НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»

ФАКУЛЬТЕТ КІБЕРБЕЗПЕКИ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

28 листопада 2025 року

КІБЕРБЕЗПЕКА В СУЧАСНОМУ СВІТІ: АКТУАЛЬНІ ВИКЛИКИ

МАТЕРІАЛИ VI МІЖНАРОДНОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Одеська юридична академія»
Факультет кібербезпеки та інформаційних технологій
Кафедра кібербезпеки

КІБЕРБЕЗПЕКА В СУЧАСНОМУ СВІТІ: АКТУАЛЬНІ ВИКЛИКИ

МАТЕРІАЛИ VI МІЖНАРОДНОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

28 листопада 2025 року, м. Одеса

Одеса, 2025

MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE
National University «Odesa Law Academy»
Faculty of Cybersecurity and Information Technologies
Department of Cybersecurity

CYBERSECURITY IN TODAY'S WORLD: ACTUAL CHALLENGES

MATERIALS OF THE VI INTERNATIONAL SCIENTIFIC AND PRACTICAL CONFERENCE

November 28, 2025, Odesa

Odesa, 2025

УДК 004.056

Відповідальній редактор:

О. В. Дикий, декан факультету кібербезпеки та інформаційних технологій, кандидат юридичних наук, доцент

Матеріали видано в авторській редакції.
Повну відповідальність за достовірність та якість поданого матеріалу несуть учасники конференції, їхні наукові керівники, які рекомендували ці матеріали до друку.

Рекомендовано до друку
Вченою радою Національного університету
«Одеська юридична академія»
(протокол №3 від 29.11.2025 р.)

Матеріали Міжнародної науково-практичної конференції «Кібербезпека в сучасному світі: актуальні виклики» (м. Одеса, 28 листопада 2025 р.). Одеса, 2025. 287 с.

У конференції взяли участь студенти, аспіранти, молоді вчені, викладачі та науковці. Конференція проводиться на базі Національного університету «Одеська юридична академія».

UDC 004.056

Editor-in-chief:

O. V. Dykyi, Dean of the Faculty of Cybersecurity and Information Technologies,
Candidate of Law, Associate Professor

The materials were published in the author's edition.
Full responsibility for the reliability and quality of the submitted material
bears the participants of the conference, their scientific supervisors,
who recommended these materials for publication.

Recommended for printing
by the Academic Council of the National University
«Odesa Law Academy»
(Minutes No. 3 dated 11/29/2025)

Materials of the International Scientific and Practical Conference «Cybersecurity in the Modern World: Current Challenges» (Odessa, November 28, 2025). Odesa, 2025. 287 p.

The conference was attended by students, postgraduates, young scientists, teachers and researchers. The conference is held at the National University «Odesa Law Academy».

VI Міжнародна науково-практична конференція

«Кібербезпека в сучасному світі: актуальні виклики»

28 листопада 2025 року

ТЕМАТИЧНІ НАПРЯМКИ КОНФЕРЕНЦІЇ:

Секція 1. Алгоритмічні та технічні аспекти кібербезпеки

Секція 2. Штучний інтелект та інформаційні технології

Секція 3. Управлінські, соціальні та психологічні аспекти взаємодії з кіберпростором

Секція 4. Нормативно-правові засади кібербезпеки та захисту інформації

E-mail: kiberprostirconf@gmail.com (Для питань та тез)

VI International Scientific and Practical Conference

«Cybersecurity in today's world: actual challenges»

28 November 2025 year

THEMATIC DIRECTIONS OF THE CONFERENCE:

Section 1. Algorithmic and technical aspects of cybersecurity

Section 2. Artificial intelligence and information technologies

Section 3. Management, social and psychological aspects of interaction with cyberspace

Section 4. Regulatory and legal principles of cybersecurity and information protection

E-mail: kiberprostirconf@gmail.com (Для питань та тез)

СТВОРЕННЯ ФІШИНГОВОГО СЦЕНАРІЮ ТА АНАЛІЗ РЕАКЦІЇ КОРИСТУВАЧІВ

Тинкевич Дана

студентка 4-го курсу факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

Фішинг залишається однією з найпоширеніших і найрезультативніших форм кібератак, спрямованих на компрометацію конфіденційних даних користувачів і організацій. Сучасні фішингові повідомлення та вебсторінки дедалі точніше імітують легітимні сервіси, використовуючи знання про поведінкові особливості та емоційні тригери людини. Попри розвиток технічних засобів захисту, ефективність протидії фішингу значною мірою обмежується людським фактором. У цьому контексті навчальні фішингові симуляції є важливим інструментом для виявлення реальних поведінкових вразливостей і формування практичних навичок кібергігієни.

