УДК 004.056

К ВОПРОСУ О РАЗРАБОТКЕ АНАЛИЗАТОРА ТРАФИКА

Нкодиа Д.-К. (Университет ИТМО)
Научный руководитель – к.т.н. Юрьева Р.А.
(Университет ИТМО)

Для повышения защищенности ИСУП поставлена задача о разработке анализатора сетевого трафика. В рамках исследования проанализированы подходы к разработке анализатор трафика, исполняющего две задачи: обнаружение известных атак с помощью классификации трафика и обнаружение ранее неизвестных атак с помощью выявления аномалий.

Каждый год увеличивается количество и разнообразие совершенных атак на ИСУП. На данный момент проведено большое количество исследований с использованием разных методов классификации трафика на известные типы атак, но гораздо реже встречаются работы, посвященные методам обнаружения аномалий в сетевом трафике. Возможность выявлять неизвестные атаки обеспечит ИСУП защищенность от угроз нулевого дня.

В качестве основных входных данных для анализатора предложено использовать параметры NetFlow для добавления возможности обнаруживать утечки информации, которую не могут осуществить система DLP, IDS и IPS.

Для обнаружения известных атак предложено использовать метод машинного обучения с учителем, демонстрирующий наилучшие результаты на основе проведенного аналитического обзора – Boosting. В качестве основного параметра сравнения существующих алгоритмов классификации для применения в области ИБ был выбран Recall, показывающий долю элементов положительного класса по результатам работы алгоритма из всех элементов положительного класса.

Для своевременного детектирования аномалий в сетевом трафике и обновления базы данных атак предложено сравнить работу алгоритмов без учителя для выявления аномалий и выбрать метод кластеризации, точнее обнаруживающий неизвестные атаки.

Описанное программное решение может быть использовано в качестве составной части SIEM систем для повышения защищенности с возможностью выявлять неизвестные атаки и обнаруживать аномалии в сети.