УДК 004

Шайнурова А.Г.
Уфимский университет науки и технологий, Уфа

Научный руководитель:
Шагапов И.А.
Уфимский университет науки и технологий, Уфа

РАССЛЕДОВАНИЕ ИНЦИДЕНТОВ С ПОМОЩЬЮ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Аннотация. Расследование инцидентов информационной безопасности с помощью искусственного интеллекта становится важным инструментом при решении задач защиты информации. В статье рассмотрены некоторые подходы при расследовании инцидентов информационной безопасности с помощью искусственного интеллекта, а также этапы проведения данного типа расследований.

Ключевые слова: информация, информационная безопасность, инциденты информационной безопасности, искусственный интеллект.

В эпоху цифровизации информация приобрела статус важнейшего актива, обеспечение информационной безопасности (ИБ) которой выдвигается на важное место в деятельности организации. Но оперативное и безошибочное определение инцидентов в сфере кибербезопасности предполагает обработку огромных массивов данных. В настоящее время искусственный интеллект (ИИ) может помочь в данном вопросе и предоставить эффективные средства для автоматизации и улучшения процесса расследования инцидентов ИБ. Более того, ИИ способен прогнозировать вероятные угрозы и разрабатывать защитные стратегии. Так, автоматизированные системы контроля и анализа данных с применением ИИ могут оперативно обнаруживать нетипичную активность в сетевой среде и сигнализировать о потенциальной опасности.

На данный момент искусственный интеллект способствует автоматизации этапа анализа и выявления угроз при расследовании инцидентов ИБ, применяя методы машинного обучения для анализа обширных объемов данных, таких как сетевой трафик, журналы серверов, электронные почты и прочие источники. Благодаря алгоритмам

машинного обучения, ИИ способен выявлять аномалии и нестандартную активность в сети, устанавливать взаимосвязи между различными событиями и идентифицировать возможные угрозы [1]. Также, ИИ может быть использован для формирования профилей пользователей и определения типовых моделей поведения, что позволяет выявлять отклонения и предотвращать потенциальные атаки злоумышленников еще до их реализации. В целом, автоматизация процессов анализа и выявления угроз в ходе расследования инцидентов значительно повышает результативность работы специалистов по информационной безопасности и обеспечивает более надежную защиту от угроз [2].

Этапы расследования инцидентов ИБ с использованием ИИ могут включать в себя:

1. Сбор и анализ данных. ИИ может помочь в этом процессе, используя алгоритмы машинного обучения для выявления аномалий и закономерностей в данных. Методами анализа данных может являться машинное обучение, анализ сетевого трафика и др.

2. Обнаружение угроз. ИИ может использоваться для мониторинга и анализа различных источников данных, включая журналы событий, сетевой трафик и поведение пользователей для выявления потенциальных угроз и уязвимостей.

3. Реагирование на инцидент. ИИ может автоматически инициировать процессы реагирования, такие как изоляция зараженных узлов, блокировка учетных записей и восстановление резервных копий. Основные шаги реагирования на инцидент: изоляция зараженного узла; блокировка учетных записей; восстановление резервных копий; уведомление заинтересованных сторон об инциденте ИБ.

4. Глубокий анализ и прогнозирование. ИИ может помочь в определении причины инцидента, его последствий и возможных мер профилактики.

5. Профилактика и улучшение мер безопасности. Полученные знания используются для улучшения общей стратегии безопасности организации. ИИ может предложить рекомендации по улучшению политики безопасности, настройке систем защиты и обучению сотрудников [3].

Для создания системы предотвращения инцидентов ИБ с применением искусственного интеллекта необходимо собирать и обрабатывать обширные массивы информации об инцидентах и слабых местах в защите информации. Эти сведения служат основой для обучения алгоритмов машинного обучения, способных анализировать и выявлять закономерности в подобных атаках. В дальнейшем, система использует накопленные знания для прогнозирования вероятных атак и разработки защитных стратегий. Специалисты в области информационной безопасности могут опираться на эти модели для определения наиболее актуальных угроз и принятия упреждающих мер. Более того, система способна автоматически обнаруживать и блокировать данные инциденты. Алгоритмы машинного

обучения анализируют данные о поведении пользователей и параметрах безопасности, автоматически реагируя на выявление подозрительной деятельности. Система для расследования инцидентов ИБ должна обладать интегрированным и многофункциональным характером, охватывая следующие возможности:

– отслеживание сетевого трафика и визуализация сетевой активности: выявление и анализ всех сетевых операций с целью обнаружения аномалий или потенциальных угроз, а также предоставление графического отображения трафика в сети с выделением уязвимых зон для оперативного обнаружения рисков;

– анализ рисков: предварительная оценка угроз с применением технологий искусственного интеллекта;

– оповещение на ранней стадии появления угроз: распознавание типичных или повторяющихся угроз с использованием анализа данных и машинного обучения для превентивных мер;

– активная и актуальная защита информации: обеспечение адаптации состояния безопасности в зависимости от текущей ситуации;

– оперативное расследование инцидентов: оценка и отчетность по инцидентам, их детальное расследование и предоставление полной информации для принятия мер и усиления защиты сети.

