

2 **Карпова, Т. П.** Процесс оценки кадрового потенциала организации в управлении персоналом / Т. П. Карпова, М. О. Фурсов // Вестник самарского муниципального института управления. – 2024. – № 3. – С. 49–56.

3 **Юсупова, Т. А.** Анализ кадрового потенциала: обзор эффективных методов оценки / Т. А. Юсупова, З. Ш. Амерханова, В. Х. Хадисов // Индустриальная экономика. – 2022. – Т. 1, № 2. – С. 69–77.

Получено 24.05.2026

ISSN 2227-1155. Сборник студенческих научных работ.
Вып. 31. Гомель, 2026

УДК 004.8:004.056

И. А. ГАВРИЛЕНКО (ЭМ-31)

Научный руководитель – ст. преп. *В. Е. МИНИН*

ПРИМЕНЕНИЕ ТЕХНОЛОГИЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В АРХИТЕКТУРЕ КИБЕРБЕЗОПАСНОСТИ

Рассматриваются методологические и архитектурные аспекты интеграции технологий искусственного интеллекта в процессы обеспечения информационной безопасности. Проведён анализ современного инструментария (SAST/DAST, NDR, автономный пентестинг) и роли поведенческого анализа в обнаружении угроз. Представлена методология оценки эффективности на основе ретроспективного анализа реальных инцидентов. Рассмотрены подходы к построению адаптивной защиты на базе фреймворка MITRE D3FEND, а также практики использования ИИ на тренировочных стендах (Cyber Range) для генерации синтетических данных и моделирования атак. Сформулированы ограничения ИИ-решений и обоснована необходимость комбинированного подхода к защите.

Центральными направлениями применения ИИ в защите приложений и сетей являются интеллектуальный статический и динамический анализ (SAST/DAST), сетевой анализ (NDR) и автономный пентестинг.

При проведении анализа приложения ключевым элементом является представление исходного кода в виде графа свойств кода (Code Property Graph), объединяющего абстрактное синтаксическое дерево, граф потока управления и граф зависимостей данных. Для обработки таких структур применяются графовые нейронные сети (GNN) и трансформерные модели, способные выявлять сложные цепочки уязвимостей (например, SQL-инъекции) без жестких сигнатурных шаблонов [3]. В динамическом анализе используется интеллектуальный фаззинг на базе обучения с подкреплением, оптимизирующий генерацию входных данных для максимизации покрытия кода.

В системах NDR (Network Detection and Response) основой является построение модели «нормального» поведения сети с помощью обучения без учителя (алгоритмы кластеризации k-means, DBSCAN, Isolation Forest) и рекуррентных нейросетей (LSTM) для анализа временных рядов. Графовый анализ позволяет выявлять сценарии горизонтального перемещения (lateral movement) злоумышленника внутри сети.

Автономный пентестинг моделирует поведение атакующего через построение графов атак. ИИ-агент, используя обучение с подкреплением, последовательно выполняет действия (разведка, эксплуатация, повышение привилегий), получая «награду» за успех и «штраф» за риск обнаружения, что позволяет находить критические цепочки компрометации.

Оценка эффективности ИИ-систем целесообразно рассмотреть через ретроспективный анализ реальных инцидентов, демонстрирующих пробелы классических средств защиты.

В сентябре 2023 года компания MGM Resorts International подверглась масштабной кибератаке, парализовавшей операционную деятельность на срок более 10 дней. Злоумышленники из группировки Scattered Spider применили методы социальной инженерии, связавшись со службой технической поддержки и убедив персонал сбросить параметры многофакторной аутентификации. После получения доступа к внутренним системам с использованием легитимных учетных данных было развернуто ransomware-шифрование. Финансовые потери составили приблизительно 8,4 миллиона долларов в сутки, общий ущерб превысил 100 миллионов долларов, было похищено около 6 терабайт конфиденциальной информации.

