УДК 004

Юнусова Д.С., Султанов Д.Ж.
Уфимский университет науки и технологий, Уфа

НЕЙРОСЕТЕВОЙ АНАЛИЗ URL-АДРЕСОВ ДЛЯ ВЫЯВЛЕНИЯ ФИШИНГОВЫХ АТАК

Аннотация. Фишинговые URL продолжают быть одним из наиболее частых инструментов в арсенале киберпреступников. В данной статье рассматривается нейросетевая модель для распознавания фишинговых URL-адресов, сотоящая из CNN части для обработки символьных

последовательностей домена и полносвязной части для обработки структурированных признаков.

Ключевые слова: фишинг, URL-адрес, нейронная сеть.

В эпоху цифровизации, когда интернет стал неотъемлемой составляющей повседневной жизни, возросло и количество киберугроз, в том числе фишинговых URL-адресов, представляющих серьезную угрозу для пользователей.

Фишинговые URL-адреса представляют собой специально сконструированные веб-ссылки, которые визуально имитируют адреса легитимных сайтов, но ведут на веб-ресурсы злоумышленников.

Использование черных списков становится малоэффективным, так как злоумышленники быстро создают новые адреса. В связи с этим сегодня востребованы системы обнаружения фишинга на основе нейронных сетей. Во время обучения нейронные сети могут распознавать такие особенности URL-адреса, как длина, спецсимволы и структура домена.

Для анализа и обучения нейросетевой модели был выбран набор данных «Malicious URLs dataset» с платформы Kaggle, включающий 651 191 URL-адрес. В данном датасете содержится 428 103 безопасных URL-адреса, 96 457 испорченных, 94 111 фишинговых и 32 520 URL-адреса, содержащего вредоносное ПО. Данные были собраны из пяти разнообразных источников, что позволяет обеспечить широкий спектр примеров. Это является ключевым аспектом при подготовке данных для проектов машинного обучения.

Для оптимизации работы на локальной машине и ускорения процесса обучения датасет был сокращен до 195 120 строк с равномерным распределением по всем классам.

Для векторизации URL-адресов использовался комбинированный подход, включающий следующие методы:

1. TF-IDF по символьным n-граммам (1–3).
2. OneHotEncoder (OHE) для доменных суффиксов.
3. Статистические признаки URL (длина, спецсимволы и др.).
4. Энтропия Шеннона для пути URL;
5. Символьные индексы домена (для анализа данных CNN).

Для решения задачи применялась нейросетевая модель, состоящая из нескольких компонентов:

1. CNN часть для обработки символьных последовательностей домена:
- слой эмбеддинга (размерность 32);
- два сверточных слоя (64 и 128 фильтров соответственно);
- Global Max Pooling для извлечения наиболее важных признаков.
2. Полносвязная часть для обработки структурированных признаков:
- отдельные полносвязные слои;
- слой объединения всех признаков из обоих ветвей;
- выходной полносвязный слой для финальной классификации;

3. В качестве функции активации выбрана функция ReLu.

4. В архитектуре модели используется функция dropout(0.3), которая случайным образом отключает 30 % нейронов на каждой итерации, тем самым снижая зависимость между нейронами.

Применение такой комбинированной архитектуры позволило достичь высокой точности классификации, так как сверточная часть эффективно выявляет паттерны в символьных последовательностях, а полносвязная часть обрабатывает статистические характеристики URL. Схема работы модели и графики процесса обучения представлены на рис. 1 и 2.

