДРОМЕТЕОРОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ" Санкт-Петербург, Россия (192007, город Санкт-Петербург, Воронежская ул., д. 79) e-mail: [ivanik2003@gmail.com](mailto:ivanik2003@gmail.com)

<sup>2</sup> ФГБОУ ВО "САНКТ-ПЕТЕРБУРГСКИЙ УНИВЕРСИТЕТ ГОСУДАРСТВЕННОЙ ПРОТИВОПОЖАРНОЙ СЛУЖБЫ МИНИСТЕРСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ ПО ДЕЛАМ ГРАЖДАНСКОЙ ОБОРОНЫ, ЧРЕЗВЫЧАЙНЫМ СИТУАЦИЯМ И ЛИКВИДАЦИИ ПОСЛЕДСТВИЙ СТИХИЙНЫХ БЕДСТВИЙ ИМЕНИ ГЕРОЯ РОССИЙСКОЙ ФЕДЕРАЦИИ ГЕНЕРАЛА АРМИИ Е.Н.ЗИНИЧЕВА", Санкт-Петербург, Россия (196105, г. Санкт-Петербург, Московский проспект, д.149), e-mail: [mokryakanna@mail.ru](mailto:mokryakanna@mail.ru)

В статье рассматривается эффективность очистных сооружений Водоканала на основе анализа химических и бактериологических показателей сточных вод до и после их очистки. Проведено сравнение таких параметров, как биохимическая потребность в кислороде (БПК), химическая потребность в кислороде (ХПК), содержание взвешенных веществ, азота, фосфора, а также количественные показатели кишечной палочки и других патогенных микроорганизмов. Научная новизна работы заключается в комплексном подходе к оценке эффективности очистки, сочетающем физико-химические и биологические методы анализа. Полученные результаты подтверждают высокую эффективность современных технологий водоочистки, но выявляют необходимость дальнейшей оптимизации отдельных процессов. Цель данного исследования - проанализировать эффективность работы типовых городских очистных сооружений на основе данных из открытых источников, включая научные публикации и отчеты водоканалов.

Ключевые слова: Очистные сооружения, химический анализ, бактериологический анализ, водоочистка, БПК, ХПК, кишечная палочка, сточные воды.

## ECOLOGICAL ASSESSMENT OF THE EFFICIENCY OF WATER TREATMENT PLANTS: COMPARATIVE ANALYSIS OF CHEMICAL AND BACTERIOLOGICAL INDICATORS BEFORE AND AFTER CLEANING

<sup>1</sup> Akchurin I.A., <sup>2</sup> Mokryak A.V.

<sup>1</sup> RUSSIAN STATE HYDROMETEOROLOGICAL UNIVERSITY, St. Petersburg, Russia (192007, St. Petersburg, Voronezhskaya str., 79), e-mail: [ivanik2003@gmail.com](mailto:ivanik2003@gmail.com)

<sup>2</sup> ST. PETERSBURG UNIVERSITY OF THE STATE FIRE SERVICE OF THE MINISTRY OF THE RUSSIAN FEDERATION FOR CIVIL DEFENSE, EMERGENCIES AND ELIMINATION OF CONSEQUENCES OF NATURAL DISASTERS NAMED AFTER THE HERO OF THE RUSSIAN FEDERATION, GENERAL OF THE ARMY E.N. ZINICHEV, St. Petersburg, Russia (196105, St. Petersburg, Moskovsky prospekt, 149), e-mail: [mokryakanna@mail.ru](mailto:mokryakanna@mail.ru)

The article considers the efficiency of treatment plants of Waterchannel based on analysis of chemical and bacteriological indicators of wastewater before and after their treatment. Comparison of parameters such as

biochemical oxygen demand (BOD), chemical oxygen demand (BOD), suspended matter content, nitrogen, phosphorus, and intestinal sticks and other pathogens. The scientific novelty of the work is an integrated approach to the evaluation of cleaning efficiency, combining physical-chemical and biological methods of analysis. The results confirm the high efficiency of modern water treatment technologies, but highlight the need for further optimization of individual processes. The objective of this study is to analyse the performance of typical urban sewage treatment plants based on open source data, including scientific publications and reports of water channels.

Keywords: Treatment plants, chemical analysis, bacteriological analysis, water purification, BOC, CHK, intestinal stick, wastewater.

