УДК 316.776:004.58 DOI: 10.31673/2412-4338.2026.019013

Коршун Наталія Володимирівна
доктор технічних наук, професор, професор кафедри інформаційної
та кібернетичної безпеки імені професора Володимира Бурячка
Київський столичний університет імені Бориса Грінченка
ORCID ID: 0000-0003-2908-970X
n.korshun@kubg.edu.ua

Бондарчук Андрій Петрович
доктор технічних наук, професор, завідувач кафедри комп'ютерних наук
Київський столичний університет імені Бориса Грінченка
ORCID ID: 0000-0001-5124-5102
a.bondarchuk@kubg.edu.ua

Складанний Павло Миколайович
кандидат технічних наук, доцент, завідувач кафедри інформаційної
та кібернетичної безпеки імені професора Володимира Бурячка
Київський столичний університет імені Бориса Грінченка
ORCID ID: 0000-0002-7775-6039
p.skladannyi@kubg.edu.ua

Соколов Володимир Юрійович
кандидат технічних наук, доцент, доцент кафедри інформаційної
та кібернетичної безпеки імені професора Володимира Бурячка
Київський столичний університет імені Бориса Грінченка
ORCID ID: 0000-0002-9349-7946
v.sokolov@kubg.edu.ua

Крижанівська Тетяна Миколаївна
здобувач освіти кафедри інформаційної
та кібернетичної безпеки імені професора Володимира Бурячка
Київський столичний університет імені Бориса Грінченка
ORCID ID: 0009-0002-8036-9539
tmkryzhanivska.fitm24m@kubg.edu.ua

МОДЕЛЮВАННЯ ТА РЕАЛІЗАЦІЯ АТАК СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ

Анотація. *Соціотехнічні атаки, зокрема фішингові, залишаються однією з найпоширеніших загроз інформаційній безпеці, оскільки вони експлуатують когнітивні упередження користувачів поряд із технічними вразливостями систем. Людина як найслабша ланка в системі безпеки стає основною мішенню для маніпуляцій, що базуються на її емоціях, довірі чи недостатній обізнаності. Соціальна інженерія виступає первинним вектором, що відкриває шлях для технічних методів, утворюючи єдину атаку. У контексті сучасних викликів, наприклад, під час гібридних війн зловмисники можуть використовувати соціальну інженерію для поширення дезінформації, поєднавши цей процес з технічними атаками на критичну інфраструктуру. Це робить такі атаки загрозою для національної безпеки, вимагаючи інтеграції психологічних і технологічних стратегій захисту. Захист від соціотехнічних атак вимагає комплексного підходу, що включає освіту персоналу, симуляцію атак та використання автоматизованих систем виявлення У статті розглядається моделювання та практична реалізація симуляції фішингових атак із застосуванням платформи GoPhish. Представлено методику проєктування кампаній, яка включає створення шаблонів повідомлень, налаштування кампаній, автоматизований збір та моніторинг поведінки користувачів у реальному часі. Дані, отримані під час симуляцій, аналізуються для виявлення поведінкових патернів і оцінки вразливості окремих підрозділів організації. На основі результатів формуються рекомендації щодо підвищення ефективності багаторівневого захисту, який інтегрує дані з кількох кампаній, забезпечуючи довготривалий моніторинг і зниження ризику атак. Використання автоматизованих платформ для симуляції фішингових кампаній створює контрольоване*

середовище для вивчення соціальної інженерії, що сприяє як проведенню досліджень, так і підвищенню обізнаності користувачів.

