УДК 004.032.26

АНАЛИЗ ВРЕМЕННЫХ РЯДОВ В ЗАДАЧАХ КЛАССИФИКАЦИИ ОБЪЕКТОВ КИБЕРАТАКИ НА ОСНОВЕ ОТКРЫТЫХ ИСТОЧНИКОВ ДАННЫХ

Григорьев А.М. (федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский университет ИТМО»)

Научный руководитель – кандидат технических наук, доцент факультета БИТ Менщиков А.А. (квалификационная категория "ординарный доцент")
(федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский университет ИТМО»)

Аннотация.

В данной работе рассматривается анализ временных рядов в задачах классификации объектов кибератаки на основе открытых источников данных с использованием нейронных сетей.

Введение.

Эксперты по кибербезопасности должны определять приоритеты на основе характера целей и чувствительности данных. Одним из способов решения этой проблемы является использование методов интеллектуального анализа данных, которые используются в различных областях, включая кибербезопасность. Это исследование направлено на изучение использования нейронной сети в задачах классификации для прогнозирования типа целей при кибератаках, которые могут помочь экспертам по кибербезопасности идентифицировать и определить приоритеты требований и возможных уязвимостей в любом типе бизнеса.

Основная часть.

Для решения поставленной проблемы предлагается использовать алгоритмы многослойного перцептрона способные идентифицировать объект кибератаки. Для этого необходимо произвести отбор параметров и преобразовать данные для дальнейшего анализа: проверка источника информации, очистка от символов, преобразование категориальных параметров и времени. После этого осуществляется настройка нейронной сети. Существует несколько параметров нейронной сети, требующих оптимизации: количество скрытых слоев и нейронов в них, функция активации, регуляризация, максимальное число итераций и пр. Также требуется рассмотреть различные методы анализа временных рядов. В итоге нужно рассмотреть параметры модели и оценить ее эффективность.

Выводы.

Это исследование подчеркнуло важность и значимость использования методов классификации для анализа прошлых кибератак для прогнозирования типа целей. Прогнозирование типа целей дает экспертам по кибербезопасности возможность разработать киберстратегию, основанную на различных секторах в отношении прошлого опыта.

Григорьев А.М. (автор) Подпись
Менщиков А.А. (научный руководитель) Подпись