УДК 004.056

Владимиров Андрей Николаевич

студент

5 курс, факультет «Кибербезопасности»

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича

Россия, г. Санкт-Петербург

АВТОМАТИЗАЦИЯ ЦИФРОВОЙ КРИМИНАЛИСТИКИ И РЕАГИРОВАНИЯ НА ИНЦИДЕНТЫ: ИСПОЛЬЗОВАНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ДЛЯ УСКОРЕНИЯ РАССЛЕДОВАНИЯ ИНЦИДЕНТОВ, СБОРА ДОКАЗАТЕЛЬСТВ И ПРЕДОТВРАЩЕНИЯ КИБЕРАТАК

Аннотация. Статья посвящена исследованию современных тенденций и достижений в области автоматизации цифровой криминалистики и реагирования на инциденты (DFIR) с применением искусственного интеллекта (ИИ). Рассматриваются ключевые технологии и методы, используемые для повышения эффективности и скорости обработки данных, обнаружения угроз и реагирования на киберугрозы, а также выделены основные проблемы и перспективы дальнейшего развития данного направления. Особое внимание уделено вопросам качества данных, этическим аспектам и стоимости внедрения решений. В заключение подчёркиваются возможности дальнейшего улучшения методов автоматизированного реагирования на инциденты благодаря развитию технологий глубокого обучения и интеграции с облачными технологиями.

Ключевые слова: цифровая криминалистика, реагирование на инциденты, искусственный интеллект, автоматизация, кибербезопасность.

Annotation. The article is devoted to the study of current trends and achievements in the field of automation of digital forensics and incident response (DFIR) using artificial intelligence (AI). Key technologies and methods used to improve the efficiency and speed of data processing, threat detection and response to cyber threats are considered, and the main problems and prospects for further development of this area are highlighted.. Special attention is paid to the issues of data quality, ethical aspects and the cost of implementing solutions. In conclusion, the possibilities for further improvement of automated incident response methods are highlighted through the development of deep learning technologies and integration with cloud technologies.

Keywords: digital forensics, incident response, artificial intelligence, automation, cybersecurity.

Введение. Цифровая криминалистика и реагирование на инциденты (DFIR) являются критическими элементами современной кибербезопасности. По мере роста числа и сложности кибератак потребность в быстром и эффективном реагировании становится всё более актуальной. В последние годы наблюдается значительный прогресс в применении искусственного интеллекта (ИИ) и машинного обучения (МО) для автоматизации и оптимизации процессов DFIR. В настоящем исследовании рассматриваются современные тренды и достижения в области автоматизации цифровой криминалистики и реагирования на инциденты с использованием ИИ.

Что такое DFIR. Цифровая криминалистика и реагирование на инциденты (DFIR) охватывает ряд мероприятий, направленных на выявление, расследование и ликвидацию последствий кибератак. Процесс включает этапы:

- Сбор доказательств: извлечение и сохранение цифровых данных.
- Анализ: изучение собранных данных для определения характера и масштабов атаки.

- Реакция: принятие мер по ликвидации последствий и восстановлению работоспособности систем.
- Предотвращение: разработка рекомендаций по улучшению безопасности и снижению риска повторных атак.

Эти мероприятия становятся всё более сложными ввиду увеличения объёма данных и разнообразия используемых инструментов злоумышленниками. Именно здесь вступает в игру искусственный интеллект.

Технологические аспекты автоматизации DFIR. Одним из наиболее трудоемких этапов цифровой криминалистики (DFIR) является сбор цифровых доказательств. Ранее эта работа проводилась вручную специалистами, что требовало значительных временных затрат и часто сопровождалось ошибками. Сегодня благодаря развитию технологий искусственного интеллекта появилась возможность автоматизировать этот процесс. Специальные инструменты на основе нейросетей способны самостоятельно идентифицировать и сохранять значимую информацию, включая анализ журналов событий, сетевого трафика и метаданных файлов.

