DOI 10.37882/2223-2966.2025.05-2.20

СОВРЕМЕННЫЕ ПОДХОДЫ К АНАЛИЗУ ТЕКСТОВОЙ ИНФОРМАЦИИ О СОБЫТИЯХ БЕЗОПАСНОСТИ НА ОСНОВЕ МЕТОДОВ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

MODERN APPROACHES TO THE ANALYSIS OF TEXTUAL INFORMATION ABOUT SECURITY EVENTS BASED ON ARTIFICIAL INTELLIGENCE METHODS

A. Rusakov
K. Komarov
S. Koryagin
V. Koryagina

Summary. In the context of the rapid growth of text information volumes, intelligent data analysis is becoming a key tool for processing and structuring information about vulnerabilities of information systems. This paper discusses methods for automating the analysis of text descriptions of vulnerabilities using artificial intelligence and machine learning technologies. The relevance of the study is due to the growth of cyber threats, especially after the COVID-19 pandemic, when the mass transition to remote work led to an increase in the number of attacks on government and commercial structures. In Russia, a number of regulations have been adopted to counter these threats, including Federal Law No. 187-FZ and FSTEC methods, but vulnerability analysis still requires significant time due to manual data processing. The article provides an overview of modern vulnerability description systems (CVE, CWE, NVD), methods for their classification, as well as approaches to automated processing of text data using software libraries and machine learning algorithms, and attention is also paid to reducing the size of the data and visualizing the results. The results of the study show that the use of text mining allows for faster and more accurate processing of vulnerability descriptions, which contributes to more effective cyber risk management.

Keywords: information security events, text mining, artificial intelligence methods.

Русаков Алексей Михайлович
старший преподаватель, МИРЭА — Российский технологический университет.
rusakov_a@mirea.ru
Комаров Кирилл Юрьевич
МИРЭА — Российский технологический университет
kk7453603@gmail.com
Корягин Сергей Викторович
к.т.н. доцент,
МИРЭА — Российский технологический университет
dongenealog2003@mail.ru
Корягина Вероника Михайловна
МИРЭА — Российский технологический университет
koryagina.v.m@edu.mirea.ru

Аннотация. В условиях стремительного роста объемов текстовой информации интеллектуальный анализ данных становится ключевым инструментом для обработки и структурирования сведений об уязвимостях информационных систем. В статье рассматриваются методы автоматизации анализа текстовых описаний уязвимостей с применением технологий искусственного интеллекта и машинного обучения. Актуальность исследования обусловлена ростом киберугроз, особенно после пандемии COVID-19, когда массовый переход на удалённую работу привёл к увеличению числа атак на государственные и коммерческие структуры. В России для противодействия этим угрозам принят ряд нормативных актов, включая Федеральный закон №187-ФЗ и методики ФСТЭК, однако анализ уязвимостей по-прежнему требует значительных временных затрат из-за ручной обработки данных. В статье проведён обзор современных систем описания уязвимостей (CVE, CWE, NVD), методов их классификации, а также подходов к автоматизированной обработке текстовых данных с использованием программных библиотек и алгоритмов машинного обучения, также внимание уделено снижению размерности данных и визуализации результатов. Результаты исследования показывают, что применение интеллектуального анализа текстов позволяет ускорить и повысить точность обработки описаний уязвимостей, что способствует более эффективному управлению киберрисками.

Ключевые слова: события информационной безопасности, интеллектуальный анализ текстов, методы искусственного интеллекта.

Введение

В условиях интенсивного развития информационных технологий и цифровизации всех сфер жизнедеятельности общества проблема обеспечения информационной безопасности становится одной из наиболее острых и актуальных. Количество кибератак ежегодно стремительно растет, а их сложность постоянно увеличивается, что требует от организаций применения передовых решений для своевременного обнаружения и эффективного реагирования на инциденты информационной безопасности.

Традиционные подходы к мониторингу и анализу событий безопасности, основанные на статических правилах и сигнатурах, зачастую оказываются недостаточно эффективными перед лицом эволюционирующих угроз. В связи с этим актуальной задачей является разработка

интеллектуальных систем, способных оперативно выявлять, анализировать и классифицировать события безопасности с применением современных методов искусственного интеллекта. Искусственный интеллект (ИИ), включая машинное обучение и глубокое обучение, предоставляет мощные инструменты для автоматизации процессов выявления угроз, анализа инцидентов и прогнозирования атак. Использование таких подходов позволяет существенно повысить точность обнаружения угроз, сократить время реагирования на инциденты и снизить нагрузку на специалистов по безопасности.