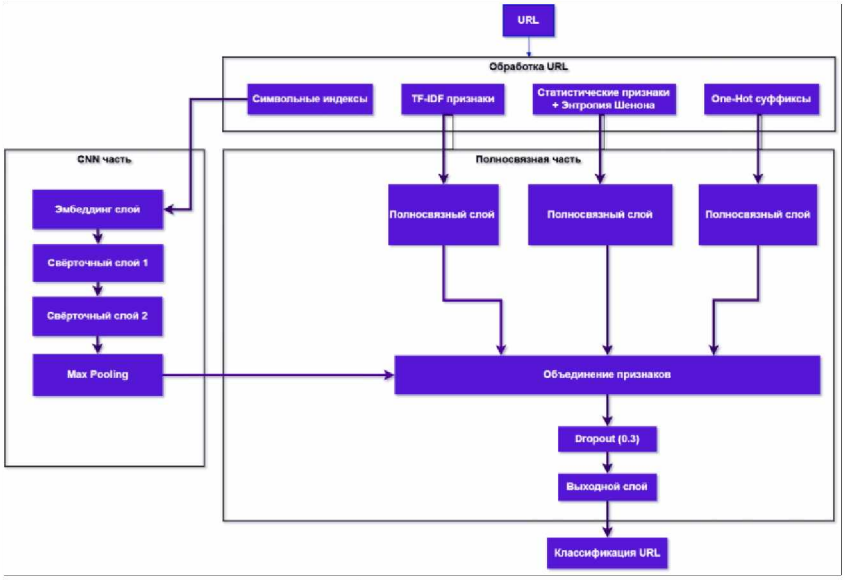

Рис. 1. Схема работы нейросетевой модели

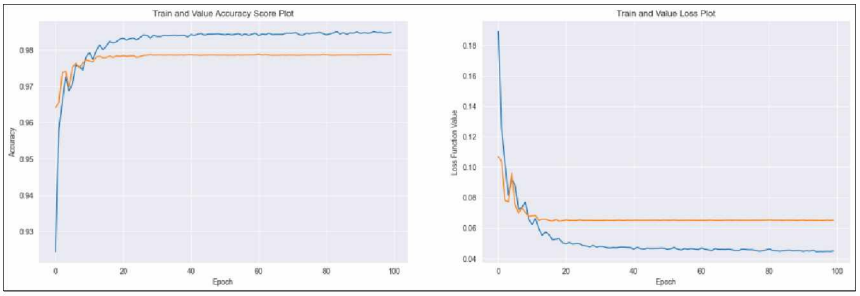

Рис. 2. График процесса обучения

Из графика видим, что на тренировочных данных точность обучения растет от 92,44 % до 98,48 %, а на валидационных – от 96,41 % до 97,87 %.

Разница между точностью на тестировочных и валидационных данных меньше 1 %, что указывает на отсутствие переобучения.

Значение функции потерь во время обучения на тренировочных данных падает от 0,1889 до 0,0449, а на валидационных – от 0,1068 до 0,0652. Функция потерь на валидационных данных не растет, а колеблется около 0.065, что также указывает на отсутствие переобучения.

Таким образом, модель демонстрирует стабильное обучение и хорошую обобщающую способность, успешно классифицируя URL-адреса.

Список использованных источников:

1. Тарасова Ю.А. Анализ проблемы фишинга в цифровом пространстве // Международный журнал прикладных и фундаментальных исследований. 2023. № 11. С. 56–60. URL: https://applied-research.ru/ru/article/view?id=13594 (дата обращения: 30.04.2025).
2. Механизм распознавания фишинговых сайтов по косвенным признакам // Молодой ученый. URL: https://moluch.ru/archive/318/72550/.
3. Mohammed Nazim Feroz, Susan Mengel Phishing URL detection using URL Ranking // Texas Tech University: 2015.
4. Корнюхина С.П., Лапонина О.Р. Исследование возможностей алгоритмов глубокого обучения для защиты от фишинговых атак. 2023.
5. Phishing URL Detection Using CNN-LSTM and Random Forest Classifier // Research Square. URL: https://www.researchsquare.com/article/rs-2043842/v1.

Yunusova D.S., Sutlanov D.Zh.
Ufa University of Science and Technology, Ufa

NEURAL NETWORK ANALYSIS OF URLS TO DETECT PHISHING ATTACKS

Abstract. Phishing URLs continue to be one of the most common tools in the cybercriminals' arsenal. This paper discusses a neural network model for recognizing phishing URLs, consisting of a CNN part for processing domain character sequences and a fully connected part for processing structured features.

Keywords: phishing, URL, neural network.