УДК 004.4

Разработка приложения для анализа и фильтрации сетевых взаимодействий

Тюмин Н. С. (Университет ИТМО)
Научный руководитель – инженер факультета инфокоммуникационных технологий, Мигулаева Т. А.
(Университет ИТМО)

Введение. В условиях растущей сложности современных сетевых инфраструктур вопросы мониторинга и фильтрации сетевого трафика приобретают особую значимость. Анализ сетевых взаимодействий позволяет выявлять аномалии, предотвращать угрозы безопасности и оптимизировать использование ресурсов. В рамках данного исследования рассматриваются возможности разработки приложения, которое обеспечивает сбор, анализ и фильтрацию сетевых данных в реальном времени, предоставляя пользователю удобные инструменты для управления сетевым трафиком.

Основная часть. Разработанное приложение ориентировано на автоматизированный сбор информации о сетевых взаимодействиях, их анализ и применение фильтрации на основе заданных правил. Используемые алгоритмы позволяют выявлять подозрительные соединения, аномальное поведение трафика и потенциальные угрозы. В ходе исследования были разработаны механизмы фильтрации, обеспечивающие блокировку нежелательных соединений. Для проверки эффективности разработанного приложения были проведены эксперименты с различными наборами данных, включающими нормальный и аномальный трафик. Анализ результатов показал, что предложенное решение позволяет значительно сократить время на обнаружение потенциальных угроз и повысить общую безопасность сетевого взаимодействия.

Выводы. Результаты исследования подтверждают, что автоматизированный анализ и фильтрация сетевого трафика позволяют повысить безопасность и управляемость сетевой инфраструктуры. Разработанное приложение предоставляет удобные инструменты для мониторинга, анализа и реагирования на потенциальные угрозы в режиме реального времени. Дальнейшее развитие системы может включать интеграцию с механизмами машинного обучения для повышения точности классификации сетевых событий и предсказания возможных инцидентов.

Список использованных источников:

1. Sommer R., Paxson V. Outside the Closed World: On Using Machine Learning for Network Intrusion Detection // 2010 – IEEE, 2010. – С. 305-316.
2. Roesch M. Snort – Lightweight Intrusion Detection for Networks // Proceedings of LISA '99, 1999.
3. Scarfone K., Mell P. Guide to Intrusion Detection and Prevention Systems (IDPS) // National Institute of Standards and Technology, 2007.