DOI 10.37882/2223-2966.2025.06-2.32

# ИССЛЕДОВАНИЕ ИНТЕЛЛЕКТУАЛЬНЫХ МЕТОДОВ АНАЛИЗА ЖУРНАЛОВ СОБЫТИЙ ДЛЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

## RESEARCH OF INTELLIGENT METHODS FOR ANALYZING EVENT LOGS FOR INFORMATION SECURITY

***A. Rusakov***
***A. Bobyr-Bukhanovsky***

*Summary*. The article presents an analytical review of modern methods of intelligent event log analysis in the field of information security, focusing on the integration of neural networks and heuristic approaches. The relevance of the study is due to the rapid growth in the volume and complexity of analyzing system event logs, as well as the need to promptly identify new types of threats. Such as APT attacks and Zero-day vulnerabilities that cannot be effectively detected by traditional methods (signature analysis, manual filtering).

The key features of neural network architectures for analyzing time sequences presented in event logs are considered. Including LSTM and GRU architectures, autoencoders for anomaly detection, as well as hybrid models combining machine learning with signature methods and manual methods. Special attention was paid to heuristic approaches that complement neural network solutions, increasing the interpretability of results and reducing the burden on computing resources. Practical solutions are being found, such as the use of entropy clustering methods and dynamic adaptation of trigger thresholds based on historical statistics.

The article details the stages of log mining: from data collection and preprocessing to training models and evaluating their effectiveness using accuracy, half-note, and F1-measure metrics. The integration of methods into industrial SIEM systems, including MaxPatrol SIEM and Kaspersky Unified Monitoring and Analysis Platform, is described, with an emphasis on technical aspects (software interfaces, scalability, data transfer security). The key problems of introducing new approaches are discussed, such as the interpretability of neural network «black boxes», optimization of resources for processing big data, and the need to adapt models to evolving threats (new threats). Self-learning systems, standardization of event log formats for intelligent analysis, as well as the introduction of Explicable AI (XAI) to increase confidence in solutions are noted as promising areas of development.

*Keywords*: event log analysis, security event management systems (SIEM), information security, anomaly detection, artificial intelligence, machine learning.

***Русаков Алексей Михайлович***
*старший преподаватель,*
*МИРЭА — Российский технологический университет*
*rusakov_a@mirea.ru*
***Бобырь-Бухановский Александр Игоревич***
*Лаборант,*
*МИРЭА — Российский технологический университет*
*s5696998@yandex.ru*

*Аннотация*. В статье представлен аналитический обзор современных методов интеллектуального анализа журналов событий в сфере информационной безопасности, фокусирующийся на интеграции нейронных сетей и эвристических подходов. Актуальность исследования обусловлена стремительным ростом объёмов и сложности анализа журналов событий систем, а также необходимостью оперативного выявления новых типов угроз. Таких как APT-атаки (от англ. сложная постоянная угроза) и Zero-day уязвимости (уязвимости нулевого дня), которые не могут быть эффективно обнаружены традиционными методами (сигнатурный анализ, ручная фильтрация). Рассматриваются ключевые особенности архитектур нейронных сетей для анализа временных последовательностей представленных в журналах событий. Включая архитектуры LSTM и GRU, автоэнкодеры для обнаружения аномалий, а также гибридные модели, сочетающие в себе машинное обучение с сигнатурными методами и ручными методами. Особое внимание было уделено эвристическим подходам, которые дополняют нейросетевые решения, повышая интерпретируемость результатов и снижая нагрузку на вычислительные ресурсы. Приводятся практические решения, такие как применение энтропийных методов кластеризации и динамической адаптации порогов срабатывания на основе исторической статистики.

