УДК 004.056.5

МЕТОД ПЕРЕНОСА ДЕТЕКТИРУЮЩЕЙ ЛОГИКИ МЕЖДУ СИСТЕМАМИ ОБНАРУЖЕНИЯ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Козлов И.А. (ИТМО)
Научный руководитель – аспирант Мешков А.В.
(ИТМО)

Введение. В условиях стремительного развития технологий и увеличения числа киберугроз, обеспечение информационной безопасности становится одной из важнейших задач в современных информационных системах. Важным аспектом этой задачи является перенос детектирующей логики между различными системами обнаружения угроз, что позволяет адаптировать и улучшать методы защиты информации, а также осуществлять быстрый переход с одной системы защиты информации на другую. В данной исследовании рассматриваются ключевые подходы к разработке эффективных методов переноса детектирующей логики, а также их влияние на повышение уровня безопасности информационных систем.

Основная часть. Исследование направлено на разработку метода переноса детектирующей логики между системами обнаружения угроз информационной безопасности, позволяющей быстро и эффективно переходить с одной системы защиты информации на другую. Предложенный метод включает в себя алгоритмы адаптации и интеграции детектирующих механизмов, позволяющие учитывать уникальные характеристики каждой системы и специфические условия эксплуатации.
Для разработки предполагаемого метода переноса детектирующей логики необходимо выполнить следующий комплекс задач:

1. Изучение текущих методов переноса детектирующей логики, выявление их недостатков и проблем, возникающих при интеграции в различные системы обнаружения угроз.
2. Создание и теоретическое обоснование усовершенствованного метода, который будет учитывать особенности функционирования систем безопасности и характерные угрозы для разных информационных сред.
3. Проведение экспериментального анализа и оценка эффективности предложенного метода на основе реальных сценариев киберугроз и тестирования в различных системах обнаружения.
4. Интеграция созданного метода с существующими системами обнаружения киберугроз и его развитие для адаптации к новым системам.

Выводы. Разработанный метод переноса детектирующей логики показывает заметное улучшение в способности систем обнаружения угроз адаптироваться к изменяющимся условиям. Это особенно важно для обеспечения надежной защиты информации в условиях постоянно изменяющихся киберугроз. Также данный метод позволяет не зависеть от конкретного решения обнаружения угроз информационной безопасности.

Список использованных источников:

1. Sigma - Generic Signature Format for SIEM Systems [Электронный ресурс] / GitHub. – Режим доступа: https://github.com/SigmaHQ/sigma?utm_source=Securitylabru (дата обращения: 05.02.2025)
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: 05.02.2025)

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: 05.02.2025)