УДК 004.056.5

В. А. Гарнага
М. В. Гнатюк

ЗАСІБ ВИЯВЛЕННЯ ФІШИНГОВИХ САЙТІВ ІЗ ВИКОРИСТАННЯМ МАШИННОГО НАВЧАННЯ

Вінницький національний технічний університет

Анотація

Фішингові атаки є однією з найбільш поширених та небезпечних загроз інформаційній безпеці користувачів мережі Інтернет. Традиційні засоби протидії фішингу, що базуються на використанні чорних списків або сигнатурного аналізу, мають обмежену ефективність через динамічне створення нових фішингових веб-ресурсів та постійну зміну тактик зловмисників. У статті представлено програмний засіб для автоматичного виявлення фішингових сайтів із використанням алгоритмів машинного навчання. Розроблений засіб здійснює аналіз структурних, доменних та поведінкових ознак веб-ресурсів і використовує ансамблевий алгоритм Random Forest для класифікації сайтів. Програмний засіб реалізовано у вигляді браузерного плагіна, який забезпечує перевірку веб-сторінок у режимі реального часу та інформує користувача про рівень потенційної загрози. Результати експериментальних досліджень підтвердили високу точність і практичну ефективність розробленого програмного засобу.

Ключові слова: фішинг, машинне навчання, Random Forest, веб-безпека, URL-аналіз, виявлення загроз.

Abstract

Phishing attacks are among the most widespread and dangerous threats to information security in the Internet environment. Traditional anti-phishing tools based on blacklists or signature analysis are limited in effectiveness due to the dynamic creation of new phishing websites and constantly evolving attack techniques. This paper presents a software tool for automatic detection of phishing websites using machine learning algorithms. The developed tool analyzes structural, domain, and behavioral features of web resources and applies the Random Forest ensemble algorithm for classification. The software is implemented as a browser extension that performs real-time website analysis and notifies users about potential security risks. Experimental results confirm the high accuracy and practical effectiveness of the proposed software tool.

Keywords: phishing, machine learning, Random Forest, web security, URL analysis, threat detection.

Вступ

З розвитком цифрових технологій і зростанням кількості онлайн-сервісів фішинг залишається однією з найнебезпечніших форм кіберзагроз [1]. Фішингові атаки спрямовані на отримання конфіденційної інформації користувачів шляхом створення підроблених веб-ресурсів, що імітують легітимні сайти банків, соціальних мереж або електронних сервісів. Основною проблемою таких атак є їх динамічний характер, що ускладнює своєчасне виявлення фішингових ресурсів традиційними програмними засобами [2].

Метою даної роботи є розробка програмного засобу для виявлення фішингових сайтів із використанням алгоритмів машинного навчання, який забезпечує автоматичну перевірку веб-ресурсів у режимі реального часу на основі аналізу їхніх структурних, доменних та поведінкових характеристик.

Результати дослідження

Сучасні засоби виявлення фішингових веб-сайтів здебільшого ґрунтуються на використанні статичних методів аналізу, зокрема чорних списків, сигнатурного пошуку або простих евристичних правил. Такі підходи реалізовані у відомих системах безпеки браузерів і антивірусних продуктів та передбачають перевірку домену або URL-адреси за попередньо сформованими базами даних відомих фішингових ресурсів. Однак ефективність подібних методів є обмеженою, оскільки сучасні фішингові сайти створюються динамічно, мають короткий життєвий цикл і часто змінюють доменні імена та структуру, що унеможливлює їх своєчасне включення до чорних списків. У результаті значна частина нових фішингових ресурсів залишається невиявленою на початкових етапах їх існування [3].

Альтернативні підходи, що використовуються у деяких існуючих рішеннях, базуються на сигнатурному або шаблонному аналізі HTML-коду веб-сторінки, перевірці SSL-сертифікатів або аналізі окремих ознак URL-адреси [4]. Проте такі методи також мають суттєві недоліки, оскільки зловмисники активно використовують безкоштовні SSL-сертифікати, легітимні хостинги та мінімальні зміни структури сторінок для обходу сигнатурних механізмів. Крім того, евристичні правила, як правило, є фіксованими та не адаптуються до появи нових схем фішингу, що знижує точність і підвищує кількість хибних спрацювань.

Запропонований програмний засіб для виявлення фішингових сайтів принципово відрізняється від традиційних аналогів завдяки використанню методів машинного навчання для інтелектуального аналізу веб-ресурсів. Основною перевагою розробленого засобу є те, що він не покладається на статичні списки або наперед визначені шаблони, а здійснює класифікацію сайтів на основі сукупності структурних, доменних та поведінкових ознак. Це дозволяє виявляти фішингові ресурси навіть у випадках, коли вони ще не відомі системам колективної безпеки та не внесені до жодних баз даних.

