УДК 004.8

О. В. Герасімова

ДОСЛІДЖЕННЯ ТА РОЗРОБКА МЕТОДУ ВИЯВЛЕННЯ ФІШИНГОВИХ ВЕБ-РЕСУРСІВ З ВИКОРИСТАННЯМ АЛГОРИТМІВ МАШИННОГО НАВЧАННЯ

Донецький національний університет імені Василя Стуса

Анотація

Робота присвячена проблемі автоматизованого виявлення шахрайських (фішингових) веб-сайтів. Розроблено програмний модуль мовою Python, який здійснює аналіз лексичних характеристик URL-адрес для класифікації посилань на безпечні та шкідливі. Як основний алгоритм класифікації обрано метод "Випадкового лісу" (Random Forest). Проведено навчання моделі на відкритих наборах даних та оцінено її ефективність. Результати дослідження показали, що запропонований підхід дозволяє виявляти фішингові атаки з високою точністю в режимі реального часу, не покладаючись виключно на "чорні списки".

Ключові слова: *кібербезпека, фішинг, машинне навчання, Random Forest, аналіз URL, Python, Scikit-learn..*

Abstract

The paper is devoted to the problem of automated detection of fraudulent (phishing) websites. A software module in Python has been developed that analyzes the lexical characteristics of URLs to classify links into safe and malicious ones. The Random Forest method was chosen as the main classification algorithm. The model was trained on open datasets and its efficiency was evaluated. The results of the study showed that the proposed approach allows detecting phishing attacks with high accuracy in real time, without relying exclusively on "blacklists".

Keywords: *cybersecurity, phishing, machine learning, Random Forest, URL analysis, Python, Scikit-learn.*

Вступ

Фішинг залишається однією із найпоширеніших загроз в інформаційному просторі. Зловмисники створюють копії відомих веб-ресурсів для викрадення конфіденційних даних користувачів. Традиційні методи захисту, що базуються на статичних базах даних, не встигають реагувати на швидку появу нових шкідливих доменів [1, 2].

Використання методів штучного інтелекту та машинного навчання (Machine Learning) дозволяє аналізувати структуру URL-адреси та вміст сторінки, виявляючи загрози, які ще не були внесені до баз даних антивірусів [3].

Це робить дослідження методів інтелектуального аналізу веб-посилань актуальним завданням, що відповідає сучасним вимогам до кіберзахисту [4].

Постановка задачі дослідження

Метою роботи є створення ефективного інструменту для класифікації веб-ресурсів. Для досягнення мети необхідно:

- проаналізувати основні ознаки фішингових URL-адрес (довжина, наявність IP-адреси замість домену, використання спеціальних символів);
- сформувати навчальну вибірку даних на основі відкритих репозиторіїв;
- обрати та налаштувати алгоритм машинного навчання (Random Forest);
- розробити програмну реалізацію класифікатора мовою Python з використанням бібліотеки Scikit-learn [2];
- провести тестування розробленої системи та оцінити ймовірність помилкових спрацьовувань.

Виклад основного матеріалу

У ході дослідження було розроблено систему, яка приймає на вхід URL-адресу та повертає оцінку її безпечності.

На етапі вилучення ознак (Feature Extraction) програмний модуль аналізує такі параметри: довжина URL, глибина вкладеності шляху, наявність HTTPS, вік домену (через WHOIS-запит) та наявність підозрілих ключових слів у піддомені.

Для класифікації було обрано алгоритм Random Forest (випадковий ліс) через його стійкість до перенавчання та високу точність при роботі з табличними даними.

Реалізація виконана у середовищі Jupyter Notebook.

Процес навчання відбувався на збалансованому датасеті, що містив 10 000 записів. Для оцінки якості моделі використано метрику F1-score, яка є середнім гармонійним між точністю та повнотою.

Результати дослідження

Експериментальна перевірка показала, що алгоритм Random Forest досягає точності класифікації 96.5%. Найбільш вагомими ознаками для виявлення фішингу виявилися: довжина URL-адреси та наявність символу «@».

Час обробки одного запиту складає менше 0.1 с, що дозволяє інтегрувати розроблений модуль у браузерні розширення або поштові шлюзи. Порівняльний аналіз, проведений з урахуванням сучасних підходів до захисту інформації [4], продемонстрував перевагу ансамблевих методів над простими лінійними моделями.

Висновки

У роботі досліджено, запропоновано та реалізовано метод виявлення фішингових веб-ресурсів на основі аналізу лексичних властивостей URL-адрес. Використання машинного навчання дозволило створити адаптивну систему, здатну виявляти нові загрози. Отримані результати підтверджують ефективність застосування алгоритму Random Forest для задач кібербезпеки.

Подальші дослідження будуть спрямовані на додавання аналізу візуального контенту веб-сторінок.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. James G., Witten D., Hastie T., Tibshirani R. An Introduction to Statistical Learning: with Applications in R. New York : Springer, 2021. URL: https://www.statlearning.com/ .
2. User Guide: 1.10. Decision Trees & Random Forests [Electronic resource] / Scikit-learn Developers. 2024. URL: https://scikit-learn.org/stable/modules/tree.html .
3. Saha I., Sarma D., Chakma R. J. Phishing Attacks Detection using Machine Learning Approach. arXiv preprint. 2020. arXiv:2009.11116. URL: https://arxiv.org/pdf/2009.11116 .
4. Гнатюк С. О., Кіндзерський В. В. Сучасні методи виявлення фішингових атак. ResearchGate. 2021. URL: https://www.researchgate.net/publication/338685858_MODERN_METHODS_OF_PHISHING_ATTACKS_DETECTION .

Герасімова Олена Віталіївна – студентка кафедри інформаційних технологій, факультет інформаційних і прикладних технологій, Донецький національний університет імені Василя Стуса, м.Вінниця, e-mail: Lenyska2004@gmail.com ;

Herasimova Olena Vitaliivna – student of Department of Information Technology, faculty of Information and Applied Technologies, Vasyl Stus Donetsk National University, Vinnytsia, e-mail: Lenyska2004@gmail.com ;