70. О МЕТОДАХ ОПРЕДЕЛЕНИЯ КИБЕРАТАК ЭЛЕКТРОННОГО БИЗНЕСА

Микулич В.С.

Белорусский государственный университет информатики и радиоэлектроники г. Минск, Республика Беларусь

Шинкевич Е.А. – канд. физ.-мат. наук

Аннотация. В работе рассмотрены методы определения кибератак, которые могут угрожать электронному бизнесу. Представлены примеры таких методов, дано их краткое описание. Рассмотрен вариант определения кибератак на основе использования нейросети, ее описание и результаты работы.

Кибератаки представляют собой значительную угрозу для электронного бизнеса, поскольку они могут привести к значительным финансовым потерям, ущербу репутации и нарушению нормальной работы. В эпоху цифровизации бизнес-процессов и увеличения объема онлайн-транзакций, кибератаки могут привести к утечке конфиденциальной информации, включая данные клиентов и коммерческую информацию. Это, в свою очередь, может подорвать доверие клиентов и привести к снижению продаж. Более того, кибератаки могут прервать работу важных систем, что может привести к простоям в работе и потере дохода.

К основным методам, позволяющим выполнить все этапы обнаружения кибертак, относятся расширенный тест Дики-Фуллера, R/S-анализ и метод DFA [1].

На первом этапе, вспомогательном, анализируются самоподобные свойства эталонного сетевого трафика. В эталонном трафике отсутствуют аномалии. В результате этого анализа определяется значение показателя Херста, соответствующее эталонному трафику. На втором, основном, этапе анализируются самоподобные свойства реального трафика, для которого могут быть характерны аномалии, вызванные воздействием кибератак. При этом также используются упомянутые выше методы определения значений показателя Херста. На третьем этапе на основе методов математической статистики осуществляется классификация кибератак в целях реализации мер защиты [2].

Для определения события, как кибератаку, можно использовать нейросеть. Алгоритм определения кибератаки строится на основе схемы перцептрона. Перцептрон – простейший вид нейронных сетей, в основе которых лежит математическая модель восприятия информации мозгом, состоящая из сенсоров, ассоциативных и реагирующих элементов [3]. Схематично простейшая нейросеть выглядит следующим образом (рис. 1).

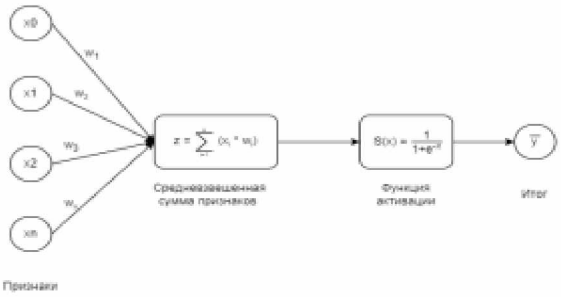

Рисунок 1 – Схема нейросети

Входные данные представляют собой значения признаков, которые могут быть равны 0 или 1. Эта строгая бинарность объясняется тем, что признаки функционируют как сенсоры, которые могут быть либо в состоянии покоя (равны 0), либо в состоянии активации (равны 1). Далее эти признаки умножаются на соответствующие веса и суммируются. С использованием функции активации получаются выходные значения в диапазоне от 0 до 1. Таким образом, основной задачей является определение таких весов, которые обеспечивают наиболее точное прогнозирование.

После нескольких циклов запуска предсказаний нейросетью были получены итоговые данные. Нейросеть точно определила кибеатаки по введенным самостоятельно признакам.

Список использованных источников:

1. Крупенин С.В. Фрактальные излучающие структуры и аналоговая модель фрактального импеданса. Дис. канд. физ.-мат. наук: 01.04.03, 01.04.04 / [Место защиты: Моск. гос. ун-т им. М.В.Ломоносова. Физ. фак.]. М., 2009. 157 с.

2. МЕТОД РАННЕГО ОБНАРУЖЕНИЯ кибератак на основе интеграции фрактального анализа и статистических методов [Электронный ресурс]/ И.Котенко, И.Саенко, О.Лаута, А.Крибель - Электрон. текстовые дан. – Москва. – Режим доступа: https://www.lastmile.su/journal/article/8990, свободный.

3. Нейросеть в Excel [Электронный ресурс]/ М.Кравец - Электрон. текстовые дан. – Москва. – Режим доступа: https://vc.ru/newtechaudit/526788-neyroset-v-excel?ysclid=ls0cnu1meq604154390, свободный.