Статья детализирует этапы интеллектуального анализа журналов: от сбора и предобработки данных до обучения моделей и оценки их эффективности с использованием метрик точности, полноты и F1-меры. Описана интеграция методов в промышленные SIEM-системы, включая MaxPatrol SIEM и Kaspersky Unified Monitoring and Analysis Platform, с акцентом на технические аспекты (программные интерфейсы, масштабируемость, безопасность передачи данных). Обсуждаются ключевые проблемы внедрения новых подходов, такие как интерпретируемость «чёрных ящиков» нейросетей, оптимизация ресурсов для обработки больших данных и необходимость адаптации моделей к evolving-угрозам (новые угрозы). В качестве перспективных направлений развития отмечены самообучающиеся системы, стандартизация форматов журналов событий для интеллектуального анализа, а также внедрение Explainable AI (XAI, от англ. объяснимый искусственный интеллект) для повышения доверия к решениям.

*Ключевые слова*: анализ журналы событий, системы управления событиями безопасности, информационная безопасность, обнаружение аномалий, искусственный интеллект, машинное обучение.

## Введение

В условиях стремительного роста объёмов и сложности информационных потоков журналы событий становятся ключевым инструментом для мониторинга и обеспечения информационной безопасности в организациях. Журналы событий фиксируют широкий спектр событий — от действий пользователей и системных процессов до сетевых взаимодействий и попыток несанкционированного доступа. Эффективный анализ этих данных позволяет своевременно выявлять инциденты, расследовать атаки, отслеживать аномалии и поддерживать высокий уровень защищённости ИТ-инфраструктуры [1, 2].

Схема организации защиты ИТ-инфраструктуры на основе анализа журналов событий представлена на рисунке 1. Однако традиционные методы анализа журналов событий, основанные на сигнатурных правилах, ручной фильтрации и статистических алгоритмах, сталкиваются с рядом существенных ограничений. Они не справляются с возрастающим объёмом и разнородностью данных, не способны обнаруживать сложные, ранее неизвестные угрозы, а также требуют значительных временных и человеческих ресурсов. Это приводит к риску пропуска критических инцидентов и увеличению времени реагирования на атаки [2, 3].

В ответ на эти вызовы всё большую актуальность приобретают интеллектуальные методы анализа, основанные на применении искусственного интеллекта и, в частности, нейронных сетей. Архитектуры нейронных сетей глубокого обучения, такие как LSTM, GRU и автоэнкодеры [4], позволяют выявлять сложные закономерности, анализировать последовательности событий и эффективно обнаруживать аномалии даже в больших и разнородных потоках данных. Вместе с тем, интеграция эвристических и экспертных правил, формируемых на основе профессиональных знаний и исторической статистики, повышает интерпретируемость решений, снижает количество ложных срабатываний и позволяет адаптировать системы к специфике конкретной инфраструктуры [5].

В современных высоконагруженных и распределённых системах всё чаще используются гибридные подходы, объединяющие преимущества нейросетевых моделей и эвристических методов. Это позволяет не только повысить точность и скорость обнаружения угроз, но и оптимизировать использование вычислительных ресурсов, а также обеспечить прозрачность и объяснимость принимаемых решений.

## Применение нейронных сетей для анализа журналов событий

Современные подходы к анализу журналов событий в информационной безопасности всё чаще опираются на методы искусственного интеллекта, в первую очередь на нейронные сети. Их использование обусловлено способностью выявлять сложные, нелинейные зависимости и паттерны в больших объёмах разнородных данных, что особенно актуально для задач обнаружения аномалий, инцидентов и новых видов атак.

*Рекуррентные нейронные сети с архитектурой LSTM и GRU*. Рекуррентные нейронные сети, в частности построенные на архитектурах LSTM (Long Short-Term Memory) и GRU (Gated Recurrent Unit), предназначены для работы с последовательностями данных, что делает их особенно эффективными для анализа временных паттернов в журналах событий и выявления взаимосвязей между ними. В области информационной безопасности эти архитектуры позволяют не только обнаруживать аномалии, но и строить сложные корреляционные правила, автоматически выявляя цепочки действий, характерные для многоэтапных атак и инсайдерских угроз.

