УДК 004.056.5

Фернега Є.І.
Грицак А.В.

АНАЛІЗ МЕТОДІВ ВИЯВЛЕННЯ ФІШИНГОВИХ САЙТІВ З ВИКОРИСТАННЯМ ШТУЧНОГО ІНТЕЛЕКТУ ТА НЕЙРОННИХ МЕРЕЖ

Вінницький Національний Технічний Університет

Анотація

В даній статті розглянуто методи виявлення фішингових сайтів з використанням штучного інтелекту та нейронних мереж. Розглянуто традиційні методи та їх порівняння з підходами на основі машинного навчання для підвищення точності виявлення. Описано систему автоматичного виявлення фішингових сайтів на базі PHP-ML, що адаптується до нових загроз.

Ключові слова: Фішингові сайти, штучний інтелект, нейронні мережі, машинне навчання.

Abstract

This article discusses methods for detecting phishing sites using artificial intelligence and neural networks. It examines traditional methods and compares them with machine learning approaches to improve detection accuracy. It describes a PHP-ML-based automatic phishing site detection system that adapts to new threats.

Key words: Phishing sites, artificial intelligence, neural networks, machine learning.

Вступ

В умовах стрімкого розвитку інтернет-технологій актуальність безпеки в онлайн-середовищі стає надзвичайно важливою для користувачів і організацій. Фішинг є однією з найбільш поширених загроз, коли зловмисники створюють фальшиві веб-сайти для крадіжки особистої інформації. У зв'язку з цим, традиційні методи виявлення фішингових сайтів часто не можуть ефективно розпізнати нові або складні атаки. Використання нейронних мереж і машинного навчання дозволяє значно підвищити точність виявлення таких сайтів, адаптуючи системи до нових загроз і забезпечуючи кращий захист користувачів. У цій доповіді розглядаються сучасні методи виявлення фішингових сайтів з використанням технологій штучного інтелекту та їх порівняння з традиційними підходами.

Дослідження

Фішинг є однією з основних загроз для користувачів інтернету, оскільки зловмисники використовують підроблені сайти для отримання конфіденційної інформації. Традиційні методи виявлення фішингових сайтів, як правило, ґрунтуються на статичних перевірках, таких як аналіз URL, перевірка наявності SSL-сертифікатів та виявлення сайтів у чорних списках. Проте ці методи не завжди ефективні через швидку еволюцію фішингових стратегій. У цьому контексті методи штучного інтелекту, зокрема нейронні мережі, дозволяють значно підвищити точність і адаптивність виявлення фішингових сайтів.

Застосування нейронних мереж для виявлення фішингових сайтів базується на аналізі різноманітних характеристик, таких як довжина URL, кількість піддоменів, структура сайту, наявність HTTPS, час створення домену та редиректи. Кожен із цих параметрів має певну вагу, яка використовується для формування вхідного вектора, що передається в нейронну мережу. Однією з основних переваг цього підходу є здатність мережі адаптуватися до нових фішингових схем, що дозволяє автоматично оновлювати ваги ознак і враховувати нові методи маскування [1].

Для навчання нейронної мережі застосовується алгоритм зворотного поширення помилки (Backpropagation), який коригує ваги на кожному етапі навчання, мінімізуючи помилки між фактичними та очікуваними результатами. Це дає змогу нейронній мережі ефективно класифікувати нові сайти як фішингові або легітимні, навіть якщо вони використовують раніше невідомі методи.

Приклад застосування такої технології показав високу точність виявлення фішингових сайтів, особливо в поєднанні з традиційними методами перевірки. Статистика свідчить, що комбіноване

використання нейронних мереж і статичних методів дозволяє значно знизити кількість помилкових спрацьовувань (false positives) і пропусків (false negatives), що робить систему більш ефективною у реальних умовах. Крім того, ця модель здатна виявляти не лише відомі фішингові сайти, а й нові, що використовують нові шаблони і техніки.

Виявлення фішингових сайтів залишається однією з головних проблем у сфері інформаційної безпеки, оскільки зловмисники постійно вдосконалюють методи маскування своїх атак. Для ефективного виявлення фішингу застосовуються різні підходи, зокрема традиційні методи перевірки URL, SSL-сертифікатів та чорних списків, а також методи на основі машинного навчання, зокрема нейронні мережі [2].

Традиційні методи мають високу швидкість виявлення, однак обмежені у своїх можливостях. Вони здатні виявляти лише відомі шаблони атак і не можуть адаптуватися до нових методів маскування фішингу. Наприклад, фішингові сайти можуть використовувати довгі URL-адреси з великою кількістю піддоменів, що робить їх схожими на легітимні сайти. Такі атаки важко виявити за допомогою традиційних методів.

З іншого боку, методи машинного навчання, зокрема нейронні мережі, дозволяють створювати адаптивні моделі, які вивчають складні взаємозв'язки між різними ознаками сайту та фішинговою активністю. Вони здатні виявляти не лише стандартні шаблони атак, а й нові, раніше невідомі, базуючись на великих масивах даних. Це підвищує точність виявлення фішингових сайтів і дозволяє адаптувати систему до нових загроз. Однак ці методи можуть бути повільнішими порівняно з традиційними, оскільки потребують обробки великих даних і постійного донавчання [3].

Для більш детального порівняння традиційних методів і методів машинного навчання можна скористатися таблицею, яка відображає основні характеристики кожного підходу.