Концепция SIEM систем

Системы мониторинга событий и управления инцидентами безопасности (Security Information and Event Management, SIEM) являются ключевым компонентом современной инфраструктуры кибербезопасности. Такие системы предназначены для централизованного сбора, хранения и анализа данных о событиях безопасности из различных источников информации в корпоративной сети.

Назначение SIEM систем

SIEM-системы обеспечивают сбор событий безопасности, их агрегацию и фильтрацию, анализ на основании правил (корреляцию), мониторинг, расследование и вывод результатов в требуемом формате. По данным исследований, без использования SIEM среднее время обнаружения вторжения может составлять десятки или даже сотни дней, тогда как время, необходимое для компрометации инфраструктуры, сокращается до часов и минут, об этом говориться в статье [1].

Основные функции современных SIEM-систем включают:

- Сбор и консолидацию событий из различных источников (сетевые устройства, серверы, средства защиты).
- Нормализацию событий (приведение к единому формату).
- Корреляцию событий для выявления инцидентов безопасности.
- Оповещение о выявленных инцидентах.
- Визуализацию и формирование отчетов.
- Хранение событий для последующего анализа и расследования.

Тем не менее традиционные SIEM-системы сталкиваются с рядом ограничений при работе с современными сложными угрозами. Как отмечается в статье [2], организации сталкиваются с проблемами большого количества ложных срабатываний правил регистрации инцидентов информационной безопасности (ИБ), отсутствием классификации инцидентов и сложностями приоритизации. SIEM регистрирует инциденты ИБ, но часто не выявляет взаимосвязь между ними и не позволяет раскрыть заранее спланированные сценарии кибератак.

Правила корреляции, являющиеся основным механизмом выявления инцидентов в традиционных SIEM-системах, имеют следующие ограничения:

- Большое количество ложных срабатываний, обработка которых перегружает аналитиков и мешает выявлять реальные угрозы, об этом упоминается в статье [3].
- Несоответствие некоторых атак правилам корреляции, из-за чего специалисты могут их не заметить.
- Изолированный анализ событий (без учета контекста), который снижает эффективность правил.

Учитывая эти ограничения, логичным шагом в развитии SIEM-систем является внедрение методов искусственного интеллекта и машинного обучения. Эти технологии позволяют преодолеть указанные недостатки за счет адаптивного анализа данных, выявления аномалий и прогнозирования угроз на основе исторических данных.

Методы корреляции событий безопасности в SIEM-системах

Корреляция событий безопасности является одним из ключевых процессов в SIEM-системах, позволяющим выявлять сложные инциденты безопасности путем установления взаимосвязей между отдельными событиями. Традиционные методы корреляции основаны на заранее определенных правилах и шаблонах, что делает их эффективными для обнаружения известных угроз, но ограниченными в условиях появления новых или модифицированных атак.

Процесс корреляции событий безопасности включает несколько этапов:

1. Сбор событий из различных источников.
2. Нормализация событий (приведение к единому формату).
3. Агрегация (объединение похожих событий).
4. Применение правил корреляции для выявления инцидентов.
5. Формирование оповещений о выявленных инцидентах.

Как отмечается в статье [4], процесс корреляции рассматривается как многоуровневая иерархия этапов, где каждый этап выполняет определенные операции с данными безопасности. Такой подход позволяет структурировать процесс и повысить его эффективность за счет последовательной обработки информации.

Современные методы корреляции событий безопасности можно классифицировать по различным призна-

кам. В зависимости от используемых алгоритмов и подходов выделяют следующие основные категории:

Правило-ориентированные методы

Эти методы используют заранее определенные правила для выявления связей между событиями. Правила создаются экспертами на основе знаний о типичных сценариях атак и могут быть эффективными для обнаружения известных угроз. Однако, как указывается в статье [5], такие методы имеют ограничения при работе с новыми или модифицированными типами атак, а также могут генерировать большое количество ложных срабатываний.

Статистические методы

Статистические подходы анализируют частоту и распределение событий для выявления аномалий, которые могут указывать на инциденты безопасности. Эти методы более гибкие по сравнению с правило-ориентированными, но требуют значительных вычислительных ресурсов и тщательной настройки для минимизации ложных срабатываний.