Ключові слова: *кібербезпека; соціальна інженерія; фішинг; атака; вразливість.*

Nataliia Korshun
Doctor of Science, Professor, Professor of the Department of
Information and Cyber Security named after Professor Volodymyr Buriachok
Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine
ORCID ID: 0000-0003-2908-970X
n.korshun@kubg.edu.ua

Andrii Bondarchuk
Doctor of Science, Professor, Head of the Department of Computer Science
Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine
ORCID ID: 0000-0001-5124-5102
a.bondarchuk@kubg.edu.ua

Pavlo Skladannyi
PhD, Associate Professor, Head of the Department of
Information and Cyber Security named after Professor Volodymyr Buriachok
Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine
ORCID ID: 0000-0002-7775-6039
p.skladannyi@kubg.edu.ua

Volodymyr Sokolov
PhD, Associate Professor, Associate Professor of the Department of
Information and Cyber Security named after Professor Volodymyr Buriachok
Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine
ORCID ID: 0000-0002-9349-7946
v.sokolov@kubg.edu.ua

Tetiana Kryzhanivska
Master of the Department of Information and Cyber
Security named after Professor Volodymyr Buriachok
Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine
ORCID ID: 0009-0002-8036-9539
tmkryzhanivska.fitm24m@kubg.edu.ua

MODELING AND EXECUTION OF SOCIAL ENGINEERING ATTACKS

Abstract. *Social engineering attacks, particularly phishing, remain among the most prevalent threats to information security, as they exploit users' cognitive biases alongside technical system vulnerabilities. Humans, being the weakest link in the security chain, become the primary targets for manipulations based on emotions, trust, or insufficient awareness. Social engineering acts as the initial vector that paves the way for technical methods, forming a unified attack. In the context of modern challenges, such as hybrid warfare, attackers can use social engineering to spread disinformation while combining it with technical attacks on critical infrastructure. This makes such attacks a national security concern, requiring the integration of psychological and technological defense strategies. Protection against social engineering attacks necessitates a comprehensive approach that includes personnel education, attack simulations, and the use of automated detection systems. This paper examines the modeling and practical implementation of phishing attack simulations using the GoPhish platform. A methodology for campaign design is presented, encompassing message template creation, campaign configuration, automated data collection, and real-time monitoring of user behavior. Data obtained during simulations are analyzed to identify behavioral patterns and assess the vulnerability of specific organizational units. Based on the results, recommendations are formulated to enhance the effectiveness of multi-layered defenses, integrating data from multiple campaigns to enable long-term monitoring and risk mitigation. The use of automated platforms for simulating phishing campaigns provides a controlled environment for studying social engineering, supporting both research activities and the improvement of user awareness.*

Keywords: *cybersecurity; social engineering; phishing; attack; vulnerability.*

1. Вступ.

В сучасних умовах цифровізації та зростання обсягів електронних комунікацій атаки соціальної інженерії набули статусу одного з найнебезпечніших і водночас найскладніших для протидії класів кіберзагроз. На відміну від традиційних технічних атак, соціальна інженерія ґрунтується на маніпулюванні людською поведінкою, когнітивними упередженнями та емоційними реакціями користувачів, що суттєво знижує ефективність класичних технічних засобів захисту.

Незважаючи на значну кількість досліджень, присвячених окремим аспектам соціальної інженерії, існуючі підходи до її моделювання та реалізації залишаються фрагментарними та недостатньо узгодженими. Більшість моделей зосереджені або на технічних характеристиках атак, або на психологічних чинниках, не забезпечуючи цілісного соціотехнічного представлення процесу атаки. Водночас відсутні уніфіковані формальні моделі, які б адекватно відображали динаміку багатокрокових атак соціальної інженерії, їх адаптивність до контексту та індивідуальних характеристик жертви.

Додатковою проблемою є обмежена кількість реалістичних імітаційних середовищ і стандартних сценаріїв, що ускладнює відтворюваність експериментів, порівняльну оцінку моделей та перевірку ефективності методів виявлення і протидії. Існуючі реалізації атак часто базуються на спрощених або статичних сценаріях, які не відображають сучасні тенденції розвитку соціальної інженерії, зокрема багатоканальність, використання генеративного штучного інтелекту та тривалу психологічну взаємодію з ціллю.

Таким чином, актуальною науковою проблемою є розробка та вдосконалення підходів до моделювання і реалізації атак соціальної інженерії, які б поєднували психологічні, поведінкові та технічні аспекти, забезпечували формалізований опис атак, можливість їх імітації в контрольованих середовищах і створювали наукове підґрунтя для побудови більш ефективних методів виявлення, оцінювання ризиків і протидії цим атакам.

