Научная статья
УДК 004.056

НОВЫЕ ИНСТРУМЕНТЫ УСТОЙЧИВОСТИ И БЕЗОПАСНОСТИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ: СОВРЕМЕННЫЕ ПОДХОДЫ И ПЕРСПЕКТИВЫ

Евгения Васильевна Анянова[1], Андрей Юрьевич Кочев[2]
[1, 2] Уральскийгосударственный лесотехнический университет, Екатеринбург, Россия
[1] anyanovagv@m.usfeu.ru
[2] Andrei.kochev.1990@mail.ru

Аннотация. В данной статье рассматриваются новые инструменты и методы, направленные на повышение устойчивости и безопасности информационных инфраструктур. Особое внимание уделяется технологиям искусственного интеллекта (ИИ), блокчейну, постквантовой криптографии и адаптивным системам мониторинга. Анализируются их преимущества, ограничения и перспективы внедрения.

Ключевые слова: кибербезопасность, устойчивость, ИИ в безопасности, блокчейн, постквантовая криптография

***Для цитирования*:** Анянова Е. В., Кочев А. Ю. Новые инструменты устойчивости и безопасности в информационных системах: современные подходы и преспективы // Цивилизационные перемены в России = Civilizational changes in Russia : материалы XV Всероссийской научно-практической конференции. Екатеринбург : УГЛТУ, 2025. С. 84−88.

Original article

NEW TOOLS FOR RESILIENCE AND SECURITY IN INFORMATION SYSTEMS: MODERN APPROACHES AND PROSPECTS

Evgeniya V. Anyanova[1], Andrey Yu. Kochev[2]
[1, 2] Ural State Forest Engineering University, Ekaterinburg, Russia
[1] anyanovagv@m.usfeu.ru
[2] Andrei.kochev.1990@mail.ru

Abstract. This article considers new tools and methods aimed at increasing the resilience and security of information infrastructures. Special attention is

given to artificial intelligence (AI) technologies, blockchain, postquantum cryptography, and adaptive monitoring systems. Their advantages, limitations, and implementation prospects are analyzed.

***Keywords*:** cybersecurity, resilience, AI in security, blockchain, post-quantum cryptography

For citation: Anyanova E. V., Kochev A. Yu. (2025) Novyye instrumenty ustoichivosti i bezopasnosti v informacyonnykh sistemakh: sovremennye podhody i perspektivy [New tools for resilience and security in information systems: modern approaches and prospects]. Civilizacionnye peremeny v Rossii [Civilizational changes in Russia] : proceedings of the XV All-Russian Scientific and Practical Conference. Ekaterinburg : USFEU, 2025. P. 84–88. (In Russ).

С развитием цифровых технологий возрастает сложность защиты информационных систем от кибератак, сбоев и эксплуатационных рисков. Традиционные механизмы безопасности, такие как антивирусы и межсетевые экраны, уже не справляются с современными угрозами. В связи с этим появляются новые инструменты, обеспечивающие более высокий уровень устойчивости и защиты.

Среди ключевых угроз можно выделить: целевые атаки (APT) – сложные многоэтапные кибератаки, уязвимости в цепочке поставок (Supply Chain Attacks) – компрометация через сторонние компоненты, а также квантовые вычисления, которые являются угрозой существующим криптографическим алгоритмам.

Для противодействия этим угрозам требуются инновационные решения. Например, искусственный интеллект и машинное обучение позволяет обнаруживать аномалии в режиме реального времени (UEBA – User and Entity Behavior Analytics), прогнозировать атаки на основе анализа больших данных, автоматизировать реагирование на инциденты (SOAR – Security Orchestration, Automation and Response). Пример: системы на основе OpenAI и специализированных ML-моделей (например, Darktrace) успешно выявляют скрытые угрозы [1].

Кейс 1. Darktrace в защите финансового сектора [2]

У крупного европейского банка Banco Santander (Испания) появилась проблема в связи с участившимися целевыми атаками (APT) и инсайдерскими угрозами. После внедрения системы Darktrace на основе машинного обучения результатом стало снижение числа успешных атак на 68 % только за первый год; обнаружение скрытого майнинга криптовалют в корпоративной сети; автоматическое блокирование аномальных действий (например, массовый экспорт данных).

Вывод: ИИ эффективен для обнаружения неизвестных угроз, но требует тонкой настройки для минимизации ложных срабатываний.

Блокчейн-технологии для обеспечения целостности данных обеспечивают децентрализованное хранение журналов событий (аудит без возможности подделки), устойчивость к DDoS за счет распределенности, смарт-контракты для автоматизации политик безопасности.

Применение: Hyperledger Fabric в корпоративных системах, защита IoT-устройств.

Пример: допустим, завод, поставщик и логистическая компания ведут общую базу поставок. Fabric фиксирует каждое действие (от заказа до доставки), и все участники видят одинаковые данные, которые нельзя скрыть или изменить задним числом.

Защита IoT-устройств с блокчейном – это как «неуязвимый замок» для умных гаджетов.

Проблема: «умные» камеры, датчики или медицинские приборы часто взламывают, потому что они слабо защищены.

Как помогает блокчейн? Каждое устройство получает уникальный цифровой паспорт в блокчейне. Если хакер попытается подменить firmware (прошивку), система это сразу заметит и заблокирует устройство. Данные с датчиков (например, температура на складе) записываются в блокчейн, поэтому их нельзя подделать.