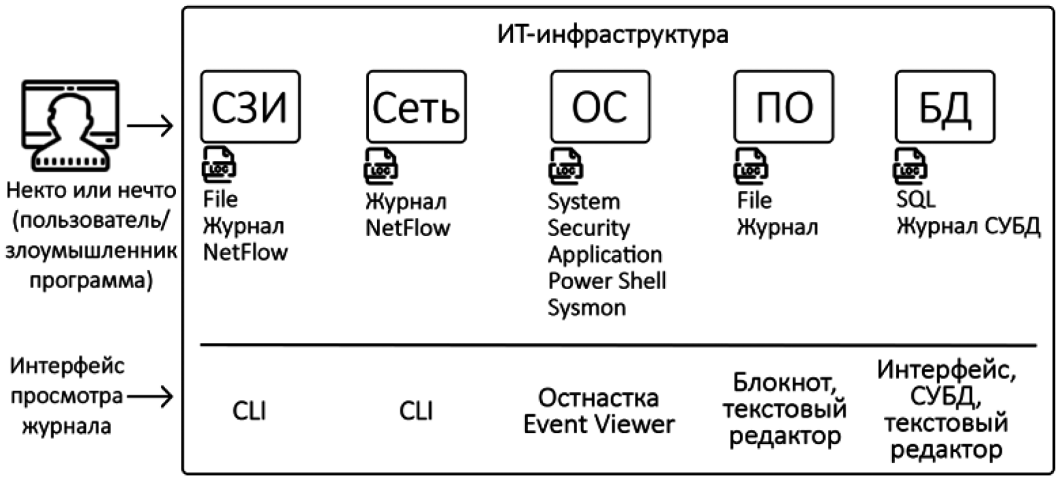


Рис. 1. Схема организации защиты ИТ-инфраструктуры на основе анализа журналов событий

Практическое применение архитектур LSTM и GRU в SIEM-системах заключается в автоматическом анализе последовательности событий, поступающих из различных источников (сетевые устройства, серверы, приложения), и выявлении подозрительных сценариев, которые сложно описать статическими правилами. Например, модель нейронной сети, основанная на LSTM, способна прогнозировать ожидаемое развитие событий и сигнализировать о появлении отклонений, что позволяет оперативно реагировать на сложные инциденты, выявлять скрытые связи между событиями и минимизировать время расследования [4]. Такие подходы особенно эффективны для обнаружения атак, реализующихся через длинные цепочки событий с временными задержками между ними.

*Автоэнкодеры для обнаружения аномалий*. Автоэнкодеры представляют собой разновидность нейронных сетей, обучающихся сжимать входные данные и восстанавливать их обратно. При обучении на нормальных событиях автоэнкодер плохо восстанавливает аномальные или ранее не встречавшиеся паттерны, что позволяет использовать ошибку восстановления как индикатор аномалии. Однако в современных системах информационной безопасности автоэнкодеры применяются не только для точечного обнаружения аномалий, но и для выявления сложных коррелированных групп событий [4].

Практически это реализуется через анализ групп логов, поступающих в определённом временном окне или связанных по идентификаторам сессий, пользователей или устройств. Автоэнкодеры способны выявлять нетривиальные взаимосвязи между событиями, которые могут указывать на координированные атаки или аномальное поведение внутри инфраструктуры. В промышленных системах (например, SCADA) применение автоэнкодеров способствует снижению числа ложных срабатываний, а также позволяет выявлять скрытые многошаговые сценарии атак, когда отдельные события по отдельности не выглядят подозрительно, но их совокупность указывает на инцидент.

*Гибридные модели на основе LSTM и SVM*. Для повышения устойчивости и точности анализа журналов событий часто применяются гибридные методы, сочетающие возможности различных архитектур нейронных сетей и алгоритмов машинного обучения. Примером является связка LSTM для анализа временных последовательностей и SVM (Support Vector Machine) для последующей классификации аномалий. Такой подход позволяет объединить преимущества глубокого обучения в выявлении сложных зависимостей с высокой интерпретируемостью и эффективностью классических алгоритмов, что особенно ценно для корпоративных и промышленных систем с высокими требованиями к объяснимости решений [4].