Таблиця 1 − Порівняння традиційних методів та методів машинного навчання

Характеристика	Традиційні методи	Методи машинного навчання
Тип аналізу:	Статичний (URL, SSL, чорні списки)	Динамічний (обробка великих даних)
Точність виявлення:	Обмежена, виявляються лише стандартні атаки	Висока, здатність адаптуватися до нових загроз
Швидкість виявлення:	Висока, але лише для відомих атак	Може бути дещо повільнішою, але точність значно вища
Адаптивність до нових загроз:	Низька, потребує оновлення чорних списків	Висока, адаптація до нових патернів фішингових атак

Аналіз порівняння показує, що традиційні методи мають високу швидкість виявлення, але їхня точність і здатність адаптуватися до нових фішингових методів є обмеженими. Водночас методи машинного навчання пропонують високий рівень точності та адаптивності, але за рахунок більшої складності та необхідності в обробці великих обсягів даних їхня швидкість виявлення може бути нижчою. В результаті поєднання традиційних методів перевірки та машинного навчання можна створити систему, яка здатна адаптуватися до нових загроз, забезпечуючи високу точність та ефективність виявлення фішингових сайтів.

Для реалізації цієї мети було обрано підхід на базі PHP-ML — бібліотеки для машинного навчання на PHP. Цей підхід дозволяє комбінувати традиційні методи перевірки з можливостями штучного інтелекту, зокрема нейронними мережами, що значно підвищує точність та здатність до адаптації [4].

Алгоритм побудови такої системи починається з попереднього збору характеристик сайтів. Зокрема, аналізуються такі параметри, як довжина URL, кількість доменних рівнів, наявність SSL-сертифікатів та час створення домену. Ці ознаки використовуються для попереднього відбору фішингових сайтів, завдяки чому система здатна на ранніх етапах виявити типові фішингові спроби. Традиційні методи, такі як перевірка наявності сайту в чорних списках чи перевірка HTTPS, допомагають фільтрувати вже відомі загрози, але їхня ефективність обмежена, оскільки нові фішингові сайти часто не встигають потрапити в ці списки.

Щоб покращити точність виявлення, використовуються нейронні мережі, зокрема модель Multilayer Perceptron (MLP). Для навчання мережі надаються числові вектори, що представляють різноманітні характеристики сайтів. Мережа здатна виявляти складні взаємозв'язки між цими ознаками, зокрема

аналізувати поєднання таких факторів, як короткий вік домену, відсутність HTTPS та наявність великої кількості редиректів [5].

Адаптивність системи забезпечується завдяки можливості донавчання нейронної мережі на нових даних. Це дозволяє моделі не лише виявляти нові фішингові сайти, а й постійно оновлювати свої ваги та враховувати зміни в поведінці зловмисників.

Таке поєднання класичних методів і методів машинного навчання надає значну перевагу в боротьбі з фішингом, оскільки дозволяє не лише виявляти нові загрози, але й адаптуватися до швидко змінюваного ландшафту інтернет-загроз.

Висновок

Підсумовуючи дане дослідження, можна зазначити, що використання нейронних мереж для виявлення фішингових сайтів дозволяє значно підвищити точність і адаптивність систем безпеки. Комбінація традиційних методів перевірки та машинного навчання забезпечує ефективне виявлення нових загроз та адаптацію до змін у поведінці зловмисників. Це дозволяє створити більш надійні та швидкі системи захисту від фішингових атак.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Федієнко О., Волівник Є., Липка С. Обережно! Кібершахраї. [Електронний ресурс] / Дія.юа // Дія.Освіта. — 2024. — Режим доступу: https://osvita.diia.gov.ua/courses/attention-cyber-fraudsters (дата звернення: 17.11.2024).
2. Гулак Г. Інформаційна та кібернетична безпека підприємства: навч. посіб. / Гулак Г., Жильцов О., Киричок Р — Львів: Марченко Т. В., 2024. — 368 с.
3. Яремчук Ю.Є. Основи інформаційної безпеки: навч. посіб. / Яремчук Ю.Є., Хорошко В.О., Дудикевич В.Б. — Вінниця: ВНТУ, 2018 — 317с.
4. Когут Ю. Штучний інтелект і безпека. / Консалтинг. компанія Сідкон — Київ, 2024 — 294с.
5. Mueller A., Guido S. Introduction to Machine Learning with Python: a guide for data scientists. / O'Reilly Media — Sebastopol, 2018 — 398с.

Фернега Євгеній Іванович – студент групи КІТС-23м, факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, Вінниця, e-mail: evgeniyfernega@gmail.com

Науковий керівник: ***Грищак Анатолій Васильович*** – кандидат технічних наук спеціальністю 125 «Кібербезпека», доцент кафедри менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, Вінниця, e-mail: grytsak.a.v@gmail.com

Fernega Yevheniy I. – student of KITS-23m group, Faculty of Management and Information Security, Vinnytsia National Technical University, Vinnytsia, e-mail evgeniyfernega@gmail.com

Supervisor: ***Hrytsak Anatoliy V.*** – Candidate of Technical Sciences in 125 "Cybersecurity", Associate Professor of the Department of Management and Security of Information Systems, Vinnytsia National Technical University, Vinnytsia, e-mail: grytsak.a.v@gmail.com