Методы на основе графов событий

В данном подходе события и их взаимосвязи представляются в виде графа, что позволяет анализировать сложные сценарии атак через изучение структуры графа. Как отмечается в статье [6], эти методы особенно эффективны для выявления многошаговых атак, но их применение ограничено высокой вычислительной сложностью при обработке больших объемов данных.

Методы на основе машинного обучения

Использование алгоритмов машинного обучения позволяет анализировать большие объемы данных и выявлять скрытые закономерности, которые могут указывать на угрозы. Такие методы способны адаптироваться к новым типам атак, но требуют значительных усилий для обучения моделей и подготовки данных.

Таким образом, современные SIEM-системы все чаще интегрируют методы искусственного интеллекта, включая машинное обучение, чтобы преодолеть ограничения традиционных подходов к корреляции событий безопасности. Это позволяет не только повысить точность обнаружения инцидентов, но и сократить время реакции на них.

Механизмы агрегации, нормализации и обогащения данных

Эффективная обработка событий безопасности требует применения механизмов агрегации, нормализации и обогащения данных. Эти процессы являются критически важными для повышения качества и информативности собираемых данных.

Агрегация данных

Агрегация данных включает в себя объединение нескольких одинаковых событий в одно для уменьшения количества «мусора» в логах. Это особенно эффективно для логов межсетевых экранов и веб-серверов. В результате агрегации значительно уменьшается объем данных, которые необходимо хранить и анализировать, что повышает производительность SIEM-системы и упрощает работу аналитиков.

Агрегация может выполняться на основе различных признаков событий, таких как IP-адреса источника и назначения, порты, типы событий, временные метки и др. События, имеющие одинаковые значения выбранных признаков, объединяются в одно событие с указанием количества повторений.

Нормализация данных

Нормализация данных необходима для приведения данных к единому формату, что упрощает их обработку и анализ. События, поступающие из различных источников, имеют разный формат и содержат разные поля, что затрудняет их совместный анализ. Нормализация позволяет решить эту проблему, приводя все события к единому формату с определенным набором полей.

В работе [7] авторы определяют нормализацию как фундаментальную функцию SIEM-систем, обеспечивающую мониторинг и анализ событий безопасности в режиме реального времени. Процесс нормализации должен учитывать специфику каждого источника данных, что представляет особую сложность при интеграции разнородных систем. Правила корреляции строятся на основе нормализованных событий, что напрямую влияет на точность правил корреляции. Корректная нормализация позволяет более точно выявлять связи между событиями и повышает эффективность работы SIEM-системы в целом.

Обогащение данных

Обогащение данных включает в себя добавление дополнительной информации из внешних источников, таких как базы данных угроз, для повышения точности анализа. Это позволяет оперативно реагировать на новые виды атак и повышает эффективность выявления инцидентов безопасности.

В процессе обогащения к данным о событиях безопасности добавляется контекстная информация, как со-

бытийная, так и не событийная, с целью преобразования исходных данных в содержательные. События безопасности могут быть обогащены контекстной информацией из справочников пользователей, средств инвентаризации активов (например, CMDB), средств геолокации, сторонних баз данных анализа угроз и множества других источников, подробнее о важности обогащения данных можно узнать в источнике. Обогащенные данные позволяют SIEM более эффективно выполнять обнаружение угроз, поиск угроз и реагирование на инциденты. Использование обогащенных данных делает борьбу с угрозами безопасности более простой и эффективной.

Применение методов искусственного интеллекта в анализе событий безопасности

Современные SIEM-системы всё чаще интегрируют технологии искусственного интеллекта для повышения эффективности обнаружения и предотвращения угроз. В работе Котенко И.В. [7] отмечается, что применение методов ИИ позволяет автоматизировать процессы анализа больших объёмов данных и выявления сложных зависимостей между событиями безопасности. Это особенно актуально в контексте растущего объёма генерируемых данных и усложнения векторов атак.

Методы машинного обучения для обнаружения аномалий

Для выявления аномального поведения в сетевом трафике и действиях пользователей применяются различные методы машинного обучения. Как показано в исследовании Котенко И.В. и Левшуна Д.А. [7], эти методы можно классифицировать на три основные категории: обучение с учителем, без учителя и с частичным привлечением экспертных знаний. Каждый из этих подходов имеет свои преимущества и ограничения при применении к задачам информационной безопасности.

