УДК 004.056.5

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

Кочев А. Ю., студент гр. мИЦЭ-21, 2 курс СЭИ,
Научный руководитель: Щепеткин Е. Н., к.т.н., доцент
Уральский государственный лесотехнический университет,
г. Екатеринбург

Современные информационные системы сталкиваются с растущими угрозами кибербезопасности и требованиями к отказоустойчивости. 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 [1].

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

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.

Кейс 1. Darktrace в защите финансового сектора

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 [2].

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 часов до 15 минут, а также предотвращение шифрования данных в 92% случаев [3].

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 плюс 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) [4].

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 удалённых сотрудников.

Таблица 1 – 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)

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 бизнес- процессов.

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 [5].

Список литературы:

1. CIS. CIS Critical Security Controls, Version 8. – East Greenbush : Center for Internet Security, 2021. – 94 p.
2. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection - Information security management systems - Requirements. – Geneva : ISO, 2022.
3. ISO/IEC 27002:2022. Information security, cybersecurity and privacy protection - Information security controls. – Geneva : ISO, 2022.
4. ENISA. ENISA Threat Landscape 2024. – Athens : European Union Agency for Cybersecurity, 2024. – 158 p.
5. Bernstein, D. J. Post-Quantum Cryptography / D. J. Bernstein, J. Buchmann, E. Dahmen. – Berlin : Springer, 2009. – 245 p. – DOI 10.1007/978-3-540-88702-7.