Незважаючи на значну кількість публікацій, присвячених технічним аспектам виявлення та блокування фішингових атак, значно менш дослідженим залишається поведінковий аспект взаємодії користувачів із фішинговими ресурсами, зокрема в умовах, наближених до реальних. Більшість наявних робіт зосереджується на автоматизованих методах захисту, тоді як емпіричні дослідження реакції користувачів у контрольованих навчальних симуляціях є обмеженими. Це ускладнює формування практично орієнтованих рекомендацій, спрямованих на зниження впливу людського фактора в системах інформаційної безпеки.

Метою даної роботи є розроблення навчального фішингового сценарію та дослідження на його основі поведінки користувачів під час взаємодії з підробною сторінкою автентифікації, з подальшою оцінкою чинників, що впливають на успішність атаки, та формуванням практичних рекомендацій щодо підвищення рівня захисту від фішингових загроз.

Фішинг – це форма соціальної інженерії, коли зловмисник під виглядом легітимного сервісу або особи змушує жертву розкрити конфіденційні дані (логіни, паролі, платіжні реквізити) або виконати небезпечну дію (завантажити шкідливий файл, перейти за посиланням) [1].

Фішингові атаки можуть бути класифіковані за цілями та каналами реалізації. Зокрема, класичний (масовий) фішинг передбачає розсилання великої кількості електронних листів або повідомлень із посиланнями на підроблені ресурси. Цільовий фішинг (spear-phishing) спрямований на конкретну особу або роль та використовує персоналізовану інформацію про жертву. Окремим різновидом є whaling, що орієнтований на керівників і посадових осіб високого рівня. Залежно від каналу комунікації виділяють smishing та vishing, які реалізуються відповідно через SMS-повідомлення та

голосові дзвінки. Крім того, pharming базується на перенаправленні користувачів на фальшиві вебресурси на рівні DNS або шляхом компрометації мережевої інфраструктури, тоді як clone phishing полягає у створенні копії легітимного повідомлення з підміною гіперпосилання на фішингове [2].

Фішингова атака зазвичай реалізується не як одноразова дія, а як послідовний багатоетапний процес, у межах якого зловмисник поєднує технічні та соціально-інженерні прийоми. Аналіз структури фішингових кампаній дозволяє виокремити ключові етапи, кожен з яких відіграє окрему роль у досягненні кінцевої мети:

1. *Розвідка* – збір публічної інформації про ціль (профілі, контакти, корпоративна структура).
2. *Створення приманки* – дизайн листа/сторінки, імітація бренду (логотипи, стилістика, мова).
3. *Доставка* – вибір каналу (email, месенджери, соцмережі, SMS).
4. *Захоплення даних* – сторінки введення, форми, скрипти для логування.
5. *Використання* – доступ до акаунтів, фінансові операції, ескалація атак.

Ефективність фішингових атак значною мірою зумовлена використанням психологічних механізмів впливу на користувачів. Застосування відчуття терміновості, апеляція до страху втрати (наприклад, можливого блокування облікового запису), обіцянка потенційної вигоди, імітація авторитетного джерела, а також персоналізація повідомлень у сукупності знижують рівень критичного сприйняття інформації та істотно підвищують імовірність введення конфіденційних даних користувачем.

Для досягнення поставленої мети було розроблено навчальний фішинговий сценарій, реалізований у вигляді контрольованої технічної симуляції. Технічна частина дослідження спрямовувалася на відтворення типових елементів фішингової атаки в безпечному ізольованому середовищі з дотриманням етичних вимог та мінімізацією потенційних ризиків для учасників експерименту:

- Застосовано ізольовану тестову інфраструктуру (локальний сервер на LAMP/LEMP) для безпечного проведення експерименту.
- Створено HTML/CSS/JS-шаблон, що імітує сторінку входу популярного сервісу, без викликів до реальних доменів.
- Серверна частина (Python/Flask) забезпечувала логування анонімізованих введень у файл або базу даних; дані шифрувалися і не зберігалися довгостроково.

- Після введення користувачу показувалось нейтральне повідомлення або перенаправлення, щоб не викликати додаткових підозр.

- Дотримано етичних обмежень: участь тільки за письмовою згодою, відсутність збору реальних паролів від робочих систем, подальше інформування учасників та навчальні матеріали після завершення.