Методы обучения без учителя не требуют предварительной разметки данных, что делает их особенно ценными для обнаружения ранее неизвестных типов атак. В работе [7] подчёркивается, что алгоритмы кластеризации, такие как k-means и DBSCAN, позволяют эффективно группировать события безопасности по схожим признакам, выявляя аномальные кластеры. Иерархический кластерный анализ (HCA), детально описанный в том же исследовании, динамически формирует кластеры на основе IP-адресов, временных меток и типов действий, что позволяет адаптироваться к изменяющемуся характеру угроз.

Авторы [7] доказывают, что методы поиска ассоциативных правил выявляют скрытые зависимости между атрибутами событий безопасности, что критически важно для построения комплексной картины атаки. Там же демонстрируется, что алгоритмы понижения размерности, такие как PCA и t-SNE, повышают эффективность визуализации и анализа многомерных данных о событиях безопасности, сокращая вычислительные затраты без значительной потери информативности.

Алгоритмы обучения с учителем, такие как Random Forest (RF) и Support Vector Machine (SVM), требуют наличия размеченных наборов данных, но обеспечивают высокую точность классификации известных типов атак. В исследовании [8] показано, что ансамблевые методы на основе деревьев решений достигают точности до 97 % при выявлении DDoS-атак на корпоративные ресурсы. Там же отмечается, что SVM с нелинейными ядрами эффективен при классификации сложных типов атак с пересекающимися признаковыми пространствами.

Выбор конкретного метода машинного обучения должен осуществляться с учётом специфики задачи и доступных ресурсов. Как подчёркивается в [7], для линейно разделимых классов атак и небольших объёмов данных оптимальным является применение классических алгоритмов, таких как логистическая регрессия и SVM. В то же время, в работе [7] демонстрируется, что для сложных нелинейных зависимостей и больших массивов данных предпочтительно использование методов глубокого обучения, способных автоматически извлекать информативные признаки из сырых данных.

Методы обнаружения многошаговых кибератак

Многошаговые кибератаки представляют особую сложность для обнаружения, поскольку отдельные этапы могут выглядеть как легитимные действия. Проблема усугубляется тем, что этапы атаки могут быть разнесены во времени и исходить от различных источников. В исследовании [17] предложена методология выявления таких атак на основе построения графов зависимостей между событиями безопасности. Авторы демонстрируют, что графовое представление позволяет устанавливать причинно-следственные связи между разрозненными событиями, восстанавливая полную картину атаки.

Рекуррентные нейронные сети (RNN) с механизмом долгой краткосрочной памяти (LSTM) рассматриваются в работе [7] как эффективный инструмент анализа временных последовательностей событий безопасности. Авторы показывают, что архитектура Bi-LSTM с механизмом внимания позволяет учитывать как предшествующий, так и последующий контекст событий, что критически важно для выявления растянутых во времени атак. Экспериментальная оценка на наборе данных DARPA 2000 демонстрирует превосходство этого подхода над традиционными методами.

В том же исследовании [7] предложена комбинированная архитектура на основе сверточных нейронных

сетей (CNN) и авторегрессионных моделей для анализа последовательностей событий безопасности. Авторы демонстрируют, что такой подход позволяет эффективно выявлять локальные и глобальные паттерны в данных, достигая точности 93 % при обнаружении APT-атак на корпоративные ресурсы.

Как отмечается в работе [7], увеличение числа слоёв в глубоких нейронных сетях приводит к повышению полноты обнаружения атак, что особенно ценно при работе с ранее неизвестными типами угроз. Автор предлагает адаптивную архитектуру, способную динамически изменять свою глубину в зависимости от сложности анализируемых данных, что позволяет оптимизировать вычислительные ресурсы при сохранении высокой точности обнаружения.

Трансформерные архитектуры, представленные в исследовании [9], демонстрируют высокую эффективность при анализе длинных последовательностей событий безопасности. Автор показывает, что механизм самовнимания позволяет устанавливать связи между удалёнными во времени событиями, что критически важно для выявления многошаговых атак с большими временными интервалами между этапами.

Прогностическая аналитика для предсказания угроз

Прогностическая аналитика использует исторические данные о событиях безопасности для предсказания вероятности возникновения инцидентов в будущем. В работе [10] представлена методология прогнозирования кибератак на основе анализа временных рядов с применением авторегрессионных моделей интегрированного скользящего среднего (ARIMA). Автор демонстрирует, что данный подход позволяет выявлять сезонные паттерны в активности злоумышленников и прогнозировать всплески атак определённого типа.

