УДК 004.056.5

МЕТОД ПЕРЕНОСА ДЕТЕКТИРУЮЩЕЙ ЛОГИКИ МЕЖДУ СИСТЕМАМИ ОБНАРУЖЕНИЯ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ С ПОМОЩЬЮ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Козлов И.А.
Научный руководитель – преподаватель Мешков А.В.
Университет ИТМО
cozl.il@yandex.ru

Работа выполнена в рамках темы НИР №623106 «Автономные интеллектуальные системы».

Введение

В условиях стремительного развития технологий и роста киберугроз обеспечение информационной безопасности остается критической задачей современных систем. Ключевым направлением здесь выступает перенос детектирующей логики между системами обнаружения угроз с использованием искусственного интеллекта, что обеспечивает гибкую адаптацию правил обнаружения, автоматизированный переход между платформами и повышение эффективности защиты.

Основная часть

Исследование фокусируется на создании метода переноса детектирующей логики между системами обнаружения угроз ИБ с помощью ИИ, позволяющего оперативно мигрировать с одной платформы на другую без потери качества детекции. Предложенный подход интегрирует алгоритмы машинного обучения для семантического анализа, трансформации и адаптации правил, учитывая специфику данных, форматов логов и моделей угроз в каждой системе. Для реализации метода решаются следующие задачи:

1. Анализ существующих подходов к переносу логики (включая скрипты и ручные конвертеры), выявление их ограничений, таких как потеря контекста и зависимость от экспертов.
2. Создание и теоретическое обоснование усовершенствованного метода, который будет учитывать особенности функционирования систем безопасности и характерные угрозы для разных информационных сред.
3. Разработка и интеграция ИИ-модели на базе нейронных сетей или трансформеров для автоматизированной генерации и оптимизации детектирующих правил под целевую систему.
4. Экспериментальная верификация на реальных сценариях с метриками точности, скорости переноса и снижения ложных срабатываний.
5. Интеграция метода в существующие решения с возможностью масштабирования на новые системы.

Выводы

Разработанный ИИ-ориентированный метод переноса детектирующей логики значительно повышает адаптивность систем обнаружения угроз к динамичным киберугрозам и изменениям инфраструктуры. Он минимизирует зависимость от вендоров, ускоряет миграцию и обеспечивает устойчивую защиту в разнородных средах. Это особенно актуально для организаций с несколькими SIEM-системами, где ручной перенос логики становится узким местом.

Литература

1. Sigma - Generic Signature Format for SIEM Systems [Электронный ресурс] / GitHub. – Режим доступа: https://github.com/SigmaHQ/sigma?utm_source=Securitylabru (дата обращения: 17.02.2026)
2. Как писать правила корреляции в SIEM-системе без навыков программирования [Электронный ресурс] / Positive Technologies. – Режим доступа: https://www.ptsecurity.com/ru-ru/research/knowledge-base/kak-pisat-pravila-korrelyacii-v-siem-sisteme-bez-navykov-programmirovaniya/ (дата обращения: 17.02.2026)
3. Чисмон Д., Рукс М. Threat Intelligence: Collecting, Analysing, Evaluating. – 2015.
4. ATT&CK Matrix for Enterprise [Электронный ресурс] / MITRE ATT&CK. – Режим доступа: https://attack.mitre.org/ (дата обращения: 17.02.2026)
5. Автоматизация ИИ для современного бизнеса [Электронный ресурс] / Microsoft. – Режим доступа: https://www.microsoft.com/ru-ru/microsoft-copilot/copilot-101/ai-automation (дата обращения: 17.02.2026)