Таким образом, разнообразие архитектур нейронных сетей и возможность их комбинирования открывают широкие перспективы для повышения эффективности анализа журналов событий и построения интеллектуальных систем информационной безопасности.

## Этапы интеллектуального анализа журналов событий

Эффективное применение нейросетевых и гибридных методов для анализа журналов событий требует последовательного выполнения ряда этапов, охватывающих весь жизненный цикл обработки данных — от их сбора до оценки качества работы моделей. Каждый этап вносит вклад в повышение точности обнаружения аномалий, снижение числа ложных срабатываний и адаптацию системы к реальным условиям эксплуатации [6,7].

*Сбор и предобработка данных*. Первым этапом является сбор журналов событий из различных источников: операционных систем, сетевых устройств, приложений, промышленных контроллеров и облачных сервисов. На этом этапе важно обеспечить полноту и целостность данных, а также их защиту от несанкционированного изменения. Предобработка включает очистку от дублирующихся и неинформативных записей, нормализацию формата сообщений, синхронизацию временных меток и структурирование неструктурированных логов с помощью парсинга и методов обработки естественного языка (NLP). Для повышения эффективности дальнейшего анализа часто выделяются ключевые признаки (feature engineering), такие как идентификаторы пользователей, IP-адреса, коды событий и временные интервалы.

*Обучение и валидация моделей*. На следующем этапе формируются обучающие и тестовые выборки, обеспечивающие представительность как нормальных, так и аномальных событий. Для обучения нейросетевых моделей (LSTM, автоэнкодеры, гибридные схемы) используются размеченные или полуразмеченные данные, а также методы аугментации для увеличения разнообразия обучающих примеров. Валидация проводится с использованием кросс-валидации, отложенных выборок или специализированных сценариев имитации атак. Это позволяет выявить переобучение, оценить устойчивость моделей к новым типам угроз и подобрать оптимальные гиперпараметры.

## Метрики информационной безопасности

Метрики информационной безопасности, формируемые на основе журналов событий, включают количественные показатели успешных и неуспешных аутентификаций, изменений учетных записей и групп безопасности, частоты очистки журналов аудита, попыток сброса паролей и блокировок учетных записей

(по идентификаторам событий Windows) [8]. В сетевых журналах анализируются количество IDS-оповещений, число уникальных рабочих станций и учетных записей с неудачными попытками входа, а также соотношение подозрительных сетевых соединений к фоновому уровню. Метрики корреляции событий включают анализ неудачных попыток входа без последующей успешной аутентификации, выявление аномальной активности и кросс-корреляцию между разными источниками событий. Основные компоненты метрик: идентификатор события, источник, пользователь, временная метка и тип события. Дополнительно учитываются показатели устранения и выявления уязвимостей, отклонения от требований ИБ и количество потенциальных точек входа. Эти метрики обеспечивают комплексную оценку состояния информационной безопасности организации [9].

*Эвристические подходы анализа журналов событий*. Эвристические методы остаются важной составляющей анализа журналов событий, особенно в условиях высокой неопределённости данных, ограниченности обучающих выборок и необходимости быстрого реагирования на новые типы угроз. Они позволяют использовать знания и опыт экспертов, а также историческую статистику для построения практико-ориентированных решений и оптимизации вычислительных ресурсов.

*Практико-ориентированные решения*. Одной из ключевых задач эвристических подходов является разработка правил, основанных на экспертных знаниях. Такие правила могут включать фильтрацию подозрительных IP-адресов, портов, аномальных последовательностей действий пользователей, а также шаблонов поведения, характерных для определённых видов атак. Например, для обнаружения DDoS-атак или подозрительных попыток аутентификации формируются наборы признаков и пороговых значений, при превышении которых событие помечается как потенциально опасное.