Одним из решений, позволяющим проводить расследования инцидентов с применением ИИ, является KIRA (Kaspersky Investigation and Response Assistant). Это специализированная платформа, разработанная компанией «Лаборатория Касперского», предназначенная для автоматизированного расследования инцидентов информационной безопасности. Она сочетает в себе передовые технологии искусственного интеллекта и экспертные знания специалистов по информационной безопасности, обеспечивая эффективное и быстрое реагирование на инциденты. KIRA способна автоматически обрабатывать большие объемы лог-файлов, выявляя подозрительные события и аномалии. Платформа поддерживает различные форматы лог-файлов, включая Syslog, Windows Event Logs и другие стандартные форматы. Платформа оснащена интерфейсами для интеграции моделей машинного обучения, позволяющими настраивать и применять собственные аналитические модели для конкретных сценариев. KIRA предоставляет возможность настройки платформы под специфику каждого клиента, позволяя добавлять уникальные сценарии и правила для детекции инцидентов. Интерфейс KIRA интуитивно понятен и удобен для пользователей различного уровня подготовки. Даже начинающие специалисты могут эффективно использовать платформу благодаря встроенным подсказкам и инструкциям. KIRA поддерживает стандарты обмена информацией об угрозах (STIX/TAXII), что упрощает интеграцию с внешними системами управления информацией и событиями безопасности (SIEM) [4].

Технологии искусственного интеллекта значительно улучшают выявление угроз ИБ, осуществляя анализ больших массивов данных и распознавая трудноуловимые взаимосвязи. Эти системы способны идентифицировать вредоносное программное обеспечение, даже если оно замаскировано сложным шифрованием. Автоматизированное реагирование на выявленные угрозы не только ускоряет процесс, но и облегчает работу специалистов по безопасности. Прогнозирование возможных атак и своевременное принятие мер предосторожности позволяют предотвратить их возникновение. Помимо этого, искусственный интеллект способствует более эффективному расследованию инцидентов, устанавливая взаимосвязи между различными событиями и автоматизируя процесс анализа отчетной документации.

Список использованных источников:

1. Исмагилова А.С. Комплексная биометрическая аутентификация пользователей информационной системы с применением нейронных сетей / А.С. Исмагилова, Н.Д. Лушников // Инженерный вестник Дона. 2024. № 1(109). С. 178–188.

2. Жданов А.А. Автономный искусственный интеллект: учебное пособие / А.А. Жданов. 5-е изд. (эл.). М.: Лаборатория знаний, 2024. 362 с. Электрон. версия. URL: https://e.lanbook.com/book/387629 (дата обращения: 20.04.2025).

3. Кацов, И. Искусственный интеллект на предприятии: руководство / И. Кацов; перевод с англ. В.С. Яценкова. М.: ДМК Пресс, 2024. 710 с. Электрон. версия. URL: https://e.lanbook.com/book/456725 (дата обращения: 20.04.2025).

4. Терлецкий А.С. Нейронные сети и искусственный интеллект: основы нейронных сетей на языке Python: учебно-методическое пособие / А.С. Терлецкий, Е.С. Терлецкая. Липецк: Липецкий ГПУ, 2023. 76 с. Электрон. версия. URL: https://e.lanbook.com/book/439343 (дата обращения: 20.04.2025).

Shaynurova A.G.
Ufa University of Science and Technology, Ufa

Scientific supervisor:
Shagapov I.A.
Ufa University of Science and Technology, Ufa

INVESTIGATION OF INCIDENTS USING ARTIFICIAL INTELLIGENCE

Abstract. Investigation of information security incidents using artificial intelligence is becoming an important tool in solving information security

problems. The article discusses some approaches to investigating information security incidents using artificial intelligence, as well as the stages of conducting this type of investigation.

Keywords: information protection rights, information security, information security incidents, artificial intelligence.