УДК: 004.056

Я. О. Піддубчак

Т. Г. Кирилащук

ВИЯВЛЕННЯ ТА ПОПЕРЕДЖЕННЯ ФІШИНГОВИХ АТАК У СУЧАСНИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ

Вінницький національний технічний університет

Анотація

У статті розглянуто проблему фішингових атак як однієї з найпоширеніших загроз для сучасних інформаційних систем. Визначено ефективні методи виявлення та попередження фішингу, зокрема з використанням машинного навчання. Доведено, що поєднання технічних засобів та організаційних заходів дозволяє значно підвищити рівень кіберзахисту.

Ключові слова: *фішинг; кібербезпека; машинне навчання; інформаційні системи; соціальна інженерія.*

Abstract

The article examines the problem of phishing attacks as one of the most common threats to modern information systems. Effective methods of detection and prevention of phishing, in particular using machine learning, are identified. It is proved that the combination of technical means and organizational measures can significantly increase the level of cybersecurity.

Key words: *phishing; cybersecurity; machine learning; information systems; social engineering.*

Вступ

Фішингові атаки й надалі становлять одну з найпоширеніших кіберзагроз, що суттєво впливають на стабільність функціонування цифрової інфраструктури. Кількість інцидентів щороку зростає, а методи, які використовують зловмисники, постійно ускладнюються: удосконалюються способи підробки вебресурсів, активніше застосовуються технології штучного інтелекту та інструменти соціальної інженерії. Фішинг — це серйозна проблема безпеки в мережі, яка полягає в підробці справжніх веб-сайтів, щоб обдурити користувачів в інтернеті і вкрасти їх конфіденційну інформацію. Проводячи аналіз даних визначень можна зробити висновок, що «фішинг» можна розглядати по різному, однак основна мета його проведення залишається незмінною — викрадення даних. Це обумовлює потребу у впровадженні сучасних підходів, здатних оперативно ідентифікувати потенційно небезпечні ресурси.

У дослідженні застосовано методи аналізу наукових джерел, класифікації фішингових атак, а також економіко-статистичні підходи для оцінювання зміни масштабу кіберзагроз упродовж останніх років. Основне припущення роботи полягає в тому, що поєднання методів машинного навчання з аналізом контентних та технічних характеристик вебсторінок може суттєво підвищити точність виявлення фішингу. Додаткову увагу приділено оцінці тенденцій розвитку інструментів атак та факторів, що впливають на їхню ефективність у різних цифрових середовищах.

Результати дослідження

Проведений аналіз наукових джерел та узагальнення статистичних даних дозволили встановити низку важливих закономірностей щодо розвитку фішингових атак та ефективності застосовуваних засобів протидії. Насамперед підтверджено суттєве зростання кількості фішингових інцидентів упродовж 2021–2024 рр., що пов'язано з активним використанням автоматизованих платформ для створення фішингових ресурсів та появою інструментів, здатних генерувати персоналізовані фішингові повідомлення за допомогою методів штучного інтелекту. Це спричинило підвищення рівня складності атак, у тому числі завдяки адаптивним сценаріям, що змінюються залежно від поведінки користувача.

Під фішингом розуміють процес введення в оману чи соціального примусу жертви до передачі конфіденційної інформації для зловмисного використання[1].

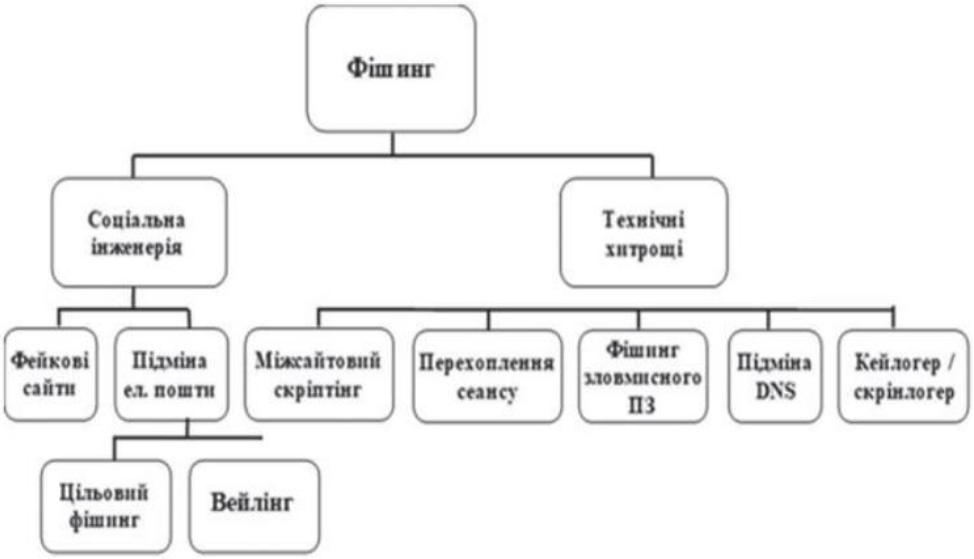

Рисунок 1 – Класифікація фішинг-атак[1]

Під конфіденційною інформацією користувачів в розрізі фішингової атаки розуміють:

- логін та пароль для входу в мобільні застосунки;
- номер, термін дії, CVV2/CVC2, ПІН платіжної картки;
- одноразові паролі підтвердження операцій;
- адреса електронної пошти;
- фінансовий номер телефону;
- слово – пароль до картки, відповіді на секретні питання.

Небезпечність фішингу обумовлена передусім прямою фінансовою шкодою, яку він завдає[1].