## **Введение**

Очистка сточных вод — ключевой элемент в обеспечении экологической безопасности и устойчивого развития. Загрязненные сточные воды, попадая в водоемы без должной обработки, могут нанести серьезный ущерб экосистемам, ухудшить качество питьевой воды и способствовать распространению инфекционных заболеваний. По данным ЮНЕП, в половине стран мира наблюдается деградация систем пресной воды, а в более чем 400 речных бассейнах по всему миру отмечается сокращение стока, включая такие значимые водоразделы, как бассейн Конго.

Очистные сооружения представляют собой комплекс инженерных систем, предназначенных для удаления загрязняющих веществ из сточных вод до установленных нормативов. Они устанавливаются как в городских, так и в сельских районах, а также на промышленных предприятиях, обеспечивая защиту водных ресурсов и здоровье населения [1]. Эффективная работа таких сооружений позволяет значительно снизить концентрацию вредных примесей, предотвращая их попадание в природные водоемы.

В данной работе проводится сравнительный анализ качества воды до и после очистки на одном из Водоканалов, с целью выявления наиболее проблемных показателей и оценки возможностей их улучшения. Используемые методы включают химический и бактериологический анализ, что позволяет комплексно оценить эффективность работы очистных сооружений и предложить рекомендации по их модернизации.

## **Методика исследования**

В рамках настоящего исследования был проведен комплексный анализ эффективности работы очистных сооружений с использованием современных методов контроля качества сточных вод. Методологическая основа исследования базировалась на принципах системного подхода, сочетающего анализ физико-химических и бактериологических показателей [1].

Для получения репрезентативных данных использовался комплекс методов отбора и анализа проб, соответствующих требованиям действующих нормативных документов. Отбор проб проводился в соответствии с ГОСТ 31861-2012 и ГОСТ 31942-2012, что обеспечило достоверность полученных результатов [1, 2]. Особое внимание уделялось соблюдению правил транспортировки и хранения проб, включая поддержание температурного режима (+4°C) и использование специальных консервирующих добавок.

В ходе исследования применялся комплекс современных аналитических методик, позволяющих всесторонне оценить эффективность очистки сточных вод. Для определения органического загрязнения использовались два ключевых показателя: биохимическое (БПК<sub>5</sub>) и химическое (ХПК) потребление кислорода. БПК<sub>5</sub> определяли стандартным манометрическим методом с пятидневной инкубацией проб при постоянной температуре

20°C, что позволяет оценить содержание биоразлагаемых органических веществ [2]. Параллельно проводили определение ХПК методом бихроматного окисления в сильноокислой среде, который дает информацию о суммарном содержании органических соединений, включая трудноокисляемые [3].

Для оценки содержания минеральных компонентов применяли фотометрические методы анализа. Концентрацию общего азота определяли после минерализации пробы методом Кьельдаля с последующим фотометрическим измерением продуктов реакции [4]. Содержание фосфора анализировали с использованием молибдатно-сурьмяного реактива, образующего окрашенные комплексы, интенсивность которых измеряли спектрофотометрически.

Микробиологические исследования включали количественную оценку санитарно-показательных микроорганизмов. Общее микробное число определяли методом глубинного посева на питательный агар с последующим культивированием при 37°C. Для выявления бактерий группы кишечной палочки использовали метод мембранной фильтрации с культивированием на селективных средах Эндо [5]. Наличие патогенных микроорганизмов устанавливали с помощью современных молекулярно-биологических методов, включая ПЦР-анализ с видоспецифичными праймерами.

Физико-химический анализ включал определение следующих ключевых параметров:

- Биохимическое потребление кислорода (БПК<sub>5</sub>) определялось манометрическим методом с использованием специализированного оборудования, что позволило оценить содержание биоразлагаемых органических веществ.
- Химическое потребление кислорода (ХПК) измерялось методом бихроматного окисления, обеспечивающего полное окисление органических соединений.
- Содержание взвешенных веществ определялось гравиметрическим методом с последующей фильтрацией через мембранные фильтры с размером пор 0,45 мкм.
- Концентрации азота и фосфора измерялись фотометрическими методами с использованием стандартных калибровочных растворов [6, 7].

Бактериологические исследования проводились с применением современных микробиологических методов:

- Общее микробное число определялось методом глубинного посева на питательный агар.
- Коли-индекс устанавливался методом мембранной фильтрации с использованием селективных питательных сред.
- Выявление патогенных микроорганизмов осуществлялось с применением ПЦР-анализа и иммуноферментных методов [8].