Кейс 2. Microsoft Azure Sentinel в здравоохранении

Крупнейшая сеть клиник в США и Великобритании (более 400 клиник) в 2020 году столкнулась с Ransomware-атакой, нарушающей работу медицинского оборудования, которая парализовала работу на 2 недели. После инцидента UHS внедрила облачные системы мониторинга (включая Azure Sentinel) для раннего обнаружения угроз, что стало результатом сокращенного времени реагирования с 4 ч до 15 мин, а также предотвращения шифрования данных в 92 % случаев.

Постквантовая криптография

С появлением квантовых компьютеров традиционные алгоритмы (RSA, ECC) станут уязвимыми. Альтернативы: алгоритмы на решетках (Lattice-based cryptography), хеш-подписи (SPHINCS+), многомерные криптосистемы.

Стандартизация: NIST уже отобрал несколько кандидатов (CRYSTALS-Kyber, CRYSTALS-Dilithium).

Кейс 3. Google Chrome и эксперименты с NIST-алгоритмами

Тестирование постквантового алгоритма CRYSTALS-Kyber в TLS соединениях явилось результатом успешной защиты от перехвата трафика в гибридном режиме (классический + постквантовый алгоритм), но это привело к росту нагрузки процессора компьютера на 15–20 %. Поэтому постквантовая криптография хоть и готова к пилотным внедрениям, но требует оптимизации.

Адаптивные системы мониторинга Zero Trust Architecture (ZTA) – «никому не доверяй, проверяй всегда». EDR/XDR – расширенное обнаружение

и реагирование на угрозы. Динамическая аутентификация – биометрия + поведенческий анализ.

Кейс 4. Внедрение Zero Trust в Корпоративную сеть Cisco, которая является мировым лидером в сетевых технологиях, поэтому использует свои же продукты (например, Duo Security для MFA, SecureX для мониторинга) в качестве «полигона» для тестирования. Они применяли поэтапный переход на модель Zero Trust Architecture (ZTA):

1. Сегментация сети (микросервисная архитектура).
2. Внедрение MFA и поведенческой аутентификации.
3. Мониторинг в реальном времени с помощью Duo Security, что привело к положительным результатам: снижение числа успешных фишинговых атак на 75 %, упрощение контроля доступа для удаленных сотрудников (таблица).

Сравнительная таблица эффективности инструментов

Инструмент	Эффективность	Сложность внедрения	Примеры использования
ИИ (Darktrace)	⋆ ⋆ ⋆ ⋆ ☆	⋆ ⋆ ⋆ ☆ ☆	Финансы, здравоохранение
Блокчейн	⋆ ⋆ ⋆ ☆ ☆	⋆ ⋆ ⋆ ⋆ ☆	Логистика, госсектор
Постквантовая	⋆ ⋆ ☆ ☆ ☆	⋆ ⋆ ⋆ ⋆ ⋆	TLS, VPN
Zero Trust	⋆ ⋆ ⋆ ⋆ ⋆	⋆ ⋆ ⋆ ☆ ☆	Корпоративные сети

⋆ – низкий; ⋆ ⋆ ⋆ ⋆ ⋆ – высокий.

Таким образом, анализ реальных кейсов подтверждает, что ИИ наиболее универсален для обнаружения угроз, однако его применение сталкивается с ключевыми ограничениями, такими как сильная зависимость от качества и репрезентативности обучающих данных, высокие требования к вычислительным ресурсам, проблема «ложных срабатываний», требующая постоянной тонкой настройки.

Блокчейн-технологии обеспечивают беспрецедентный уровень доверия и прозрачности в корпоративных системах, но остаются экономически невыгодными для массового внедрения, имеют проблемы с масштабируемостью, требуют полного пересмотра существующих бизнеспроцессов.

Постквантовая криптография становится критически важной в условиях развития квантовых вычислений, но существующие алгоритмы (NIST PQC) пока не оптимизированы для массового использования; наблюдается значительный рост нагрузки на системы, требуется поэтапный переход с сохранением обратной совместимости.

Zero Trust доказала свою эффективность в крупных корпорациях, но требует полного перепроектирования сетевой инфраструктуры, создает дополнительные сложности для пользователей, нуждается в комплексных решениях для управления политиками доступа.

Направления будущих исследований:

– особое внимание следует уделить междисциплинарным исследованиям, объединяющим достижения в области компьютерных наук, математической криптографии и когнитивной психологии. Будущее информационной безопасности лежит в создании комплексных адаптивных систем, способных эволюционировать вместе с развитием угроз;

– ключевым вызовом остается поиск баланса между безопасностью, производительностью и удобством использования, что требует тесного сотрудничества исследователей, разработчиков и конечных пользователей.

Список источников

1. Post-Quantum Cryptography Standardization // NIST : [сайт]. URL: https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Post-Quantum-Cryptography-Standardization (дата обращения: 16.09.2025).

2. Gartner’s 2024 Cybersecurity Trends: Key Takeaways // Tech Times : [сайт]. URL: https://techtimeslive.com/gartner-top-trends-in-cybersecurity-2024/ (дата обращения: 16.09.2025).

References

1. Post-Quantum Cryptography Standardization // NIST : [website]. URL: https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Post-Quantum-Cryptography-Standardization (date of accessed: 16.09.2025).

2. Gartner’s 2024 Cybersecurity Trends: Key Takeaways // Tech Times : [website]. URL: https://techtimeslive.com/gartner-top-trends-in-cybersecurity-2024/ (date of accessed: 16.09.2025).