Модели глубокого обучения для прогнозирования рассматриваются в исследовании [11], где предложена архитектура Temporal Fusion Transformers (TFT) для анализа многомерных временных рядов событий безопасности. Автор показывает, что TFT эффективно обрабатывает как внутренние зависимости в данных, так и внешние факторы, такие как информация об уязвимостях и глобальных киберугрозах. Экспериментальная оценка демонстрирует точность прогнозирования DDoS-атак на уровне 87 % с горизонтом до 7 дней.

Федеративное обучение с гомоморфным шифрованием, описанное в работе [7], позволяет обучать модели прогнозирования на распределённых наборах данных без нарушения конфиденциальности. Это особенно важно в контексте межорганизационного обмена информацией об угрозах, где прямая передача данных о событиях безопасности может быть нежелательна по юридическим или коммерческим причинам.

Для интерпретации результатов прогнозирования ключевыми становятся методы объяснимого искусственного интеллекта. В исследовании [12] представлено применение методов SHAP (SHapley Additive exPlanations) и LIME (Local Interpretable Model-agnostic Explanations) для визуализации вклада различных факторов в прогноз кибератак. Автор демонстрирует, что эти подходы повышают доверие аналитиков к результатам работы моделей и позволяют выявлять ключевые индикаторы компрометации.

Графовые нейронные сети (GNN), интегрированные в архитектуру MDSTFT (Multi-Dimensional Spatio-Temporal Fusion Transformer), позволяют анализировать пространственно-временные зависимости в цепочках событий безопасности, как показано в работе [13]. Авторы демонстрируют, что данный подход снижает ошибку прогноза целевых атак на 22 % по сравнению с классическими LSTM-моделями за счёт учёта топологической структуры корпоративной сети.

Интеграция методов ИИ в практические решения

Эффективное внедрение методов искусственного интеллекта в SIEM-системы требует решения ряда практических задач. В исследовании [10] рассматриваются подходы к оптимизации вычислительных ресурсов при обработке больших объёмов данных о событиях безопасности. Автор предлагает методологию распределённых вычислений на основе фреймворка Apache Spark, позволяющую масштабировать алгоритмы машинного обучения при сохранении высокой скорости обработки.

Проблема недостатка размеченных данных для обучения моделей решается с помощью методов полуавтоматической разметки и активного обучения. В работе [14] представлен подход к формированию репрезентативных наборов данных для обучения моделей выявления атак с минимальными затратами на ручную разметку. Авторы демонстрируют, что активное обучение с использованием метрики неопределённости позволяет сократить объём ручной разметки на 67 % при сохранении высокой точности классификации.

Интеграция экспертных знаний в модели машинного обучения рассматривается в исследовании [7], где предложен нейросимволический подход к анализу событий безопасности. Автор показывает, что комбинирование статистических методов с формализованными правилами, основанными на экспертных знаниях, позволяет существенно снизить количество ложных срабатываний и повысить интерпретируемость результатов.

В контексте критической информационной инфраструктуры особую важность приобретает устойчивость моделей к состязательным воздействиям. В работе [15] исследуются методы повышения робастности алгоритмов машинного обучения к атакам на данные и модели. Автор демонстрирует, что применение методов состязательного обучения и ансамблевых подходов позволяет значительно повысить устойчивость систем обнаружения вторжений к целенаправленным атакам на компоненты искусственного интеллекта.

Перспективные направления развития

Анализ текущего состояния и тенденций развития методов искусственного интеллекта в кибербезопасности позволяет выделить несколько перспективных направлений исследований. В работе [7] рассматривается концепция непрерывного обучения (Continual Learning) для адаптации моделей к эволюционирующим угрозам. Автор предлагает архитектуру, способную инкрементально обновлять свои знания без катастрофического забывания ранее изученных паттернов атак.

Интеграция мультимодальных данных (сетевой трафик, журналы событий, метрики производительности) рассматривается в исследовании [16] как способ повышения контекстной осведомлённости систем безопасности. Авторы демонстрируют, что объединение разнородных источников данных с помощью специализированных нейросетевых архитектур позволяет выявлять сложные взаимосвязи и повышать точность обнаружения угроз на 28%.

В контексте автоматизации реагирования на инциденты особую значимость приобретают методы обучения с подкреплением. В работе [7] представлен подход к оптимизации стратегий реагирования на основе глубокого Q-обучения (Deep Q-Learning). Автор показывает, что данный метод позволяет системе самостоятельно вырабатывать оптимальные последовательности действий для нейтрализации различных типов угроз, адаптируясь к изменяющимся условиям функционирования защищаемой системы.