2. Аналіз останніх досліджень і публікацій.

Соціальна інженерія – це специфічний тип кібератаки, яка використовує людську психологію та соціальну взаємодію для порушення безпеки, часто з мінімальним технічним хакерством або без нього, тоді як соціотехнічні атаки – це ширший підклас соціальної інженерії, який навмисно поєднує як соціальні, так і технічні підходи в одній атаці.

Соціальна інженерія — це метод психологічної маніпуляції людьми для отримання конфіденційної інформації, доступу до систем чи ресурсів без використання суто технічних засобів. Вона фокусується на експлуатації людських слабкостей (наприклад, авторитет, прихильність, терміновість чи соціальний доказ) через обман, фішинг, претекстинг (видавання себе за іншу особу), бейтинг (поширення шкідливих файлів під виглядом корисних) чи вішинг (телефонні дзвінки). Це часто слугує як етап розвідки: атакувальник збирає дані про жертву (логіни, паролі, структуру системи), не обов'язково проникаючи в технічну інфраструктуру. За оцінками, соціальна інженерія забезпечує 35–95% інформації для подальших атак і є причиною понад 70% порушень безпеки через людський фактор. Основні аспекти соціальної інженерії:

– широко визначається як атаки, що використовують людські вразливості (довіру, емоції, когнітивні упередження) через вплив, переконання, обман та маніпуляції для порушення конфіденційності, цілісності або доступності цифрових активів [1–4];

– традиційно розглядається як нетехнічне вторгнення, зосереджене на людях, а не на системах [1, 3, 5], але сучасні дослідження підкреслюють, що SE також може включати технічні компоненти, такі як фішингові веб-сайти, шкідливе програмне забезпечення або CSRF [1–3].

Соціотехнічна атака — це комплексний тип кіберзагрози, що поєднує соціальні (психологічні) та технічні (програмні, мережеві) елементи для порушення безпеки соціотехнічних систем, тобто систем, де люди взаємодіють з технологіями. Вона включає етапи: визначення мети, збір інформації (часто через соціальну інженерію), створення умов для впливу (наприклад, через стрес чи гостру потребу жертви) та безпосереднє проникнення (використання шкідливого програмного забезпечення, експлуатація вразливостей). Приклади: фальшиві pop-ups з malware, дзвінки для доступу до баз даних чи комбіновані атаки з advanced persistent threats. Мета — не просто збір даних, а повний несанкціонований доступ, витік інформації чи порушення роботи системи, з урахуванням моделювання вразливостей (наприклад, через ймовірнісні моделі реакцій користувачів). Основні аспекти соціотехнічної атаки:

– у розширених таксономіях атаки соціальна інженерія поділяються на фізичні, технічні, соціальні та соціотехнічні категорії;

– соціотехнічна атака визначається як використання поєднання соціальних та технічних підходів в одній кампанії: соціальні тактики будують довіру та спонукають до дії, тоді як технічні механізми фактично захоплюють облікові дані, встановлюють шкідливе програмне забезпечення або отримують доступ до систем;

– приклади включають «цькування» (наприклад, шкідливий USB-накопичувач) та фішинг за допомогою спеціально створених електронних листів та посилань-експлойтів, де переконання та технічне навантаження є важливими [6].

У кібербезпеці соціальна інженерія часто є «вхідною точкою» для соціотехнічної атаки: спочатку маніпулюють людиною для збору даних, а потім застосовують технічні засоби для проникнення (див. табл. 1). Наприклад, фішингова електронна пошта (соціальна інженерія) може призвести до встановлення malware (соціотехнічна атака). Захист від обох вимагає комбінації: тренінгів для персоналу, технічних засобів (файрволи, шифрування) та пентестів (симуляція атак).

