УДК 004.8

РАЗРАБОТКА АЛГОРИТМА ОБНАРУЖЕНИЯ АТАК В IP- И SDN-СЕТЯХ С ИСПОЛЬЗОВАНИЕМ ТЕХНОЛОГИЙ МАШИННОГО ОБУЧЕНИЯ

Чернякова Л.В. (Университет ИТМО)
Научный руководитель – Есипов Д.А. (Университет ИТМО)

Введение. Резкое увеличение количества подключенных к сети Интернет устройств и рост объема данных, циркулирующих между центрами обработки данных, бросили вызов существующим сетевым архитектурам. Наряду с совершенствованием традиционных методов управления IP-сетями, популярность набирает технология программно-определяемых сетей архитектуры.

Основная часть. Тема разработки алгоритма обнаружения атак в IP- и SDN-сетях является актуальной, поскольку позволяет предотвратить вторжения в сетевую инфраструктуру и снизить риски успешной реализации угроз безопасности. При решении задачи обеспечения защиты сети также становится актуальным вопрос автоматизации процесса выявления атак. Для обнаружения злоумышленников могут быть использованы подходы, основанные на машинном обучении [1, 2]. Системы обнаружения, основанные на машинном обучении, обладают большим потенциалом, поскольку являются более гибкими и адаптируемыми к изменяющейся среде угроз. В данном решении подготавливается набор данных сети и на основе машинного обучения разрабатывается модель обнаружения атак. Алгоритм, лежащий в основе модели, впоследствии может быть использован в основе систем обнаружения и предотвращения вторжений.

Выводы. В результате проделанной работы были рассмотрены известные методы обнаружения атак в IP- и SDN-сетях, основанные на машинном обучении. На основании рассмотренных методов был разработан собственных алгоритм, который позволяет снизить риски проведения успешных атак на сетевую архитектуру и, как следствие, повысить безопасность сети.

Список использованных источников:

1. Волков, С.С. Применение методов машинного обучения в sdn в задачах обнаружения вторжений / С.С. Волков, И.И. Курочкин // КиберЛенинка : электронный журнал. – URL: https://cyberleninka.ru/article/n/primenenie-metodov-mashinnogo-obucheniya-v-sdn-v-zadachah-obnaruzheniya-vtorzheniy. – Дата публикации: 06.06.2019.
2. Network intrusion detection system: A systematic study of machine learning and deep learning approaches / A. Zeeshan, A. Khan, W. Cheah, J. Abdullah // Transactions on Emerging Telecommunications Technologies : электронный журнал. – URL: https://onlinelibrary.wiley.com/doi/10.1002/ett.4150. – Дата публикации: 16.10.2020.

Чернякова Л.В. (автор) Подпись

Есипов Д.А. (научный руководитель) Подпись