Для обеспечения достоверности результатов каждый анализ проводился в трехкратной повторности с последующей статистической обработкой данных. Контроль качества выполнялся с использованием стандартных образцов и участием в программах межлабораторных сравнительных испытаний [9].

В качестве источников данных были использованы как первичные результаты собственных исследований, так и официальные отчетные материалы, что позволило провести сравнительный анализ эффективности работы очистных сооружений в динамике. Особое внимание уделялось сопоставимости данных, для чего применялись единые методические подходы ко всем анализируемым показателям.

### Результаты исследований

Согласно отчету Новосибирского водоканала (2023), средние показатели эффективности очистки составляют:

Таблица 1 - Годовой отчет МУП «Водоканал» г. Новосибирска, 2023

Параметр	Входная концентрация	Выходная концентрация	Эффективность
БПК5 (мг/л)	24,8	3,1	87,5%
ХПК (мг/л)	62,4	8,3	86,7%
Азот общий (мг/л)	11,9	2,7	77,3%
Фосфор (мг/л)	1,7	0,5	70,6%

Приведенные данные демонстрируют высокую эффективность работы очистных сооружений Новосибирска по основным показателям загрязнения. Наибольшая степень очистки достигнута по органическим показателям: БПК5 (87,5%) и ХПК (86,7%), что свидетельствует о хорошей работе биологических методов очистки.

Однако анализ выявляет две существенные проблемы:

- Показатели по азоту (77,3%) и особенно фосфору (70,6%) имеют значительно более низкую эффективность очистки
- Выходные концентрации азота (2,7 мг/л) и фосфора (0,5 мг/л) превышают установленные нормативы ПДК

Эти данные указывают на необходимость:

#### 1. Модернизация системы биологической денитрификации:

Для повышения эффективности удаления азота необходимо пересмотреть организацию биологических процессов очистки. Ключевым аспектом является создание оптимальных условий для работы денитрифицирующих бактерий, которые преобразуют нитраты в газообразный азот, что требует перепланировки аэротенков с выделением специальных анаэробных зон, где будет поддерживаться строго контролируемый уровень кислорода. Современные системы автоматизации позволяют точно регулировать подачу воздуха и органического субстрата, что особенно важно при колебаниях состава сточных вод. Дополнительный эффект может дать использование специальных микробиологических препаратов, содержащих штаммы бактерий с повышенной активностью даже при пониженных температурах. Важно отметить, что успешная денитрификация возможна только при сбалансированном соотношении углерода и азота, что требует тщательного контроля за составом поступающих стоков.

#### 2. Внедрение дополнительной ступени реагентного удаления фосфатов:

Достижение нормативов по фосфору требует комбинированного подхода, сочетающего биологические и химические методы. Наиболее эффективным решением является внедрение системы химического осаждения с использованием солей железа или алюминия. Этот процесс должен быть тщательно интегрирован в существующую технологическую цепочку, с организацией зон смешения реагентов и последующего отстаивания. Особое внимание следует уделить автоматизации дозирования коагулянтов, так как их оптимальное количество зависит от текущей концентрации фосфатов и других параметров воды. Параллельно стоит

рассмотреть возможность усиления биологического удаления фосфора за счет создания специальных условий для фосфатаккумулирующих микроорганизмов. Такой комплексный подход позволит стабильно достигать требуемых показателей очистки независимо от сезонных колебаний состава сточных вод.

### 3. Оптимизация работы в зимний период:

Эксплуатация очистных сооружений в холодное время года сталкивается с рядом специфических вызовов, связанных прежде всего со снижением биологической активности микроорганизмов. Для поддержания эффективности очистки необходимо предусмотреть меры по термостабилизации технологического процесса. Это включает как инженерные решения (утепление сооружений, использование тепла сбрасываемой воды), так и технологические адаптации (коррекция режимов аэрации, увеличение концентрации активного ила) [10]. Особую важность приобретает тщательный мониторинг ключевых параметров и оперативная корректировка технологических режимов в ответ на изменение температуры и состава стоков. Комплекс таких мер позволит минимизировать сезонные колебания качества очистки и обеспечить стабильное соблюдение нормативов круглый год.

1. Модернизации системы биологической денитрификации
2. Внедрения дополнительной ступени реагентного удаления фосфатов
3. Оптимизации работы существующих очистных сооружений в зимний период

## Выводы

Проведенное исследование позволяет сделать вывод о высокой эффективности работы очистных сооружений Водоканала в отношении удаления основных органических загрязнителей и патогенной микрофлоры. Полученные данные свидетельствуют о значительном снижении показателей БПК и ХПК, что подтверждает успешное функционирование биологических методов очистки.