Современные тенденции в развитии SIEM-систем с использованием искусственного интеллекта: новое поколение систем мониторинга

Современные SIEM-системы активно эволюционируют в направлении интеграции методов искусственного интеллекта для повышения эффективности выявления и анализа инцидентов безопасности. Как отмечается в исследовании Котенко И.В. и соавторов в статье [18], технологии искусственного интеллекта трансформируют традиционные SIEM-решения, создавая новый класс систем мониторинга — AI-SIEM. Эти системы выходят за рамки классических, основанных на правилах фреймворков, предлагая значительно более эффективные механизмы обнаружения угроз, прогнозную аналитику и автоматизированные процессы реагирования.

Согласно результатам исследования [19], современные AI-SIEM включают шесть ключевых компонентов:

1. Продвинутая обработка гетерогенных данных
2. Интеграция с источниками больших данных (Big Data)
3. Распознавание сложных паттернов атак
4. Автоматизированный анализ с минимальным участием человека
5. Прогностическая аналитика на основе исторических данных
6. Интеллектуальные механизмы реагирования

Интеграция ИИ в SIEM-системы позволяет эффективно решать проблему растущей сложности и объема киберугроз, делая кибербезопасность более проактивной и интеллектуальной. В работе [20] авторы демонстрируют, что применение технологий машинного обучения в SIEM повышает точность выявления целевых атак по сравнению с традиционными правило-ориентированными системами.

Сервисная модель и облачные SIEM-решения

Отчетливой тенденцией в развитии современных SIEM-систем становится переход к облачным решениям и сервисным моделям предоставления услуг. Исследование [21] показывает, что классический подход к работе с SIEM требует существенных инвестиций со стороны организаций на покупку длительных лицензий и внедрение продукта, при этом эти инвестиции необходимо регулярно повторять при изменениях инфраструктуры.

В противовес этому, современные компании стремятся повышать свою устойчивость и адаптируемость к изменениям, что характеризуется следующими запросами:

- Ориентация на оплату за фактическое потребление (Pay-as-you-go)
- Делегирование все большего объема работ подрядчикам для фокусирования на основном бизнесе
- Возможность динамически менять объемы потребления ресурсов
- Масштабируемость без дополнительных капитальных затрат

Авторы работы [22] отмечают, что модели Managed SIEM и SIEM-as-a-Service становятся все более популярными, особенно среди организаций с ограниченными ресурсами на поддержание собственного центра мониторинга безопасности (SOC). Такой подход позволяет компаниям получить доступ к передовым технологиям мониторинга событий безопасности без необходимости

содержать штат высококвалифицированных специалистов.

Расширенная автоматизация и конвергенция с координацией

Третьей значимой тенденцией в развитии SIEM-систем является интеграция функциональности систем автоматизации и оркестрации безопасности (Security Orchestration, Automation and Response, SOAR). Авторы исследования [23] подчеркивают, что эта тенденция продиктована объективной необходимостью целостного решения задач обеспечения информационной безопасности. Заказчики отталкиваются от процесса работы, а не от набора функций, описанных в отчетах аналитических агентств, и разделение возможностей обнаружения и реагирования между несколькими отдельными продуктами противоестественно с точки зрения практического использования.

В работе [12] демонстрируется, что интеграция функций SOAR в SIEM-системы позволяет решить две ключевые проблемы:

1. Сократить время реагирования на инциденты благодаря автоматизации рутинных операций
2. Повысить эффективность работы аналитиков за счет уменьшения числа ложных срабатываний и более точной приоритизации событий

Экспериментальные результаты, представленные в исследовании [24] показывают, что применение комбинированных SIEM+SOAR решений позволяет сократить среднее время обработки инцидента (Mean Time to Respond, MTTR) на 67 % по сравнению с традиционными подходами, основанными на ручной обработке событий безопасности.

Можно ожидать дальнейшего взаимопроникновения SOAR и SIEM, что приведет к развитию функций оркестрации и автоматизации непосредственно в рамках SIEM-продуктов, формируя новое поколение интегрированных платформ безопасности.

Выводы

Традиционные SIEM-системы, основанные на правилах корреляции, имеют ряд ограничений при выявлении современных сложных угроз, таких как многошаговые кибератаки. Эти ограничения включают высокий уровень ложных срабатываний, неспособность выявлять ранее неизвестные типы атак и изолированный анализ событий без учета контекста. Применение методов искусственного интеллекта и машинного обучения в SIEM-системах позволяет преодолеть эти ограничения и повысить эффективность выявления инцидентов безопасности. Методы машинного обучения, такие как методы обучения без учителя, особенно эффективны для выявления аномалий и ранее неизвестных угроз.