У межах експериментального сценарію учасникам, об'єднаним у закриту навчальну групу, надсилалося повідомлення з пропозицією виконати дію, що імітувала типову фішингову комунікацію (наприклад, перевірити обліковий запис або отримати результат). Повідомлення містило посилання на підробну сторінку автентифікації, на якій користувачам пропонувалося ввести логін і пароль. Усі введені дані фіксувалися в анонімізованому вигляді виключно з дослідницькою метою. Після завершення експерименту учасники отримували роз'яснення щодо характеру проведеної симуляції та навчальні матеріали з основ кібергігієни.

Для оцінювання результатів експерименту було сформовано систему кількісних і якісних показників, що характеризують поведінкові реакції користувачів під час взаємодії з навчальним фішинговим сценарієм. Узагальнення отриманих даних засвідчило наявність стійких поведінкових патернів, пов'язаних із реагуванням на фішингові стимули. Зокрема, було зафіксовано переходи за фішинговим посиланням та введення облікових даних без попередньої перевірки доменного імені або параметрів безпеки з'єднання, тоді як випадки звернення уваги на потенційно підозрілі ознаки ресурсу мали поодинокий характер. Аналіз часових характеристик взаємодії, відмов від введення даних і звернень за допомогою свідчить про те, що застосування базових соціально-інженерних тригерів, зокрема терміновості та апеляції до авторитету, позитивно корелює з ефективністю навіть технічно простих імітацій інтерфейсу.

Висновки. У ході дослідження було продемонстровано, що ефективність фішингових атак значною мірою визначається не технічною складністю підробки, а якістю соціально-інженерного впливу. Отримані результати свідчать про те, що правильно сформульована легенда, використання психологічних тригерів і форма комунікації здатні забезпечувати високу результативність навіть за умови спрощеної візуальної імітації інтерфейсу.

Аналіз поведінкових реакцій користувачів підтвердив домінуючу роль людського фактора в сучасних загрозах фішингу. Це зумовлює необхідність поєднання технічних засобів захисту, зокрема двофакторної автентифікації, антифішингових фільтрів, механізмів захищеного DNS і контролю сертифікатів, із системними організаційними та освітніми заходами. Регулярні тренінги, контрольовані симуляції фішингових атак і формування культури

інформаційної безпеки істотно підвищують здатність користувачів розпізнавати загрози та коректно реагувати на інциденти.

Окрему увагу в роботі приділено етичним і правовим аспектам проведення навчальних фішингових симуляцій. Показано, що подібні дослідження є допустимими виключно за умов інформованої згоди учасників, мінімізації потенційної шкоди, прозорості методики та обов'язкового видалення чутливих даних після завершення аналізу.

Практична значущість отриманих результатів полягає в можливості їх застосування під час розроблення програм підвищення обізнаності з кібербезпеки, створення внутрішніх регламентів реагування на фішингові інциденти та впровадження обов'язкових механізмів багатофакторного захисту в освітніх і корпоративних інформаційних системах.

Список використаної літератури:

1. Putra F. P. E. et al. Analysis of phishing attack trends, impacts and prevention methods: literature study. Brilliance: Research of Artificial Intelligence. 2024. Vol. 4, No. 1. P. 413-421.
2. Alghenaim M. F. et al. Phishing attack types and mitigation: A survey. The International Conference on Data Science and Emerging Technologies. Singapore : Springer Nature Singapore, 2022. P. 131-153.

Ключові слова: фішинг, фішингова атака, поведінкові вразливості, людський фактор, соціальна інженерія, навчальна фішингова симуляція, кібергігієна, аналіз реакції користувачів, кібербезпека.
Keywords: phishing, phishing attack, behavioral vulnerabilities, human factor, social engineering, educational phishing simulation, cyber hygiene, user reaction analysis, cybersecurity.

СИСТЕМА ВИЯВЛЕННЯ ВТОРГНЕНЬ ЗА ДОПОМОГОЮ ТЕХНОЛОГІЇ БЛОКЧЕЙН ДЛЯ ЗАХИСТУ ЛОГІВ

Бойко Віктор

доцент кафедри кібербезпеки Національного університету «Одеська юридична академія», кандидат технічних наук

Вуль Анастасія

студентка 4-го курсу факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

Сучасні інформаційно-комунікаційні системи (ІКС) генерують величезні обсяги логів – журналів подій, що є основним джерелом інформації для моніторингу, виявлення інцидентів безпеки та розслідування кібератак [1]. Саме на основі логів фахівці з кібербезпеки визначають, коли і як відбулося

ЗМІСТ