УДК: 004.4, 004.02
Название: Разработка метода распознавания сетевых атак на ресурсы на основе алгоритмов машинного обучения
Автор: Чернышкова Кристина Алексеевна, Университет ИТМО
Научный руководитель: Спивак Антон Игоревич, Университет ИТМО

Введение

Задача интернет-провайдера – предоставлять клиентам доступ в сеть Интернет, а также связанные с этим услуги. Для выполнения провайдером этих и других задач необходимо своевременно реагировать на различные угрозы, которые могут возникать как по отношению к информации, передаваемой и хранящейся в сети, так и по отношению к сервисам и оборудованию.

Но всегда существуют недобросовестные пользователи, которые будут использовать сервера для осуществления какой-либо аномальной сетевой активности, которая может навредить и оборудованию, и другим пользователям, и нанести ущерб на саму репутацию поставщика услуг. Поэтому крайне важно сразу же определять такие аномальные активности, чтобы не была возможна реализация описанных выше угроз. Еще требуется сделать такой метод, который бы не воспринимал обычную активность пользователя за аномальную.

Целью исследования

Разработка метода распознавания сетевых атак на ресурсы, который позволит своевременно обнаруживать аномальные активности и определять, какая именно атака произошла с помощью алгоритмов машинного обучения.

Планируемые результаты:

Итоговым результатом данной работы будет являться разработанный метод распознавания сетевых атак на ресурсы. В ходе научно-исследовательской части будут рассмотрены все основные сетевые атаки, проанализированы существующие подходы обнаружения сетевых атак с применением машинного обучения. В ходе практической части будут произведены следующие действия: 1) собран сетевой трафик с узлов сети на которых были обнаружены сетевые атаки; 2) данные, которые были обнаружены в первом пункте, маркируются; 3) разработка классификатора; 4) разработка метода обнаружения сетевых атак; 5) сравнение разработанного метода с существующими программами для обнаружения сетевых атак

В результате данной работы будет разработан метод, который позволит своевременно обнаруживать сетевые атаки и определять их.