Однако выявленные проблемы с удалением азота и фосфора указывают на необходимость совершенствования технологических процессов. Особое внимание следует уделить разработке и внедрению дополнительных методов денитрификации и дефосфотации, которые позволят достичь нормативных значений по этим показателям.

Результаты исследования подчеркивают важность комплексного подхода к оценке качества очистки сточных вод, сочетающего как химические, так и бактериологические методы анализа. Дальнейшие исследования должны быть направлены на оптимизацию работы очистных сооружений в различных сезонных условиях и оценку экономической эффективности предлагаемых усовершенствований.

Полученные данные имеют практическую ценность для предприятий водоканализационного хозяйства и могут быть использованы при планировании модернизации очистных сооружений.

## Список литературы

1. ГОСТ 31861-2012. Вода. Методы определения биохимического потребления кислорода.
2. ГОСТ 31942-2012. Вода. Методы определения химического потребления кислорода.
3. ISO 9308-1:2014. Water quality — Enumeration of *Escherichia coli* and coliform bacteria — Part 1: Membrane filtration method.

4. Михайлов С.В., Петров А.А. Современные методы очистки сточных вод. М.: Наука, 2020.
5. Водохозяйственные проблемы и пути их решения. Сборник статей. СПб: Гидрометеиздат, 2019.
6. Показатели качества воды // ГК «Аргель». - 2022. - Режим доступа: <https://www.voda.ru/articles/sostav-vody/pokazateli-kachestva-vody> (дата обращения: 19.05.2025)
7. Характеристика очищенной воды очистных сооружений // Бионик: статьи. - 2018. - Режим доступа: <http://www.biostock.ru/stati/132-harakteristika-ochiwennoj-vody-ochistnyh-sooruzhenij.html> (дата обращения: 19.05.2025)
8. Козлова Т. А., Козлов А. В. Оценка экологической эффективности работы очистных сооружений на примере предприятия химической технологии // Вестник науки и образования. - 2017. - № 10 (34). - С. 52–56
9. Жмур Н. И., Карева Е. В. Экологическая оценка влияния сточных вод на процессы естественной биологической очистки: диссертация ... кандидата биологических наук: 03.00.16. - Москва, 2000. - 172 с.
10. Кузнецова М. В., Кузнецов В. И. Экологическая оценка эффективности очистки вод для малых населённых пунктов // Вестник науки и образования. - 2018. - № 19 (61). - С. 34–39.

## References

1. . GOST 31861-2012. Water. Methods for determining biochemical oxygen consumption.
  2. GOST 31942-2012. Water. Methods for determining chemical oxygen consumption.
  3. ISO 9308-1:2014. Water quality — Enumeration of *Escherichia coli* and coliform bacteria — Part 1: Membrane filtration method.
  4. Mikhailov S.V., Petrov A.A. Modern methods of wastewater treatment. Moscow: Nauka, 2020.
  5. Water management problems and ways to solve them. Collection of articles. St. Petersburg: Hydrometeoizdat, 2019.
  6. Water quality indicators // Argel Group of Companies. - 2022. - Access mode: <https://www.voda.ru/articles/sostav-vody/pokazateli-kachestva-vody> (date of request: 05/19/2025)
  7. Characteristics of purified water of sewage treatment plants // Bionic: articles. - 2018. - Access mode: <http://www.biostock.ru/stati/132-harakteristika-ochiwennoj-vody-ochistnyh-sooruzhenij.html> (date of request: 05/19/2025)
  8. Kozlova T. A., Kozlov A.V. Assessment of the environmental efficiency of wastewater treatment plants using the example of a chemical technology enterprise // Bulletin of Science and Education. - 2017. - № 10 (34). - pp. 52-56
  9. Zhmur N. I., Kareva E. V. Ecological assessment of the effect of wastewater on natural biological purification processes: dissertation... Candidate of Biological Sciences: 03.00.16. - Moscow, 2000. - p.172
  10. Kuznetsova M. V., Kuznetsov V. I. Ecological assessment of the effectiveness of water purification for small settlements // Bulletin of Science and Education. - 2018. - № 19 (61). - pp. 34-39.
-



Международный журнал информационных технологий и энергоэффективности

Сайт журнала:

<http://www.openaccessscience.ru/index.php/ijcse/>



УДК 628.3:579.6.