Методика роботи програмного засобу базується на багаторівневому аналізі веб-ресурсу та інтеграції результатів, отриманих із різних джерел даних. Програмний засіб реалізовано у вигляді браузерного плагіна з модульною архітектурою, що забезпечує чіткий поділ функціональних компонентів і ефективну взаємодію між ними. Під час відкриття веб-сторінки засіб автоматично ініціює процес збору ознак, формує вектор характеристик сайту та передає його на вхід моделі машинного навчання для подальшої класифікації.

Модуль URLAnalyzer відповідає за аналіз структурних характеристик URL-адреси. У межах цього модуля обчислюються такі параметри, як довжина URL, кількість піддоменів, наявність спеціальних символів, використання IP-адреси замість доменного імені, а також підозрілі ключові слова. Зазначені характеристики є типовими індикаторами фішингових ресурсів і дозволяють виявляти спроби маскування легітимних сайтів шляхом маніпуляції адресним рядком.

Модуль DomainAnalyzer здійснює аналіз доменних характеристик веб-ресурсу, зокрема віку домену, тривалості його реєстрації, наявності DNS-записів, використання HTTPS-протоколу та SSL-сертифіката. Молоді домени з коротким терміном реєстрації або відсутністю повноцінної інфраструктури, як правило, мають підвищений рівень ризику та часто використовуються для фішингових атак.

Модуль ContentFeatureExtractor відповідає за обробку контентних і поведінкових ознак веб-сторінки. У межах цього модуля аналізується кількість внутрішніх і зовнішніх гіперпосилань, наявність елементів <iframe>, форм введення облікових даних, перенаправлень, а також використання підозрілих JavaScript-скриптів. Отримані параметри дозволяють виявляти сторінки, що імітують процеси авторизації або намагаються приховано перенаправити користувача на інші ресурси.

Ключовим компонентом програмного засобу є модуль MLClassifier, у якому реалізовано модель машинного навчання на основі алгоритму Random Forest. Модель була навчена на збалансованому наборі даних фішингових і легітимних сайтів та продемонструвала високу точність класифікації. Алгоритм Random Forest забезпечує стійкість до шуму в даних і дозволяє ефективно працювати з великою кількістю різнорідних ознак, що є критично важливим для аналізу веб-ресурсів.

Модуль DecisionExplainer виконує аналіз важливості ознак та формує пояснення результатів класифікації. У випадку виявлення фішингового сайту користувачеві відображається інформація про основні фактори, які вплинули на рішення моделі, наприклад підозрілий домен, відсутність індексації у пошукових системах або аномальна структура URL. Такий підхід підвищує прозорість роботи засобу та сприяє формуванню довіри до результатів автоматичного аналізу.

Модуль UserNotification забезпечує інформування користувача шляхом відображення повідомлень у браузері у вигляді попереджень або інформаційних сповіщень. Це дозволяє оперативно реагувати на потенційні загрози без переривання роботи користувача та без значного впливу на продуктивність браузера.

Таким чином, результати проведеного дослідження підтверджують, що запропонований програмний засіб демонструє суттєві переваги над традиційними методами виявлення фішингових сайтів. Завдяки використанню машинного навчання, багаторівневому аналізу ознак і модульній архітектурі, засіб забезпечує високу точність, адаптивність та здатність виявляти нові фішингові ресурси у режимі реального часу. Отримані експериментальні результати свідчать про ефективність розробленого програмного засобу та доцільність його використання для підвищення рівня інформаційної безпеки користувачів мережі Інтернет.

Результати роботи розробленого програмного засобу візуалізуються у вигляді інтерактивного повідомлення браузерного плагіна, яке відображається користувачеві під час відвідування потенційно небезпечного веб-ресурсу. У повідомленні надається попередження про можливу фішингову загрозу, відображається обчислена ймовірність фішингу, а також пропонуються варіанти подальших дій користувача, зокрема продовження перегляду сайту, повернення на попередню сторінку або збереження ресурсу як безпечного (Рисунок 1-2). Такий підхід забезпечує зручну взаємодію з користувачем і дозволяє оперативно реагувати на потенційні загрози інформаційній безпеці.

