УДК 004.056.5

РАЗРАБОТКА МЕТОДИКИ ПРИМЕНЕНИЯ НЕЙРОННЫХ СЕТЕЙ ДЛЯ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ В СЕТИ IoT.

Науменко В.С. (Университет ИТМО)
Научный руководитель – к.т.н., доцент Донецкая Ю.В.
(Университет ИТМО)

В работе будет описан процесс разработки и последующего тестирования методики применения нейросетей в средствах обнаружения вторжений в сети IoT. Описана IoT-сеть, подробно указаны все этапы методики, содержится тест-план методики.

Введение. В настоящее время сети IoT заполняют огромную часть нашей жизни, присутствуя буквально в любой сфере взаимодействия человека и техники. Все больше данных находится в сетях, что влечет за собой интерес со стороны злоумышленников, которые стремятся получить доступ к этой информации. В работе предлагается методика для повышения эффективности СОВ путем внедрения в них нейронных сетей, что привнесет возможность непрерывного улучшения качества обнаружения сетевых вторжений.

Основная часть. Примером системы IoT была выбрана навигационная система. В ней все данные обрабатываются на сервере, к которому подключаются устройства, передающие местоположение пользователя, данные о трафике и других дорожных событиях. Состоит система из умных навигаторов, смартфонов, дорожных устройств (светофор) и умных автомобилей (или систем навигации в них). Для системы были определены актуальные угрозы и посчитаны риски информационной безопасности. После этого пошел процесс разработки методики.

Методика описывает процессы, которые в последствии приведут к повышению эффективности работы СОВ. В первую очередь оценивается работа СОВ без нейронных сетей (современные варианты, например, Snort). Далее следует переход к работе с нейронными сетями: собираются сетевые дампы трафика (для обучающей и тестовой выборок нейронной сети, объем - около тысячи реальных кейсов вторжений каждая), пишется непосредственно нейросеть с учителем на языке Python. После написанного кода начинается процесс обучения: выборка из сетевых инцидентов посылается на вход программе с нейронной сетью, после чего она с помощью специалиста определяет необходимый вес данных и, за счет этого, обучается. После чего происходит программная интеграция кода нейронной сети в СОВ, тестирование этой связки.

Для оценивания методики, а именно проверки ее эффективности будут проведены тесты с использованием тех же сетевых дампов, собранных в начале. Результаты реагирования на тестовые инциденты будут сравниваться с подобными в других методиках или научных статьях для подтверждения повышения эффективности при использовании разрабатываемой методики. Также на основе тестов будут рассчитаны ошибки первого и второго рода, а также подведены итоги на основе сравнения с другими методиками, уже используемыми специалистами.

Выводы. В работе рассмотрена разработка методики, при помощи которой можно значительно поднять потолок эффективности систем обнаружения вторжений в сети IoT, реализация которой может быть представлена на примере навигационной системы.

Науменко В.С. (автор) _____

Донецкая Ю.В. (научный руководитель) _____