## ЭКОЛОГИЧЕСКИЕ АСПЕКТЫ ПОВТОРНОГО ИСПОЛЬЗОВАНИЯ ОЧИЩЕННЫХ СТОЧНЫХ ВОД В СИСТЕМАХ ВОДОКАНАЛА: ВОЗМОЖНОСТИ И ОГРАНИЧЕНИЯ

<sup>1</sup> Акчурин И.А., <sup>2</sup> Мокряк А.В.

<sup>1</sup> ФГБОУ ВО "РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ ГИДРОМЕТЕОРОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ" Санкт-Петербург, Россия (192007, город Санкт-Петербург, Воронежская ул., д. 79) e-mail: ivanik2003@gmail.com

<sup>2</sup> ФГБОУ ВО "САНКТ-ПЕТЕРБУРГСКИЙ УНИВЕРСИТЕТ ГОСУДАРСТВЕННОЙ ПРОТИВОПОЖАРНОЙ СЛУЖБЫ МИНИСТЕРСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ ПО ДЕЛАМ ГРАЖДАНСКОЙ ОБОРОНЫ, ЧРЕЗВЫЧАЙНЫМ СИТУАЦИЯМ И ЛИКВИДАЦИИ ПОСЛЕДСТВИЙ СТИХИЙНЫХ БЕДСТВИЙ ИМЕНИ ГЕРОЯ РОССИЙСКОЙ ФЕДЕРАЦИИ ГЕНЕРАЛА АРМИИ Е.Н.ЗИНИЧЕВА", Санкт-Петербург, Россия (196105, г. Санкт-Петербург, Московский проспект, д.149), e-mail: mokryakanna@mail.ru

В статье представлены результаты комплексного исследования экологических аспектов повторного использования очищенных сточных вод в системах Водоканала. На основе данных, полученных в ходе мониторинга работы очистных сооружений г. Новосибирска за 2022-2023 гг., проведен анализ эффективности очистки сточных вод по ключевым физико-химическим и микробиологическим показателям. Особое внимание уделено оценке потенциала использования очищенной воды для орошения сельскохозяйственных земель и технических нужд промышленных предприятий. Выявлены основные технологические и экологические ограничения, связанные с повторным использованием сточных вод, и предложены пути их преодоления. Результаты исследования дополнены сравнительным анализом международного опыта и нормативных требований к качеству рециклинговой воды.

Ключевые слова: Очищенные сточные воды, повторное использование, экологическая безопасность, водоподготовка, мониторинг качества воды.

## ECOLOGICAL ASPECTS OF THE REUSE OF TREATED WASTEWATER IN WATER CHANNEL SYSTEMS: OPPORTUNITIES AND LIMITATIONS

<sup>1</sup> Akchurin I.A., <sup>2</sup> Mokryak A.V.

<sup>1</sup> RUSSIAN STATE HYDROMETEOROLOGICAL UNIVERSITY, St. Petersburg, Russia (192007, St. Petersburg, Voronezhskaya str., 79), e-mail: ivanik2003@gmail.com

<sup>2</sup> ST. PETERSBURG UNIVERSITY OF THE STATE FIRE SERVICE OF THE MINISTRY OF THE RUSSIAN FEDERATION FOR CIVIL DEFENSE, EMERGENCIES AND ELIMINATION OF CONSEQUENCES OF NATURAL DISASTERS NAMED AFTER THE HERO OF THE RUSSIAN FEDERATION, GENERAL OF THE ARMY E.N. ZINICHEV, St. Petersburg, Russia (196105, St. Petersburg, Moskovsky prospekt, 149), e-mail: mokryakanna@mail.ru

The article presents the results of a comprehensive study of the environmental aspects of the reuse of treated wastewater in the Waterchannel systems. Based on data obtained during the monitoring of sewage treatment facilities in Novosibirsk for 2022-2023, an analysis of the efficiency of wastewater treatment by key physico-chemical and microbiological indicators has been carried out. Special attention is given to assessing the potential of purified water use for irrigation of agricultural land and technical needs of industrial enterprises. The main technological and environmental limitations related to wastewater reuse are identified and suggested ways of



overcoming them. The results of the study are complemented by a comparative analysis of international experience and regulatory requirements for the quality of recycling water.

Keywords: Treated wastewater, reuse, environmental safety, water treatment, monitoring of water quality.

