МЕТОДИ ВИЯВЛЕННЯ ФІШИНГОВИХ ВЕБ-РЕСУРСІВ

Бочарова М.І., Настенко А.О.
Харківський національний університет радіоелектроніки, Харків, Україна

З розвитком цифрових технологій та активним використанням веб-сервісів у повсякденному житті проблема фішингових атак набуває дедалі більшої актуальності [1, 2]. Фішинг є одним із найпоширеніших видів атак соціальної інженерії, метою яких є введення користувача в оману для отримання його конфіденційних даних [3]. Зловмисники часто використовують підроблені електронні листи, повідомлення в месенджерах або SMS-повідомлення, що містять посилання на фальшиві веб-сайти, зовні схожі на офіційні ресурси банків, онлайн-сервісів або державних установ. Унаслідок цього користувач може помилково ввести логін, пароль, реквізити банківської картки або іншу конфіденційну інформацію [4].

Метою роботи є дослідження актуальних методів виявлення фішингових веб-ресурсів та визначення ознак, які можуть бути використані для їх автоматичної класифікації.

У результаті проведеного дослідження визначено найбільш поширені ознаки фішингових веб-ресурсів, зокрема використання доменних імен, подібних до назв відомих сервісів, нетипову структуру URL-адрес, наявність форм введення конфіденційних даних, а також елементи, що імітують інтерфейс легітимних веб-ресурсів.

На основі виявлених ознак визначено основні методи виявлення фішингових веб-ресурсів, а саме: методи аналізу URL-адреси, методи аналізу домену та інфраструктури ресурсу, методи аналізу HTML/DOM-структури веб-сторінки, а також методи виявлення візуальної подібності до легітимних сервісів.

Отримані результати можуть бути використані як основа для формування набору ознак та подальшої побудови моделей машинного навчання в системах автоматичного виявлення фішингових веб-ресурсів.

Список літератури

1. Moruf Akin Adebowale, Khin T. Lwin, Mohammad Alamgir Hossain. Intelligent phishing detection scheme using deep https://doi.org/10.1108/jeim-01-2020-0036
2. Д'якова, Н. Є., Сєвєрінов, О. В. (2022). Тестування вразливостей сучасних веб-ресурсів / Проблеми інформатизації: десята міжнародна науково-технічна конференція, 24–25 листопада 2022 року, Том 1. - Черкаси – Баку – Бельсько-Бяла – Харків.
3. Shivam Lohani. Social Engineering: Hacking into Humans. International Journal of Advanced Studies of Scientific Research, Vol. 4, No. 1, 5 лютого 2019, URL: https://ssrn.com/abstract=3329391
4. Голубничий, Д.Ю., Сєвєрінов, О.В., Коломійцев, О.В., Місюра, О.М., Третяк, В.Ф., Власов, А.В., Крук, Б.М. (2021). Аналіз сучасних загроз в інформаційних системах за складовими загроз: кібербезпеки, інформаційної безпеки та безпеки інформації.
5. Що таке фішинг і фішингова атака. HostIQ. URL: https://hostiq.ua/blog/ukr/internet-phishing/