УДК 004.056.53:004.8

ПРИМЕНЕНИЕ ТЕХНОЛОГИЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В SIEM ДЛЯ МИНИМИЗАЦИИ ОГРАНИЧЕНИЙ ПРАВИЛ КОРРЕЛЯЦИИ

Г.А. Славинский, В.А. Быстрова, Н.Л. Боброва

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», г. Минск, Республика Беларусь

Аннотация. В статье исследуется развитие SIEM-систем под влиянием технологий искусственного интеллекта. Систематизированы ключевые ограничения правил корреляции и проведен анализ возможностей современных интеллектуальных инструментов для их преодоления. Определены преимущества и недостатки подобной интеграции, выдвинуто предположение о будущем SIEM.

Ключевые слова: информационная безопасность; мониторинг событий; SIEM; искусственный интеллект; машинное обучение.

APPLICATION OF ARTIFICIAL INTELLIGENCE TECHNOLOGIES IN SIEM TO MINIMISE THE LIMITATIONS OF CORRELATION RULES

G.A. Slavinsky, V.A. Bystrova, N.L. Bobrova
Educational Institution "Belarusian State University of Informatics and Radioelectronics", Minsk, Republic of Belarus

Abstract. The article examines the evolution of SIEM systems under the influence of Artificial Intelligence technologies. It categorises the key limitations of correlation rules and analyses how modern AI-enhanced tools can overcome them. The study identifies the advantages and disadvantages of such integration and offers a perspective on the future of SIEM.
Keywords: information security; event monitoring; SIEM; artificial intelligence; machine learning.

Введение

SIEM – это решение для управления информацией и событиями безопасности, обеспечивающее централизованный сбор, нормализацию, корреляцию и анализ данных из множества источников инфраструктуры [1]. Его основная задача – формирование перечня инцидентов.

Решения класса SIEM можно классифицировать по архитектуре, модели поставки и функциональным возможностям [2]. В контексте данной статьи, ключевым критерием является метод выявления угроз: от использования заданных правил к адаптивным механизмам на базе технологий искусственного интеллекта. Существенные различия между этими подходами определяют их применимость в условиях роста сложности атак, что подчеркивает актуальность проводимого исследования.

Основная часть

Правила корреляции представляют собой набор условий для автоматического анализа событий и выявления признаков уже известных атак, их эффективность зависит от полноты и актуальности базы правил, что приводит к ряду существенных ограничений:

избыточный объем данных, высокая доля ложноположительных срабатываний;

неспособность обнаружения новых угроз из-за отсутствия известных шаблонов поведения;

проблема выявления сложных атак на основе последовательности событий, распределенных во времени и по их источникам;

необходимость экспертизы со стороны опытного аналитика для быстрого расследования инцидента.

Указанные ограничения являются основанием для внедрения перспективных технологий – искусственного интеллекта (ИИ), способного повысить эффективность обнаружения угроз [3]. Среди ключевых возможностей ИИ: извлечение знаний и закономерностей из больших объемов данных, выявление скрытых паттернов, автоматизация бизнес-логики.

Эволюция SIEM предполагает переход к новым архитектурным решениям. Основой автоматизации бизнес-логики являются методы машинного обучения.

Машинное обучение позволяет адаптироваться к новым угрозам за счет непрерывного обучения на исторических и реальных данных: обучение без учителя для выявления неизвестных угроз и аномалий в поведении, обучение с учителем для быстрой идентификации известных типов атак.

Преимущество машинного обучения – динамические профили нормального поведения пользователей и систем. Точность обучения зависит от целостности входных данных. Важно учитывать чувствительность данных.

Глубокое обучение позволяет анализировать сложные структуры данных для обнаружения скрытых зависимостей, недоступных классическим алгоритмам. Важно отметить, что вместо единой модели эффективнее использовать архитектуру, состоящую из нескольких моделей.

Интеллектуальные методы находят применение в ключевых функциях систем мониторинга: от обработки естественного языка, упрощающей взаимодействие с системой через NLP-запросы, до поведенческого анализа, необходимого для предотвращения несанкционированного доступа.

Интеграция ИИ трансформирует SIEM, превращая ее в проактивную платформу защиты со следующими возможностями:

минимизация ложных срабатываний, фиксация реальных угроз;
обнаружение ранее неизвестных угроз;
выявление сложных и распределенные во времени атак;
предотвращение инцидентов на начальных стадиях (разведки).

Ожидается, что дальнейшее развитие интеллектуальных алгоритмов приведет к появлению систем обнаружения и реагирования, минимизирующих участие человека в решении однотипных задач.

Заключение

Интеграция технологий искусственного интеллекта является ключевым направлением эволюции SIEM, и повышает эффективность обнаружения сложных угроз, улучшает качество корреляции событий, снижает уровень нагрузки на специалистов информационной безопасности, ускоряет процесс реагирования на инциденты.

К сдерживающим факторам можно отнести необходимость качественных и не всегда стандартных данных для обучения, риск ошибок при некорректной настройке параметров, сложность интерпретации конкретных выводов, высокие требования к вычислительным ресурсам.

Наиболее перспективным подходом выглядит гибридная модель, сочетающая логику классических правил корреляции с адаптивными возможностями технологий искусственного интеллекта.

Список использованных источников

1. Рубанова К. В., Голуб А. А. (2025) Сравнительный анализ SIEM для киберцентров. *Сборник материалов 61-й научной конференции аспирантов, магистрантов и студентов БГУИР.* 34–37.

2. Алейникова Д. И. (2025) Системы управления информационной безопасностью и событиями информационной безопасности. *Технические средства защиты информации.* 51–54.

3. Булгакова Е. В., Дойников Д. С., Кубанков А. Н. (2026) Проблема точности и объяснимости при внедрении искусственного интеллекта в системы управления информацией и событиями безопасности. *Наукоемкие технологии в космических исследованиях Земли.* 17 (3) 35–41.

References

1. Rubanova K. V., Golub A. A. (2025) Comparative Analysis of SIEM for Cyber Centers. *Collection of Materials of the 61st Scientific Conference of Postgraduates, Master Students and Students of BSUIR.* 34–37.

2. Aleinikova D. I. (2025) Information Security and Information Security Event Management Systems. *Technical Means of Information Protection.* 51–54.

3. Bulgakova, E. V., Doinikov, D. S., Kubankov, A. N. (2026). The Problem of Accuracy and Explainability in the Implementation of Artificial Intelligence in Security Information and Event Management Systems. *High-Tech Technologies in Earth Space Exploration.* 17 (3) 35–41.

Сведения об авторах

Славинский Г.А., магистрант, Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», gr.slavin.sci@mail.ru.

Быстрова В.А., магистрант, Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», veronikabystrova94@gmail.com.

Боброва Н.Л., доцент, Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», bobrova@bsuir.by.

Information about the authors

Slavinsky G.A., master's degree student, Educational Institution "Belarusian State University of Informatics and Radioelectronics", gr.slavin.sci@mail.ru.

Bystrova V.A., master's degree student, Educational Institution "Belarusian State University of Informatics and Radioelectronics", veronikabystrova94@gmail.com.

Bobrova N.L., associate professor, Educational Institution "Belarusian State University of Informatics and Radioelectronics", bobrova@bsuir.by.