УДК 004.7

Разработка методики обнаружения сетевых аномалий на основе анализа данных Netflow

Ярошевский Дмитрий Сергеевич,
Университет ИТМО, Санкт-Петербург
Научный руководитель: к.т.н., доцент Гирик Алексей Валерьевич
Университет ИТМО, Санкт-Петербург
dimonyarosh@mail.ru

В настоящее время возникает достаточно большое количество инцидентов информационной безопасности, связанных с реализацией сетевых атак. Существует необходимость в своевременном обнаружении атак и в принятии мер для их предотвращения. Цель работы – обнаружение сетевых аномалий на основе анализа данных Netflow.

Протокол Netflow – это сетевой протокол, предназначенный для учета сетевого трафика, разработанный компанией Cisco Systems. Архитектура Netflow предусматривает следующие компоненты: сенсоры, коллекторы, системы обработки и представления данных. Протокол использует UDP или SCTP для передачи данных о проходящем через сенсор трафике коллектору.

В ходе работы была разработана методика обнаружения сетевых аномалий на основе анализа данных Netflow. Методика протестирована в сети телекоммуникационного оператора. Сбор данных о сетевых потоках осуществлялся с помощью ipt_netflow – программного средства, позволяющего отправлять собранную информацию на указанный IP-адрес (адрес сервера, на котором осуществлялся анализ полученных данных). Для проверки обнаружения сетевых аномалий была выполнена симуляция атак.

По результатам тестирования было принято решение в дальнейшем усовершенствовать разработанную методику для повышения точности распознавания и классификации сетевых аномалий.