Економіко-статистичний аналіз динаміки поширення фішингових загроз підтвердив, що найбільші темпи зростання демонструють атаки, спрямовані на

банківський сектор, сервіси електронної комерції та хмарні корпоративні системи[5]. Зокрема, окремі дослідження вказують, що частка фішингових інцидентів, орієнтованих на викрадення банківських даних, перевищила інші типи атак і зросла приблизно на третину за останні три роки[5]. Крім того, збільшується кількість випадків компрометації корпоративних облікових записів через підроблені сторінки авторизації, зокрема у хмарних сервісах.

Під час аналізу існуючих технічних підходів встановлено, що найефективнішими є системи, які поєднують декілька типів ознак — сигнатурні, технічні, контентні та поведінкові. Такі системи дозволяють здійснювати багатовимірний аналіз кожного вебресурсу, що істотно підвищує точність класифікації. Зокрема, визначено такі ключові групи ознак:

- структурні ознаки URL (довжина рядка, кількість параметрів, використання IP-адреси замість доменного імені, аномальні символи та енкодинг);
- технічні параметри вебресурсу (метадані SSL-сертифікатів, швидкість змін DNS-записів, наявність прихованих редиректів, ознаки fast-flux);
- контентні характеристики (наявність елементів, що копіюють дизайн офіційних сайтів, вставка підроблених форм авторизації, некоректно завантажені ресурси);
- візуальні та графічні ознаки (співставлення з шаблонами легітимних інтерфейсів, аналіз логотипів та кольорових схем за допомогою комп'ютерного зору);
- поведінкові патерни (аномальні взаємодії з користувачем, швидке оновлення сторінки, автоматичне перенаправлення без явної причини)[2].

На основі оброблених наукових даних визначено, що застосування алгоритмів машинного навчання, зокрема ансамблевих моделей (Random Forest, Gradient Boosting, XGBoost) та глибинних нейронних мереж, дозволяє досягати точності виявлення фішингових ресурсів у межах 95–99%. Перевагою таких моделей є здатність адаптуватися до появи нових атак шляхом перенавчання на оновлених вибірках, що включають сучасні приклади фішингових сторінок[4].

Окрему увагу приділено аналізу гібридних систем, що поєднують машинне навчання з методами аналізу природної мови, комп'ютерного зору та евристичними алгоритмами[4]. Такі системи демонструють підвищену ефективність у виявленні фішингу, який замасковано під популярні вебресурси та сервіси державних установ. Доведено, що гібридні підходи здатні успішно ідентифікувати фішингові сторінки навіть у випадках, коли URL-адреса та технічні параметри не мають виражених ознак підозрілості.

Важливим результатом є також встановлення залежності між рівнем цифрової грамотності користувачів і вразливістю до фішингу. Дослідження показали, що впровадження системного навчання персоналу та регулярних тренінгів з розпізнавання фішингових повідомлень знижує ймовірність успішної атаки на 30–50%. Це підтверджує необхідність поєднання технічних рішень із організаційними заходами, що формують культуру інформаційної безпеки в організаціях[3].

Крім того, визначено, що впровадження багатофакторної автентифікації, використання токенів доступу, контроль аномальної активності та застосування принципу Zero Trust значно обмежують можливості зловмисників отримати доступ до конфіденційних даних навіть у разі часткової компрометації облікового запису[3]. Це підкреслює важливість комплексного підходу до безпеки, у межах якого технічні та людські фактори взаємодоповнюють один одного.

ВИСНОВКИ

У результаті проведеного дослідження встановлено, що фішинг залишається однією з ключових загроз для інформаційних систем, а його методи постійно вдосконалюються. Визначено основні види фішингових атак і напрями їх виявлення. Класифіковано сучасні технології протидії фішинговим загрозам, серед яких особливо ефективними є моделі, побудовані на машинному навчанні. Аргументовано, що поєднання технічних засобів і організаційних заходів є найрезультативнішим підходом до зниження ризику фішингових інцидентів. Отримані результати можуть бути використані для вдосконалення систем кіберзахисту в організаціях різних рівнів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. *Штонда Р., Черниш Ю., Терещенко Т. та ін. Класифікація та методи виявлення фішингових атак. Кібербезпека: освіта, наука, техніка, 2024. DOI: 10.28925/2663-4023.2024.24.6980.*
2. *A Systematic Review of Deep Learning Techniques for Phishing Email Detection. MDPI.*
3. *Staying ahead of phishers: a review of recent advances and emerging methodologies in phishing detection - Artificial Intelligence Review. SpringerLink.*
4. *Pal R., Pandey M. K., Pal S., Yadav D. C., Phishing Detection: A Hybrid Model with Feature Selection and Machine Learning Techniques. International Journal of Experimental Research and Review, Vol. 36, 2023*
5. *Татомир І. Кібербезпека університетів як спосіб протидії фішинговому шахрайству. Економічний дискурс, 2020. DOI: 10.36742/2410-0919-2020-1-7.*

***Піддубчак Яна Олександрівна** – студентка групи 2КІТС-24б, факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, м. Вінниця, e-mail: viaan23ok@gmail.com*

***Науковий керівник: Тетяна Генадіївна Кирилащук** – асистент кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця, e-mail: kgt0998@gmail.com.*

***Piddubchak Yana Oleksandrivna** – student of group 2KITS-24b, Faculty of Management and Information Security, Vinnytsia National Technical University, Vinnytsia, e-mail: viaan23ok@gmail.com*

Supervisor: Tatiana G. Kyrylashchuk *– Assistant of the Department of Information Protection, Vinnytsia National Technical University, Vinnytsia, e-mail: kgt0998@gmail.com.*