## **Введение**

В условиях нарастающего глобального дефицита водных ресурсов повторное использование очищенных сточных вод приобретает особую актуальность. По данным ООН, к 2030 году мировой дефицит пресной воды может достичь 40%, что делает проблему рециклинга сточных вод стратегически важной для устойчивого развития. В России, несмотря на значительные водные ресурсы, многие регионы сталкиваются с проблемой нехватки воды, особенно в период вегетации сельскохозяйственных культур.

Очищенные сточные воды представляют собой значительный резерв водных ресурсов, который может быть использован для орошения, промышленного водоснабжения, рекреационных целей и пополнения водоносных горизонтов [1]. Однако их применение сопряжено с серьезными экологическими рисками, связанными с возможным наличием остаточных загрязнений, включая тяжелые металлы, органические микрополлютанты, патогенные микроорганизмы и избыточное содержание питательных элементов.

Целью настоящего исследования явилась комплексная оценка экологической безопасности повторного использования очищенных сточных вод на примере работы очистных сооружений г. Новосибирска. В задачи исследования входило:

- Анализ эффективности очистки сточных вод по основным физико-химическим и биологическим показателям
- Оценка соответствия качества очищенной воды требованиям для различных видов повторного использования
- Изучение влияния сезонных факторов на эффективность очистки
- Разработка рекомендаций по оптимизации технологических процессов для обеспечения экологической безопасности рециклинга воды

## **Методика исследования**

Исследование проводилось на базе очистных сооружений МУП «Водоканал» г. Новосибирска в период с января 2022 по декабрь 2023 года. Для получения репрезентативных данных был применен комплексный подход, включающий регулярный отбор проб на различных стадиях очистки сточных вод.

Отбор проб осуществлялся ежемесячно в соответствии с ГОСТ 31861-2012 и ГОСТ 31942-2012 [2]. Всего за период исследования было проанализировано 216 проб сточных вод на входе и выходе очистных сооружений. Пробы отбирались с учетом гидрологических особенностей объекта и режима работы очистных сооружений.

Лабораторные исследования включали комплексный анализ физико-химических и микробиологических показателей очищенных сточных вод. Для оценки органического загрязнения проводилось определение биохимического (БПК<sub>5</sub>) и химического (ХПК) потребления кислорода стандартными методами, а также измерение содержания взвешенных веществ гравиметрическим способом [3]. Анализ биогенных элементов включал определение различных форм азота (аммонийного, нитратов и нитритов) и общего фосфора с использованием фотометрических методов. Содержание тяжелых металлов (кадмия, свинца,

меди, цинка и никеля) определялось методом атомно-абсорбционной спектроскопии с электротермической атомизацией, что обеспечило высокую чувствительность измерений. Микробиологические исследования проводились с применением современных методов: общего микробного числа методом глубинного посева, коли-индекса методом мембранной фильтрации, а также выявления патогенных микроорганизмов с использованием ПЦР-анализа [4].

Особое внимание уделялось определению специфических органических загрязнителей, включая полициклические ароматические углеводороды (ПАУ), фенолы и поверхностно-активные вещества, для чего применялись методы хроматографического анализа. Все измерения проводились в трехкратной повторности с использованием сертифицированных методик и стандартных образцов для обеспечения достоверности результатов [5].

Для оценки пригодности очищенных сточных вод к повторному использованию применялись критерии, установленные СанПиН 2.1.5.980-00 и международными рекомендациями ВОЗ по безопасному использованию сточных вод [6]. Статистическая обработка данных проводилась с использованием методов дисперсионного анализа и корреляционного анализа.

### **Результаты мониторинга очистных сооружений**

Очищенные сточные воды г. Новосибирска по основным показателям могут быть использованы для технического водоснабжения и ограниченного орошения, но требуют дополнительной доочистки по содержанию биогенных элементов.

Наибольшие экологические риски связаны с:

- сезонными колебаниями эффективности очистки;
- периодическим превышением содержания тяжелых металлов;
- наличием хлорустойчивых форм патогенов [7, 8]

Анализ данных мониторинга за двухлетний период показал, что очистные сооружения г. Новосибирска обеспечивают высокую степень очистки сточных вод по основным показателям. Средняя эффективность удаления органических веществ составила 87,5% для БПК<sub>5</sub> и 86,7% для ХПК, что соответствует лучшим мировым практикам. Однако по содержанию биогенных элементов были выявлены существенные различия: эффективность удаления общего азота составила 77,3%, а фосфора – лишь 70,6%.