Следующим этапом после сбора данных становится предварительный анализ и фильтрация. Алгоритмы машинного обучения помогают классифицировать полученные сведения по разным критериям (тип файла, источник происхождения, степень важности), сокращая объем данных, подлежащих ручной обработке, и позволяя специалистам сосредоточиваться именно на ценных доказательствах.

Ключевое преимущество применения ИИ в области анализа заключается в способности быстро выявлять отклонения от нормального функционирования системы. Нейронные сети умеют распознавать подозрительные паттерны активности, предупреждая специалистов о потенциальных угрозах вроде несанкционированного увеличения объема сетевых пакетов или изменений структуры важных файлов.

Еще одной важной задачей искусственного интеллекта является объединение разнородных источников данных для построения полной картины инцидента. Система способна сопоставлять события из разных регистраторов, таких как журнал сервера, сетевые статистики и записи действий пользователей, формируя четкую последовательность происходящего и помогая найти взаимосвязи между событиями.

При обнаружении угрозы важным моментом становится своевременная реакция на нее. Современные решения с применением ИИ поддерживают функции автоматического реагирования, включающие изоляцию зараженных компонентов инфраструктуры, изменение конфигураций защиты и уведомление службы безопасности организации. Благодаря этому удается существенно сократить время реакции и минимизировать последствия кибератаки.

Кроме оперативного реагирования, технологии ИИ активно используются для долгосрочной профилактики повторных вторжений. На основании исторических данных модели строят сценарии развития будущих атак, предлагая превентивные меры по защите слабых мест инфраструктуры, например, обновление программного обеспечения или пересмотр архитектуры сетей.

Проблемы и ограничения. Несмотря на очевидные преимущества, применение технологий искусственного интеллекта (ИИ) в области цифровой криминалистики и реагирования на инциденты информационной безопасности (DFIR) сталкивается с рядом серьезных вызовов. Эффективность работы любой системы на основе ИИ напрямую зависит от качества исходных данных. Важно учитывать полноту, точность и актуальность предоставляемых данных. Если данные неполные, устаревшие или содержат ошибки, результаты, полученные системой, будут недостоверными. Это создает серьезную проблему для организаций, поскольку недостаточное внимание к подготовке данных может привести к ошибочным выводам и неправильному принятию решений. Для обеспечения высокого уровня точности аналитики важно регулярно обновлять и

очищать наборы данных, проводить их предварительную обработку и нормализацию.

Использование ИИ в цифровом расследовании и анализе безопасности вызывает ряд этических вопросов. Сбор и обработка больших объемов персональных данных ставят под угрозу конфиденциальность пользователей. Вопросы приватности становятся особенно важными, когда речь идет о сборе и обработке чувствительной информации, такой как финансовые транзакции, медицинские записи или другие личные сведения. Организации обязаны обеспечивать соблюдение законов о защите данных и избегать несанкционированного доступа к личной информации. Возникают проблемы законности методов сбора и обработки данных. Автоматический мониторинг поведения сотрудников внутри организации может нарушать права человека на частную жизнь и свободу выражения мнений. Компании должны внедрять четкую политику управления персональными данными и информировать всех заинтересованных лиц о целях и методах обработки данных.

Создание и внедрение эффективных систем на основе ИИ требует значительных инвестиций. Затраты включают приобретение необходимого оборудования, разработку программного обеспечения, обучение персонала и поддержку инфраструктуры. Высокие требования к вычислительным ресурсам, памяти и пропускной способности сети также увеличивают расходы компаний. Особенно остро эта проблема стоит перед малыми и средними предприятиями, которым сложно конкурировать с крупными корпорациями в этой сфере. Помимо капитальных затрат, организациям требуются высококвалифицированные специалисты для разработки, настройки и сопровождения интеллектуальных систем. Найти и удержать талантливых профессионалов в области ИИ становится сложной задачей, учитывая дефицит специалистов и высокую стоимость их услуг. Эти факторы существенно ограничивают доступ малых предприятий к современным технологиям ИИ и создают неравенство возможностей среди игроков рынка.