Гибридные методы, сочетающие сигнатурный анализ и машинное обучение, позволяют повысить эффективность обнаружения как известных, так и новых угроз. Примером может служить работа [10], где для выявления DDoS-атак используются как заранее определённые сигнатуры, так и обучаемые модели, способные адаптироваться к изменяющимся сценариям атак.

*Оптимизация ресурсов*. Для повышения производительности и снижения нагрузки на вычислительные системы применяются эвристики, направленные на предварительную кластеризацию событий. Энтропийный подход, предложенный [11], позволяет группировать события по степени их информационной насыщенности, выделяя наиболее значимые для дальнейшего анализа.

Динамическое изменение порогов срабатывания на основе исторической статистики позволяет адаптировать систему к изменяющимся условиям эксплуатации и снижать количество ложных срабатываний. Например, если в определённые периоды наблюдается всплеск активности, система может автоматически корректировать пороговые значения, чтобы избежать избыточных оповещений и сосредоточиться на действительно критических инцидентах.

В целом, интеграция эвристических подходов с нейросетевыми и гибридными моделями обеспечивает баланс между эффективностью, прозрачностью и адаптивностью систем анализа журналов событий, что особенно важно для практического применения в корпоративных и промышленных инфраструктурах.

*Секвенционный анализ*. Секвенционный анализ, направленный на выявление закономерностей в последовательностях событий, играет ключевую роль в обнаружении сложных многоэтапных атак, таких как APT (Advanced Persistent Threat) и целенаправленные фишинговые кампании. В работах [12,13] предложен метод, сочетающий эвристические правила с вероятностными моделями для анализа временных цепочек событий.

Основой подхода является построение марковских моделей, описывающих переходы между состояниями системы (например, «нормальная активность», «подозрительный доступ», «попытка эксплуатации уязвимости»). Для каждого состояния вычисляются вероятности перехода к другим состояниям на основе исторических данных. Отклонения от ожидаемых переходов (например, резкий скачок попыток доступа к критическим ресурсам после сканирования портов) маркируются как потенциальные индикаторы атаки.

Практическое применение метода включает:

- Автоматическую генерацию шаблонов атак на основе анализа успешных инцидентов.
- Корреляцию событий из разных источников (сети, хосты, приложения) для построения единой временной линии угроз.
- Динамическую адаптацию моделей при появлении новых типов событий, что особенно важно для противодействия evolving-угрозам (эволюционирующие угрозы).

Исследования [12] демонстрируют, что комбинация секвенционного анализа с эвристическими правилами позволяет снизить уровень ложных срабатываний на 25 % по сравнению с чисто статистическими методами, а также сократить время обнаружения многоэтапных атак в корпоративных сетях.

Таким образом, интеграция секвенционного анализа в эвристические подходы обеспечивает более глубокое понимание контекста событий и повышает эффектив-

ность систем мониторинга, особенно в условиях ограниченной размеченной обучающей выборки.

## Интеграция исследуемых методов в SIEM-системы

Интеграция нейросетевых, эвристических и гибридных методов анализа журналов событий в современные SIEM-системы (Security Information and Event Management) позволяет существенно повысить уровень автоматизации, точность обнаружения угроз и скорость реагирования на инциденты. На рисунке 2 представлена схема организации работы центра обеспечения информационной безопасности.

*Positive Technologies MaxPatrol SIEM*. Платформа поддерживает внедрение гибридных аналитических модулей [14], сочетающих возможности машинного обучения, нейросетей и эвристических правил. Через специализированные API и плагины обеспечивается автоматизированная передача событий из журналов в интеллектуальные анализаторы, а результаты обработки возвращаются в систему для дальнейшей корреляции и визуализации. Такой подход позволяет не только выявлять сложные и ранее неизвестные угрозы, но и оперативно адаптировать правила реагирования на основе новых паттернов атак.

*Kaspersky Unified Monitoring and Analysis Platform*. Платформа интегрирует методы глубокого обучения (например, LSTM, автоэнкодеры) и эвристические фильтры для анализа больших потоков событий в реальном времени [15]. Платформа обеспечивает масштабируемую обработку данных, что критично для крупных промышленных и распределённых инфраструктур. Интеллектуальные модули позволяют снижать количество ложных срабатываний, автоматизировать расследование инцидентов и формировать отчёты для специалистов по информационной безопасности.