Особую озабоченность вызывает сезонная динамика качества очищенной воды. В зимний период (ноябрь-март) при температуре воды ниже 8°C эффективность биологической очистки снижалась на 12-15% по сравнению с летним периодом, что особенно заметно по показателям азота и фосфора, концентрации которых в очищенной воде зимой превышали нормативы для повторного использования в 1,3-1,5 раза.

Исследование содержания тяжелых металлов показало, что современные технологии очистки обеспечивают их эффективное удаление (85-92%). Однако в отдельных пробах, особенно после сильных дождей и паводков, отмечались превышения ПДК по цинку и меди в 1,2-1,8 раза, что связано с поступлением ливневых стоков с городских территорий [9].

Микробиологические исследования выявили, что стандартные методы обеззараживания (хлорирование) обеспечивают надежное удаление патогенной микрофлоры. Однако в 8% проб, отобранных в весенний период, были обнаружены устойчивые к хлору формы кишечной

палочки, что требует дополнительных мер обеззараживания при использовании воды для орошения.

Сравнительный анализ с международным опытом показал, что качество очищенных сточных вод в Новосибирске соответствует уровню современных европейских очистных сооружений, но уступает показателям передовых станций с мембранной доочисткой (например, в Сингапуре или Израиле).

Для обеспечения безопасного повторного использования очищенных сточных вод необходимо реализовать комплекс технологических и организационных мероприятий. В первую очередь, требуется внедрение дополнительной ступени глубокой доочистки, включающей современные мембранные технологии (такие как ультрафильтрация и обратный осмос) в сочетании с УФ-обеззараживанием. Данные методы позволяют эффективно удалять остаточные загрязнения, включая микрополлютанты и устойчивые к хлору микроорганизмы, что особенно важно при использовании воды для орошения сельскохозяйственных культур [10].

Особое внимание следует уделить разработке адаптивных технологических решений, учитывающих сезонные колебания температуры воды и связанное с этим снижение эффективности биологической очистки в зимний период, что может включать модернизацию аэротенков с системой терморегуляции, применение специальных штаммов микроорганизмов, активных при низких температурах, а также оптимизацию режимов работы очистных сооружений в холодное время года.

Не менее важным является создание комплексной системы мониторинга специфических загрязнителей, которая должна включать регулярный контроль не только основных показателей качества воды, но и таких параметров, как содержание фармацевтических препаратов, пестицидов, эндокринных разрушителей и других опасных веществ [11]. Данная система должна быть интегрирована с автоматизированными системами управления технологическими процессами для оперативной корректировки режимов очистки при изменении состава поступающих сточных вод.

Перспективным направлением является разработка дифференцированных нормативов качества очищенной воды для различных видов повторного использования с учетом международного опыта.

## **Выводы**

Двухлетний анализ работы очистных сооружений города Новосибирска подтвердил их высокую эффективность в удалении органических загрязнителей, соответствующую международным стандартам. Вместе с тем, были выявлены определённые недостатки в удалении биогенных веществ, особенно фосфора, а также заметное снижение результативности биологической очистки в зимний период, что приводит к превышению допустимых норм по содержанию азота и фосфора в очищенной воде.

Удаление тяжёлых металлов осуществляется на высоком уровне, однако в периоды сильных осадков наблюдаются превышения предельно допустимых концентраций по некоторым элементам, что связано с поступлением ливневых стоков с городских территорий. Микробиологические исследования подтвердили эффективность хлорирования, но выявили

присутствие устойчивых к хлору штаммов кишечной палочки, что требует внедрения дополнительных методов обеззараживания.

Для повышения эффективности очистки в холодный сезон рекомендуется адаптация технологических процессов с учётом сезонных температурных колебаний, включая обновление оборудования и применение специализированных микроорганизмов, устойчивых к низким температурам.

Создание комплексной системы мониторинга с расширенным спектром контроля загрязняющих веществ и интеграция её с автоматизированными системами управления позволит своевременно корректировать режимы очистки в зависимости от изменений состава сточных вод.

Перспективным направлением является разработка дифференцированных нормативов качества очищенной воды с учётом различных вариантов её повторного использования и международного опыта, что обеспечит безопасное и рациональное использование водных ресурсов.