Одним из основных ограничений современных технологий ИИ является непредсказуемость результатов при работе с нестандартными ситуациями. Многие модели машинного обучения требуют большого количества примеров и известных паттернов для эффективного распознавания угроз. Реальные атаки часто отличаются новизной и уникальностью, что затрудняет выявление аномалий традиционными методами. Эксперты отмечают необходимость постоянного участия человека в процессе расследования и принятия решений. Даже самые продвинутые алгоритмы нуждаются в регулярной калибровке и доработке специалистами. Без человеческого контроля эффективность технологии снижается, а риск пропуска критически важных сигналов возрастает. Несмотря на значительные успехи в развитии ИИ-технологий, пока невозможно полностью исключить человеческий фактор из процесса обнаружения и предотвращения кибератак.

Перспективы развития. Будущее автоматизации DFIR связано с дальнейшим развитием технологий ИИ и интеграцией их в повседневные практики предприятий. Среди перспективных направлений:

- Интерактивные помощники: создание интерактивных интерфейсов, позволяющих пользователям взаимодействовать с системой через голосовые запросы или графические интерфейсы.
- Самообучающиеся системы: дальнейшее совершенствование механизмов самообучения, позволяющих ИИ самостоятельно улучшать свою производительность на основе опыта.
- Совместимость с облачными сервисами: интеграция с облачными платформами обеспечит гибкость и доступность решений для широкого круга пользователей.

Заключение. Автоматизация цифровой криминалистики и реагирования на инциденты с использованием искусственного интеллекта является важнейшей составляющей современного подхода к обеспечению кибербезопасности.

Применение ИИ позволяет значительно ускорить процессы сбора и анализа данных, повысить точность выявления угроз и снизить ущерб от инцидентов. Вместе с тем остаются нерешёнными проблемы, связанные с качеством данных, этикой и стоимостью внедрения. Дальнейшее развитие технологий обещает сделать эти процессы ещё более эффективными и надёжными.

Использованные источники:

1. Цифровая криминалистика и реагирование на инциденты (DFIR). Сервис BAILRY. (2025). URL: https://www.bailry.com/ru/blog/72.html

2. Платонов, А. Е. Разработка алгоритма выявления аномалий в трафике на основе дампа / А. Е. Платонов, М. М. Ковцур, И. А. Ушаков // Региональная информатика и информационная безопасность : Сборник трудов Санкт-Петербургской международной конференции и Санкт-Петербургской межрегиональной конференции, Санкт-Петербург, 23–25 октября 2024 года. – Санкт-Петербург: Санкт-Петербургское Общество информатики, вычислительной техники, систем связи и управления, 2024. – С. 590-592. – EDN SRMVIV.

3. ИИ на страже кибербезопасности: как нейросети защищают от хакеров. KEDU. (2025). URL: https://kedu.ru/press-center/articles/info-it-ii-na-strazhe-kiberbezopasnosti-kak-neyroseti-zashchishchayut-ot-khakerov

4. Нейросети и безопасность данных: Инновационные решения для защиты информации. Everest Solution. (2025). URL: https://everest-solution.com/articles/nejroseti-i-bezopasnost-dannyh

5. Борисов, В. И. Исследование влияния особенностей отдельных этапов кибератаки при построении последовательностей атакующих техник в рамках проактивного реагирования на события безопасности / В. И. Борисов, Е. В. Федорченко // Актуальные проблемы инфотелекоммуникаций в науке и

образовании (АПИНО 2023) : Сборник научных статей XII Международной научно-технической и научно-методической конференции. В 4-х томах, Санкт-Петербург, 28 февраля – 01 2023 года / Под редакцией С.И. Макаренк, сост. В.С. Елагин, Е.А. Аникевич. Том 2. – Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2023. – С. 350-353. – EDN PDSZFR.

6. Виткова, Л. А. Автоматизация выявления уязвимостей информационной безопасности / Л. А. Виткова, Р. Р. Исмаилов, М. А. Пепп // Актуальные проблемы инфотелекоммуникаций в науке и образовании : Сборник научных статей XIII Международной научно-технической и научно-методической конференции в 4 т., Санкт-Петербург, 27–28 февраля 2024 года. – Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2024. – С. 186-189. – EDN LUITFM.