Таблиця 1

Порівняльний аналіз соціальної інженерії та соціотехнічної атаки

Аспект	Соціальна інженерія	Соціотехнічна атака
Мета	Розвідка та збір інформації (підготовка атаки); 35–95% даних для подальших дій.	Повна реалізація атаки: несанкціонований доступ, витік даних чи порушення системи; включає розвідку, але йде далі.
Фокус	Вузький: психологічна маніпуляція людьми (людський фактор як основна вразливість).	Широкий: гібрид соціальних і технічних елементів (люди + технології, мережі, програмного забезпечення).
Методи	Десять, претекстинг, фішинг, вішинг, бейтинг; без обов'язкового технічного втручання.	Поєднання соціальної інженерії з технічними інструментами (malware, експлойти); структурований алгоритм (наприклад, схема Шейнова: мета → збір даних → вплив → доступ).
Складність	Простіша, часто одноступенева (маніпуляція для розголошення).	Складніша, системна (моделювання уразливостей, ймовірності успіху, взаємодія користувач-хост-ресурс).
Відношення	Часто є інструментом або початковим етапом соціотехнічної атаки.	Включає соціальну інженерію як компонент, але додає технічний шар для повного ефекту.

Дослідження соціальної інженерії у сучасній науковій літературі зосереджуються як на глибинному аналізі психологічних механізмів впливу, так і на технічних аспектах виявлення та симуляції таких атак. Зокрема, низка робіт підкреслює зростання складності фішингових атак у контексті використання новітніх технологій штучного інтелекту. Так, дослідження [7] систематизує знання про фішинг, створений генеративними моделями мови, і формулює рамкову модель GenCharDef для опису особливостей таких атак, включно з їх генерацією, характеристиками та стратегіями захисту, що дозволяє краще розуміти сучасний ландшафт загроз і виклики для систем захисту. Окремі дослідження акцентують увагу на психологічних аспектах соціальної інженерії як стратегії маніпуляції. Наприклад, робота [8] систематично узагальнює принципи переконання, що використовуються в фішингових атаках, і вказує на прогалини у розумінні їх впливу, підкреслюючи необхідність подальших досліджень і глибшого психологічного аналізу таких методів впливу.

У широкому контексті впливу сучасних технологій на соціальну інженерію, дослідження [9] аналізує роль генеративного штучного інтелекту в посиленні ефективності атак за рахунок створення реалістичного контенту, просунутого таргетування та автоматизованої інфраструктури, що значно ускладнює традиційні підходи до захисту. Окремі приклади емпіричних робіт демонструють успішність моделей симуляції фішингових атак у контексті оцінювання поведінки користувачів.

Дослідження [10] моделює фішингові сценарії і показує, що такі симуляції є ефективним інструментом для вивчення реакцій жертв, а також для оцінювання ефективності методів виявлення з використанням машинного навчання та евристичного аналізу. Робота [11] демонструє, що інтерактивні симуляції фішингових атак значно підвищують здатність співробітників розпізнавати шкідливі повідомлення, що підкреслює практичну цінність таких інструментів у навчальних та корпоративних контекстах. Дослідженню моделей атак соціальної інженерії присвячена робота [12], автори якої інтегрують підходи з психології, соціології та кібербезпеки. Також дослідження останніх років висвітлюють актуальні підходи до виявлення фішингових повідомлень на основі машинного навчання, зокрема пропозиції концептуальних моделей із застосуванням методів опорних векторів для аналізу великих обсягів даних і підвищення точності розпізнавання загроз [13].

Загалом, огляд джерел демонструє, що дослідження загроз соціальної інженерії, зокрема фішингових атак, передбачають інтеграцію психологічних, технічних та технологічних аспектів.

3. Мета і задачі дослідження.

Метою дослідження є практична реалізація симуляції фішингових атак як різновиду атак соціальної інженерії з використанням платформи GoPhish, а також оцінювання її можливостей для відтворення соціотехнічних сценаріїв, аналізу поведінки користувачів і формування експериментальної бази для подальшого вдосконалення методів виявлення та протидії атакам соціальної інженерії.

4. Результати дослідження.