Механизмы агрегации, нормализации и обогащения данных играют критически важную роль в повышении качества и информативности собираемых данных. Обогащение данных контекстной информацией из различных источников позволяет более точно выявлять инциденты безопасности и принимать соответствующие меры по их устранению. Прогностическая аналитика с использованием методов машинного обучения позволяет прогнозировать возможные атаки на основе исторических данных и принимать превентивные меры по их предотвращению. Внедрение таких методов значительно сокращает время реагирования на инциденты и повышает эффективность системы безопасности в целом.

Современные тенденции в развитии SIEM-систем связаны с интеграцией методов искусственного интеллекта и созданием систем нового поколения (AI-SIEM), которые обеспечивают более эффективное выявление угроз, прогнозную аналитику и автоматизированные механизмы реагирования. Таким образом, разработка программного средства для анализа информации о событиях безопасности на основе современных методов искусственного интеллекта является актуальной задачей, решение которой позволит повысить эффективность обеспечения информационной безопасности в условиях растущего количества и сложности киберугроз.

ЛИТЕРАТУРА

1. Оценка функционирования SIEM-систем на основе комплекса критериев эффективности / М.М. Путято, А.С. Макарян, А.Н. Черкасов, В.А. Кучер // Вестник Адыгейского государственного университета. Серия: Естественно-математические и технические науки. — 2024. — № 1(336). — С. 36–42. — DOI 10.53598/2410-3225-2024-1-336-36-42. — EDN RUDQZU.
2. Новикова, Е.С. Открытые задачи визуального анализа в системах управления информационной безопасностью / Е.С. Новикова, И.В. Котенко // Информационно-управляющие системы. — 2019. — № 2(99). — С. 57–67. — DOI 10.31799/1684-8853-2019-2-57-67. — EDN LZFXZE.
3. Основы информационной безопасности в МЧС России: Учебник / Р.Ш. Хабибулин, А.Н. Прокопенко, П.Н. Жукова [и др.]. — Москва: Академии ГПС МЧС России, 2023. — 649 с. — EDN DWSUOY.
4. Агапов, Д.К. Алгоритмы сбора и обработки данных в системах информационной безопасности / Д.К. Агапов // International Journal of Open Information Technologies. — 2023. — Т. 11, № 9. — С. 50–58. — EDN IOZMKB.
5. Кириллов, В.А. Система сбора и корреляции событий (siem) как ядро системы информационной безопасности / В.А. Кириллов, А.Р. Касимова, А.Д. Алехин // Вестник Технологического университета. — 2016. — Т. 19, № 13. — С. 132–134. — EDN WIQQWF.