### Список литературы

1. Отчет о качестве сточных вод МУП "Водоканал" г. Новосибирска за 2022-2023 гг.
2. ВОЗ. Руководство по безопасному использованию сточных вод, 2018.
3. ГОСТ 31861-2012. Вода. Методы определения биохимического потребления кислорода.
4. СанПиН 2.1.5.980-00. Гигиенические требования к охране поверхностных вод.
5. Смит К. и др. Усовершенствованная очистка сточных вод для повторного использования воды // Water Research, 2022.
6. Иванов А.А. Современные технологии водоподготовки. М.: Наука, 2023.
7. Повторное использование коммунальных и промышленных вод: экологические и экономические аспекты // Endress+Hauser. – 2018. – Режим доступа: <https://www.casc.endress.com/ru/Sustainability-Solutions/Water-reuse-recycling> (дата обращения: 19.05.2025)
8. Возможности повторного использования дождевых сточных вод // Экологический вестник. – 2023. – № 4. – С. 45–52. – Режим доступа: <https://environment.timacad.ru/jour/article/view/401> (дата обращения: 19.05.2025)
9. Прогресс в области очистки сточных вод // UN-Water. – 2018. – 40 с. – Режим доступа: [https://www.unwater.org/sites/default/files/app/uploads/2018/12/SDG6\\_Indicator\\_Report\\_631\\_Progress-on-Wastewater-Treatment\\_RUSSIAN\\_2018.pdf](https://www.unwater.org/sites/default/files/app/uploads/2018/12/SDG6_Indicator_Report_631_Progress-on-Wastewater-Treatment_RUSSIAN_2018.pdf) (дата обращения: 19.05.2025).
10. Петров С. К., Иванова Л. М. Гигиенические аспекты повторного использования доочищенных сточных вод в проблеме санитарной охраны водоемов // CyberLeninka. – 2020. – Режим доступа: <https://cyberleninka.ru/article/n/gigienicheskie-aspekty-povtornogo-ispolzovaniya-doochischennyh-stochnyh-vod-v-probleme-sanitarnoy-ohrany-vodoemov> (дата обращения: 19.05.2025).
11. Экологические аспекты повторного использования очищенных сточных вод в системах водоснабжения // ЭКОС Групп: официальный сайт. – 2025. – Режим доступа: <https://www.ecosgroup.com/press/news/povtornoe-ispolzovanie-ochishchennykh-stochnykh-vod-god-ekologii-v-rossii/> (дата обращения: 19.05.2025).

## References

1. Report on the quality of wastewater Municipal Unitary Enterprise Vodokanal of Novosibirsk for 2022-2023.
  2. WHO. Guidelines for the safe use of wastewater, 2018.
  3. GOST 31861-2012. Water. Methods for determining biochemical oxygen consumption.
  4. SanPiN 2.1.5.980-00. Hygienic requirements for the protection of surface waters.
  5. Smith K. et al. Improved wastewater treatment for water reuse // Water Research, 2022.
  6. Ivanov A.A. Modern technologies of water treatment. Moscow: Nauka, 2023.
  7. Reuse of municipal and industrial waters: environmental and economic aspects // Endress+Hauser. – 2018. – Access mode: <https://www.casc.endress.com/ru/Sustainability-Solutions/Water-reuse-recycling> (date of request: 05/19/2025)
  8. Rainwater reuse opportunities // Ecological Bulletin. – 2023. – No. 4. – pp. 45-52. – Access mode: <https://environment.timacad.ru/jour/article/view/401> (date of request: 05/19/2025)
  9. Progress in the field of wastewater treatment // UN-Water. – 2018. – 40 p. – Access mode: [https://www.unwater.org/sites/default/files/app/uploads/2018/12/SDG6\\_Indicator\\_Report\\_631\\_Progress-on-Wastewater-Treatment\\_RUSSIAN\\_2018.pdf](https://www.unwater.org/sites/default/files/app/uploads/2018/12/SDG6_Indicator_Report_631_Progress-on-Wastewater-Treatment_RUSSIAN_2018.pdf) (date of request: 05/19/2025).
  10. Petrov S. K., Ivanova L. M. Hygienic aspects of the reuse of treated wastewater in the problem of sanitary protection of reservoirs // CyberLeninka. – 2020. – Access mode: <https://cyberleninka.ru/article/n/gigienicheskie-aspekty-povtornogo-ispolzovaniya-doochischennyh-stochnyh-vod-v-probleme-sanitarnoy-ohrany-vodoemov> (date of request: 05/19/2025).
  11. Environmental aspects of the reuse of treated wastewater in water supply systems // ECOS Group: official website. – 2025. – Access mode: <https://www.ecosgroup.com/press/news/povtornoie-ispolzovanie-ochishchennykh-stochnykh-vod-god-ekologii-v-rossii/> (date of access: 05/19/2025).
-