*Технические аспекты: API, масштабируемость*. Техническая интеграция интеллектуальных методов в SIEM-системы реализуется через открытые API, поддерживающие обмен данными между ядром платформы и внешними аналитическими сервисами. Для обеспечения масштабируемости используются распределённые вычисления, контейнеризация и балансировка нагрузки. Особое внимание уделяется безопасности передачи данных, разграничению прав доступа и контролю целостности журналов событий. Интеграция современных методов анализа в SIEM-платформы позволяет не только повысить эффективность мониторинга и реагирования, но и создать основу для построения проактивных, самообучающихся систем информационной безопасности, способных адаптироваться к новым угрозам и минимизировать человеческий фактор в процессе обработки инцидентов.

## Проблемы и перспективы решений по интеллектуальному анализу журналов событий

Внедрение нейросетевых и эвристических методов в анализ журналов событий открывает новые возможности для автоматизации и повышения эффективности

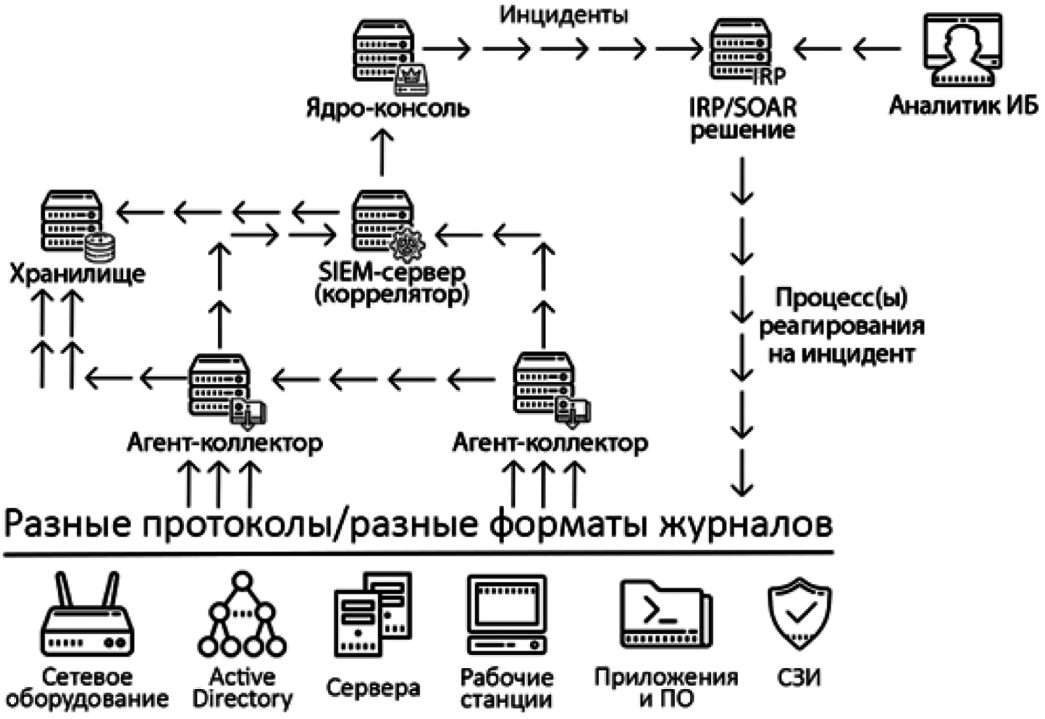


Рис. 2. Схема организации работы центра обеспечения информационной безопасности

информационной безопасности, однако сопровождается рядом вызовов, которые необходимо учитывать при проектировании и эксплуатации подобных систем.