В мае 2023 года была обнаружена критическая уязвимость нулевого дня (CVE-2023-34362) в программном обеспечении MOVEit Transfer – платформе для безопасной передачи файлов. Группировка Clor эксплуатировала уязвимость типа SQL-инъекции, позволявшую неаутентифицированным злоумышленникам получить доступ к базе данных. Пострадало более 2700 организаций по всему миру, включая British Airways, BBC и государственные учреждения США и Великобритании; скомпрометированы данные от 60 до 93,3 миллионов человек.

Атака на SolarWinds (2020): операция SUNBURST, обнаруженная в декабре 2020 года, представляет собой одну из наиболее сложных атак на цепочку поставок программного обеспечения. Группировка APT29 внедрила вредоносный код в процесс сборки программного обеспечения Orion Platform компании SolarWinds, после чего зараженные обновления были распространены среди более чем 18 000 клиентов. Реально скомпрометировано от 100 до 200 организаций, включая Министерство финансов США, Министерство энергетики, Пентагон, Microsoft и Intel. Backdoor активировался через 12–14 дней после установки обновления и использовал легитимный протокол Orion Improvement Protocol для скрытого канала связи с командно-управляющими серверами. Традиционные средства защиты не

смогли выявить угрозу, поскольку программное обеспечение было подписано цифровой подписью и считалось безопасным.

Эффективность внедрения ИИ оценивается через снижение времени обнаружения (MTTD) и реагирования (MTTR), а также через коэффициент снижения ложных срабатываний (FPR) по сравнению с базовыми правилами.

Выбор стратегии защиты определяется балансом между скоростью реакции на известные угрозы и способностью обнаруживать новые векторы атак. Сравнение подходов представлено в таблице 1.

Таблица 1 – Сравнительный анализ классических и ИИ-ориентированных подходов в ИБ

Характеристика	Классические (сигнатурные) методы	ИИ-ориентированные системы (поведенческие)
Принцип работы	Сравнение с базой известных сигнатур и правил	Построение базовой модели поведения и поиск аномалий
Эффективность против 0-day	Низкая (требуется обновление сигнатур)	Высокая (выявляет отклонения от нормы)
Скорость реакции	Мгновенная при совпадении сигнатуры	Требует времени на обучение и адаптацию модели
Ложные срабатывания	Низкие (при актуальных базах)	Высокие при изменениях в легитимной инфраструктуре
Устойчивость к обфускации	Низкая	Высокая (анализ семантики и графовых связей)

Классические системы остаются эталоном для блокировки массовых известных угроз, тогда как ИИ-решения критически важны для обнаружения сложных, многоэтапных и ранее неизвестных атак.

Фреймворк MITRE D3FEND фокусируется на контрмерах («как защищаться»), формируя граф знаний, связывающий угрозы с методами нейтрализации. Интеграция ИИ с D3FEND позволяет создавать следующие адаптивные системы защиты:

1 *Моделирование (Model)* предполагает создание «цифрового двойника» инфраструктуры в виде графа для вероятностного моделирования (например, методом Монте-Карло), что позволяет непрерывно оценивать риски при изменениях в сети.

2 *Технология обмана (Decoy)* использует алгоритмы машинного обучения для генерации адаптивных приманок, таких как поддельные серверы и учетные данные. В отличие от статических «ловушек», такие приманки динамически подстраиваются под поведение атакующего, собирая разведданные о его методах без риска для реальной инфраструктуры.

3 *Оркестрация* является ключевым элементом реагирования, обеспечивающим динамическое принятие решений о нейтрализации угроз на основе сопоставления событий с графом знаний MITRE D3FEND. В отличие от

традиционных систем безопасности, где реакции задаются статическими правилами и сценариями, ИИ-оркестратор формирует стратегию противодействия в реальном времени, учитывая контекст инцидента, критичность затронутых ресурсов и текущее состояние инфраструктуры.

Качество ИИ-моделей в кибербезопасности напрямую зависит от репрезентативности данных. Для решения проблемы дефицита размеченных данных и конфиденциальности активно применяются тренировочные среды (Cyber Range) и генерация синтетических датасетов.