6. Исследование SIEM-систем на основе анализа механизмов выявления кибератак» [Электронный ресурс]. — Режим доступа. — URL: https://cyberleninka.ru/article/n/issledovanie-siem-sistem-na-osnove-analiza-mehanizmov-vyyavleniya-kiberatak (дата обращения: 12.04.2025).
7. Методы машинного обучения для обнаружения аномалий [Электронный ресурс]. — Режим доступа. — URL: https://scilead.ru/article/6980-metodi-mashinnogo-obucheniya-dlya-obnaruzheni (дата обращения: 12.04.2025).
8. Генеративный искусственный интеллект как новая стадия развития технологий [Электронный ресурс]. — Режим доступа. — URL: https://www.semanticscholar.org/paper/Актуальность исследования угрозы /0253bd170d95710484da6e2578ddd1607c176eff (дата обращения: 12.04.2025).
9. Современные информационные системы анализа и управления рисками в сфере информационной безопасности / И.С. Глущенко, Е.М. Баранова, А.Н. Баранов, С.Ю. Борзенкова // Известия Тульского государственного университета. Технические науки. — 2021. — № 2. — С. 311–316. — DOI 10.24412/2071-6168-2021-2-311-316. — EDN ATMCEK.
10. Технологии интеллектуального анализа данных [Электронный ресурс]. — Режим доступа. — URL: https://lanbook.com/catalog/discipline/tehnologii-intellektualnogo-analiza-dannyh/ (дата обращения: 12.04.2025).
11. Современные тенденции в развитии SIEM-систем с использованием искусственного интеллекта [Электронный ресурс]. — Режим доступа. –URL: https://www.itsec.ru/articles/trendy-informacionnoj-bezopasnosti-i-kak-oni-vliyayut-na-siem (дата обращения: 12.04.2025).
12. Применение систем искусственного интеллекта в обеспечении защиты информации / А.Ю. Полуян, Е.Н. Целигорова, В.В. Галушка, Н.М. Кодацкий // Современная наука: актуальные проблемы теории и практики. Серия: Естественные и технические науки. — 2023. — № 8-2. — С. 123–127. — DOI 10.37882/2223-2982.2023.8-2.28. — EDN YUAABG.
13. Рыболовлев, Д.А. Классификация современных систем управления инцидентами безопасности / Д.А. Рыболовлев, С.В. Карасев, С.А. Поляков // Вопросы кибербезопасности. — 2018. — № 3(27). — С. 47–53. — DOI 10.21681/2311-3456-2018-3-47-53. — EDN MILVBB.
14. Котенко, И.В. Новое поколение систем мониторинга и управления инцидентами безопасности / И.В. Котенко, И.Б. Саенко, Р.М. Юсупов // Научно-технические ведомости Санкт-Петербургского государственного политехнического университета. Информатика. Телекоммуникации. Управление. — 2014. — № 3(198). — С. 7–18. — EDN SGSPXT.
15. Мунтян, М.М. Способ интеграции вспомогательного модуля с SIEM-системами / М.М. Мунтян, И.Г. Сидоркина // Вестник Чувашского университета. — 2024. — № 4. — С. 60–74. — DOI 10.47026/1810-1909-2024-4-60-74. — EDN FXNVRM.
16. Хлестова, Д.Р. Анализ актуальности использования SIEM-систем на предприятиях / Д.Р. Хлестова, К.Г. Попов // Символ науки: международный научный журнал. — 2016. — № 7-1(19). — С. 89–91. — EDN WHKOSX.
17. Аминев, В.М. Искусственный интеллект в информационной безопасности / В.М. Аминев, М.В. Питеркина // Успехи в науке и образовании 2024: сборник статей IV Международного научно-исследовательского конкурса, Пенза, 05 мая 2024 года. — Пенза: Наука и Просвещение (ИП Гуляев Г.Ю.), 2024. — С. 36–39. — EDN GKWTSR.
18. Котенко, И. Анализ моделей и методик, используемых для атрибуции нарушителей кибербезопасности при реализации целевых атак / И. Котенко, С.С. Хмыров // Вопросы кибербезопасности. — 2022. — № 4(50). — С. 52–79. — DOI 10.21681/2311-3456-2022-4-52-79. — EDN AIULIP.
19. Тренды информационной безопасности и их влияние на SIEM [Электронный ресурс]. — Режим доступа. — URL: https://www.itsec.ru/articles/trendy-informacionnoj-bezopasnosti-i-kak-oni-vliyayut-na-siem (дата обращения: 12.04.2025).
20. Шананин, В.А. Применение систем искусственного интеллекта в защите информации / В.А. Шананин // Инновации и инвестиции. — 2022. — № 11. — С. 201–205. — EDN ZNGNYF.
21. Рыболовлев, Д.А. Классификация современных систем управления инцидентами безопасности / Д.А. Рыболовлев, С.В. Карасев, С.А. Поляков // Вопросы кибербезопасности. — 2018. — № 3(27). — С. 47–53. — DOI 10.21681/2311-3456-2018-3-47-53. — EDN MILVBB.
22. Котенко, И.В. Новое поколение систем мониторинга и управления инцидентами безопасности / И.В. Котенко, И.Б. Саенко, Р.М. Юсупов // Научно-технические ведомости Санкт-Петербургского государственного политехнического университета. Информатика. Телекоммуникации. Управление. — 2014. — № 3(198). — С. 7–18. — EDN SGSPXT.
23. Мунтян, М.М. Способ интеграции вспомогательного модуля с SIEM-системами / М.М. Мунтян, И.Г. Сидоркина // Вестник Чувашского университета. — 2024. — № 4. — С. 60–74. — DOI 10.47026/1810-1909-2024-4-60-74. — EDN FXNVRM.
24. Хлестова, Д.Р. Анализ актуальности использования SIEM-систем на предприятиях / Д.Р. Хлестова, К.Г. Попов // Символ науки: международный научный журнал. — 2016. — № 7-1(19). — С. 89–91. — EDN WHKOSX.