*Интерпретируемость решений*. Одной из ключевых проблем остаётся низкая интерпретируемость сложных нейросетевых моделей, что затрудняет объяснение причин срабатывания системы и снижает доверие со стороны специалистов по информационной безопасности. Для повышения прозрачности используются методы объяснения решений, такие как визуализация важности признаков, применение XAI (Explainable AI), а также внедрение гибридных схем, где эвристические правила дополняют «чёрный ящик» ИИ и делают выводы более понятными для эксперта.

*Оптимизация вычислительных ресурсов*. Обработка больших объёмов событий в реальном времени требует значительных вычислительных мощностей, особенно при использовании глубоких нейронных сетей. Для оптимизации ресурсов применяются предварительная фильтрация, эвристическая кластеризация событий, распределённые вычисления, а также квантование и упрощение архитектуры моделей. Это позволяет снизить нагрузку на инфраструктуру и обеспечить масштабируемость решений для крупных корпоративных и промышленных систем.

*Самообучающиеся системы*. Перспективным направлением развития является создание самообучающихся и адаптивных систем, способных автоматически обновлять свои правила и параметры на основе новых данных и поведения атакующих [16]. Использование методов reinforcement learning, federated learning и динамической настройки порогов реагирования позволит системам быстрее адаптироваться к новым угрозам, минимизировать ложные срабатывания и поддерживать высокий уровень защищённости без постоянного участия эксперта.

В целом, дальнейшее развитие гибридных подходов, объединяющих нейросетевые и эвристические методы, направлено на повышение эффективности, прозрачности и устойчивости систем анализа журналов событий, что особенно важно в условиях роста объёмов данных и появления всё более сложных киберугроз.

## Выводы

Современный анализ журналов событий в информационной безопасности требует сочетания мощных инструментов искусственного интеллекта и гибких эвристических подходов. Нейронные сети, такие как LSTM, GRU и автоэнкодеры, позволяют выявлять сложные паттерны, анализировать временные зависимости и обнаруживать аномалии, ранее недоступные для классических методов. В то же время эвристические решения, основанные на экспертных правилах, исторической статистике и динамической адаптации порогов, обеспечивают прозрачность, интерпретируемость и оптимизацию вычислительных ресурсов.

Гибридные методы, объединяющие сильные стороны ИИ и эвристик, демонстрируют высокую эффективность в реальных корпоративных и промышленных системах, особенно при интеграции в современные SIEM-платформы, такие как MaxPatrol SIEM и Kaspersky Unified Monitoring and Analysis Platform. Такой подход позволяет не только повысить точность и скорость обнаружения угроз, но и снизить количество ложных срабатываний, а также обеспечить адаптацию к новым типам атак.

Ключевыми направлениями дальнейшего развития являются повышение интерпретируемости решений, внедрение самообучающихся систем и стандартизация форматов логов для интеллектуального анализах [17]. Комплексное применение нейросетевых и эвристических методов становится основой для построения надёжных, адаптивных и масштабируемых систем информационной безопасности, способных эффективно противостоять современным киберугрозам.

ЛИТЕРАТУРА


1. Sheeraz M., Durad M.H., Paracha M.A., Mohsin S.M., Kazmi S.N., Maple C. Revolutionizing SIEM Security: An Innovative Correlation Engine Design for Multi-Layered Attack Detection // Sensors. — 2024. — Т. 24, № 15. — С. 4901. — DOI: 10.3390/s24154901.
2. Sheeraz M., Paracha M.A., Haque M.U., Durad M.H., Mohsin S.M., Band S.S. и др. Effective security monitoring using efficient SIEM architecture // Human-centric Computing and Information Sciences. — 2023. — Т. 13. — С. 1–18.
3. Priambodo D.F., Prabowo H., Suryanegara M., Nugroho L.E. Collaborative Intrusion Detection System with Snort Machine Learning Plugin // JOIV: International Journal on Informatics Visualization. — 2024. — Т. 8, № 3. — С. 1230–1238.
4. Du M., Li F., Zheng G., Srikumar V. Deeplog: Anomaly detection and diagnosis from system logs through deep learning // Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security. — 2017. — С. 1285–1298.
5. Хасанова А.М. Интеллектуальный анализ процессов по данным журналов событий информационных систем / А.М. Хасанова // International Journal of Open Information Technologies. — 2022. — Т. 10, № 10. — С. 70-77. — EDN JIMCSN.
6. Анализ методов корреляции событий безопасности в Siem-системах. Часть 1 / A.V. Fedorchenko, D.S. Levshun, A.A. Chechulin, I.V. Kotenko // Труды СПИИРАН. — 2016. — № 4(47). — С. 5–27. — DOI 10.15622/sp.47.1. — EDN WHWSZZ.