Генерация «умного трафика» предполагает моделирование поведенческих паттернов легитимных пользователей с учетом рабочих процессов, временных интервалов активности и типичных ошибок операторов. В отличие от статических или случайно сгенерированных событий, такой подход создает реалистичный фон, на котором можно тестировать системы обнаружения аномалий и обучать аналитиков SOC в условиях, максимально приближенных к реальной инфраструктуре.

4 Adversarial AI заключается в создании автономных агентов-атакующих на базе обучения с подкреплением, которые последовательно выполняют этапы кибератаки – от разведки до повышения привилегий и горизонтального перемещения, получая «награду» за успешные действия и «штраф» за риск обнаружения.

Это позволяет моделировать многовекторные атаки с адаптивным поведением, которое сложно воспроизвести вручную.

5 Neural fuzzing предполагает использование нейросетевых моделей для предсказания входных данных, с наибольшей вероятностью вызывающих уязвимости или ошибки обработки, что значительно ускоряет процесс тестирования по сравнению с классическим случайным фаззингом и позволяет выявлять скрытые дефекты, проявляющиеся только при специфических условиях.

Важно отметить, что ИИ не является заменой организационных процессов. Большинство крупных инцидентов происходят из-за человеческого фактора и ошибок конфигурации, которые ИИ может лишь смягчить, но не устранить полностью.

Интеграция искусственного интеллекта в архитектуру кибербезопасности является закономерным и обязательным этапом эволюции защиты, обусловленным масштабом и сложностью современных угроз. ИИ эффективно закрывает пробелы классических методов, работая с большими объемами телеметрии и выявляя аномалии.

Однако успешное внедрение требует понимания ограничений: зависимости от качества данных, риска ложных срабатываний и неспособности ИИ компенсировать фундаментальные организационные ошибки.

Оптимальной стратегией является комбинированный подход: использование ИИ для автоматизации и первичного анализа, классических средств

для быстрого реагирования на известные угрозы и обязательное участие квалифицированных специалистов, опирающихся на структурированные фреймворки, такие как MITRE D3FEND.

СПИСОК ЛИТЕРАТУРЫ

1 **Карпов, А. В.** Применение методов машинного обучения для обнаружения аномалий в сетевом трафике / А. В. Карпов, С. И. Иванов // Вопросы кибербезопасности. – 2021. – № 3 (41). – С. 45–53.

2 **Смирнов, Д. С.** Использование графовых нейронных сетей для статического анализа исходного кода / Д. С. Смирнов // Труды Института системного анализа РАН. – 2022. – Т. 42, № 2. – С. 112–120.

3 «Лаборатория Касперского». Ежегодный отчет Kaspersky Security Bulletin 2023. Эволюция угроз и статистика киберпреступности – URL: <https://securelist.ru/kaspersky-security-bulletin-2023/> (дата обращения: 02.04.2026).

4 **Орлов, И. В.** Построение адаптивной архитектуры информационной безопасности на основе графов знаний MITRE D3FEND / И. В. Орлов // Информационная безопасность регионов. – 2024. – № 1. – С. 34–41.

5 **Федоров, К. Л.** Применение искусственного интеллекта на тренировочных стендах (Cyber Range) для моделирования атак / К. Л. Федоров // Информатика и безопасность. – 2023. – № 4. – С. 15–22.

Получено 11.06.2026

ISSN 2227-1155. Сборник студенческих научных работ.

Вып. 31. Гомель, 2026

УДК 629.1:621.396.96

Н. С. ГАПЕЕВ (БСА-31)

Научный руководитель – ст. преп. *П. А. КАЦУБО*

ПЕРСПЕКТИВЫ ВНЕДРЕНИЯ СВЧ-ТЕХНОЛОГИЙ В ДОРОЖНЫЕ ПОКРЫТИЯ

Проведен анализ перспектив внедрения СВЧ-технологий в дорожное покрытие, включая их влияние на улучшение качества и устойчивости материалов. Приведены примеры использования СВЧ-технологий в дорожном строительстве, описаны их преимущества, особенности применения и потенциальные направления для дальнейшего развития в этой области.

Современные дорожные сети требуют эффективных и экономичных методов борьбы с зимней скользкостью. Традиционные способы, такие как использование реагентов или механическая уборка, имеют ряд экологиче-