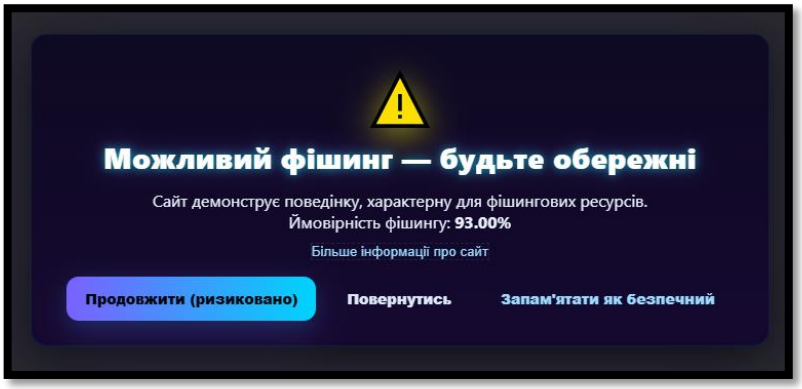

Рисунок 1 – Попередження про можливий фішинг (згорнута інформація)

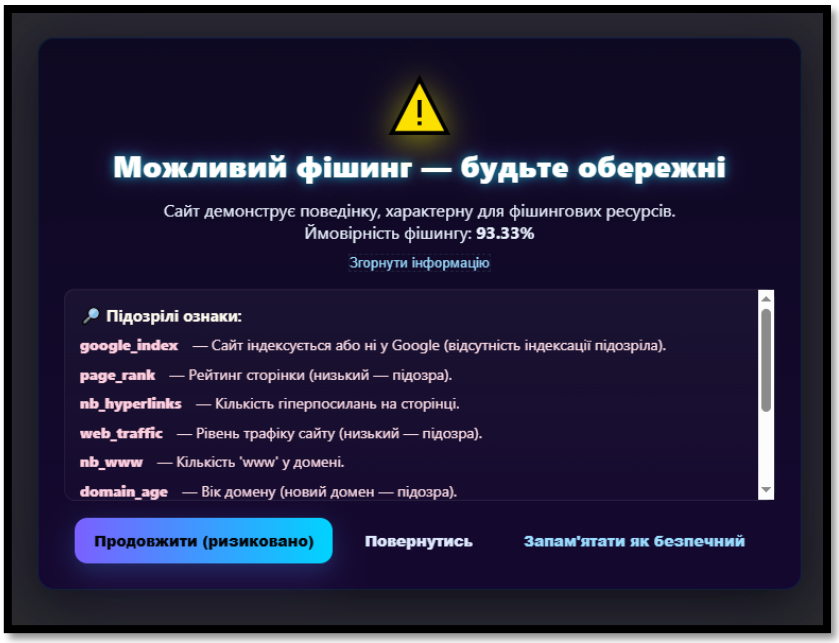

Рисунок 2 – Розгорнутий перелік підозрілих ознак сайту

Висновки

У роботі представлено програмний засіб для виявлення фішингових сайтів із використанням машинного навчання. Реалізований засіб на основі алгоритму Random Forest забезпечує високу точність класифікації веб-ресурсів і дозволяє виявляти фішингові сайти, які відсутні у традиційних чорних списках. Використання браузерного плагіна як форми реалізації забезпечує перевірку сайтів у режимі реального часу без суттєвого впливу на продуктивність системи. Отримані результати підтверджують доцільність застосування розробленого програмного засобу для підвищення рівня захисту користувачів від фішингових загроз.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. ENISA. Phishing: Threat Landscape and Mitigation Strategies. European Union Agency for Cybersecurity, 2024. (дата звернення:15.12.2025).
2. APWG. Phishing Activity Trends Report. Anti-Phishing Working Group, 2024. (accessed: 15.12.2025).
3. Dehghantanha A., Conti M., Dargahi T., Franke K. Cyber Threat Intelligence and Analytics for Phishing and Social Engineering Attacks. Springer, 2023. (дата звернення: 15.12.2025).
4. Hadnagy C. Social Engineering: The Science of Human Hacking. 2nd ed. Wiley, 2022. (дата звернення: 15.12.2025).

Науковий керівник: ***Гарнага Володимир Анатолійович*** – канд. техн. наук, доцент кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця,
e-mail: garnaga.volodymyr@vntu.edu.ua.
Гнатюк Максим Віталійович – студент групи 1БС-24м, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, м. Вінниця,
e-mail: maksgnatyuk192@gmail.com.

Supervisor: ***Garnaga Volodymyr Anatoliyovych*** — Cand. Sc., Associate Professor of Information Protection, Vinnytsia National Technical University, Vinnytsia, e-mail: garnaga.volodymyr@vntu.edu.ua.
Hnatiuk Maksym Vitaliiovych – student of group 1BS-24m, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: maksgnatyuk192@gmail.com.