7. Анализ методов корреляции событий безопасности в SIEM-системах. Часть 2 / А.В. Федорченко, Д.С. Левшун, А.А. Чечулин, И.В. Котенко // Труды СПИИРАН. — 2016. — № 6(49). — С. 208–225. — DOI 10.15622/sp.49.11. — EDN XHFTDR.
8. Методика оценивания защищенности на основе семантической модели метрик и данных / Е.В. Дойникова, А.В. Федорченко, И.В. Котенко, Е.С. Новикова // Вопросы кибербезопасности. — 2021. — № 1(41). — С. 29–40. — DOI 10.21681/2311–3456-2021-1-29-40. — EDN GUICXW.
9. Как можно и нужно пользоваться метриками информационной безопасности [Электронный ресурс] // Habr.com. — 2024. — URL: https://habr.com/ru/articles/827178/ (дата обращения: 18.04.2025).
10. Зубкова Е.В. Сигнатурный анализ и машинное обучение для повышения эффективности обнаружения известных и новых угроз // Информационная безопасность. — 2023. — № 4. — С. 45–52.
11. Полтавцева М.А. Энтропийный подход к кластеризации событий для повышения производительности вычислительных систем // Информационные технологии и вычислительные системы. — 2022. — № 3. — С. 58–65.
12. Шелухин О.И. Диагностика «здоровья» компьютерной сети на основе секвенциального анализа последовательностных паттернов / О.И. Шелухин, А.В. Осин, Д.В. Костин // T-Comm: Телекоммуникации и транспорт. — 2020. — Т. 14, № 2. — С. 9–16. — DOI 10.36724/2072–8735–2020-14-2-9-16. — EDN IHWDMD.
13. Шелухин О.И. Мониторинг и диагностика аномальных состояний компьютерной сети на основе изучения «исторических данных» / О.И. Шелухин, А.В. Осин, Д.В. Костин // T-Comm: Телекоммуникации и транспорт. — 2020. — Т. 14, № 4. — С. 23–30. — DOI 10.36724/2072–8735–2020-14-4-23-30. — EDN AQKPYX.
14. Обзор MaxPatrol SIEM 8.0, системы мониторинга ИБ-событий и реагирования на инциденты [Электронный ресурс] // Anti-Malware.ru. — 2023. — 27 октября. — URL: https://www.anti-malware.ru/reviews/MaxPatrol-SIEM-8-0 (дата обращения: 21.04.2025).
15. Обзор Kaspersky Unified Monitoring and Analysis Platform (KUMA) [Электронный ресурс] // Anti-Malware.ru. — 2021. — URL: https://www.anti-malware.ru/reviews/Kaspersky-Unified-Monitoring-and-Analysis-Platform (дата обращения: 23.04.2025).
16. Self-Learning AI in Adaptive Threat Mitigation [Электронный ресурс] // Insights2TechInfo. — 2023. — URL: https://insights2techinfo.com/self-learning-ai-in-adaptive-threat-mitigation/ (дата обращения: 3.05.2025).
17. Розум Р.С. Архитектура автоматизированной информационной системы обработки и семантического анализа запросов к системам обслуживания реального времени / Р.С. Розум, А.С. Кузнецов // Тенденции развития науки и образования. — 2024. — № 115–15. — С. 101–107. — DOI 10.18411/trnio-11-2024-709. — EDN DOSWGC.