Сучасні соціотехнічні загрози, зокрема фішингові атаки, потребують застосування багатовимірних стратегій захисту, які виходять за межі суто технічних рішень і включають програмні та організаційні механізми (рис.1). Такий підхід базується на усвідомленні того, що основні вразливості формуються на перетині людського чинника й інформаційних технологій, а отже ефективна протидія можлива лише за умови інтеграції різних методів у цілісну систему безпеки.

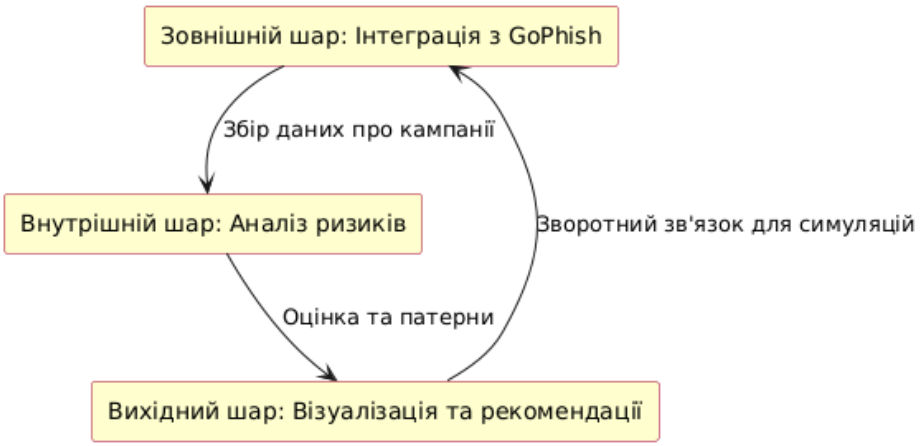

Рис. 1. Багаторівнева структура захисту в системі AntiPhishing

Для проведення симуляції фішингових атак у рамках дослідження була розроблена спеціалізована система AntiPhishing, яка інтегрується з платформою GoPhish та забезпечує автоматизацію процесів створення, проведення та оцінювання фішингових кампаній, що дає змогу збирати й аналізувати дані щодо поведінкових реакцій користувачів у контрольованому середовищі (рис.2).

Вибір інструментальних засобів для дослідження атак соціальної інженерії є надважливим, оскільки такі атаки поєднують технічні механізми доставки з психологічними методами впливу на користувачів. У межах даного дослідження для симуляції атак обрано платформу GoPhish, що зумовлено сукупністю її функціональних, методологічних та прикладних переваг.

GoPhish забезпечує високий рівень відтворюваності експериментів. Платформа дозволяє формалізувати фішингові кампанії у вигляді чітко визначених сценаріїв, які можуть бути багаторазово відтворені з контрольованою зміною окремих параметрів (текст повідомлення, дизайн сторінки, час надсилання, склад цільової групи). Це створює можливість порівняльного аналізу результатів і статистичної валідації гіпотез. Платформа поєднує технічні та поведінкові аспекти атак. З одного боку, вона реалізує технічний вектор атаки через електронну пошту та вебінтерфейси, а з іншого — дозволяє

моделювати психологічні тригери, такі як терміновість, авторитет або довіра, шляхом адаптації контенту повідомлень. Це робить її придатною для дослідження соціальної інженерії саме як соціотехнічного явища, а не лише як технічної загрози. Суттєвою перевагою GoPhish є детальний збір і фіксація метрик поведінки користувачів. Платформа автоматично реєструє події доставки повідомлення, відкриття листа, переходу за посиланням та введення облікових даних. Отримані дані можуть бути використані для кількісного аналізу ефективності атак, побудови моделей ризику та навчання систем виявлення атак соціальної інженерії. Відкритий вихідний код забезпечує прозорість реалізації та можливість модифікації, що є особливо важливим для проведення досліджень. Використання GoPhish не обмежується закритими алгоритмами або ліцензійними умовами, що уможливлює адаптацію платформи до специфічних експериментальних потреб і інтеграцію з власними аналітичними модулями. GoPhish відповідає етичним і правовим вимогам дослідження, оскільки платформа орієнтована на симуляцію атак у контрольованих середовищах і використовується переважно для навчання та підвищення обізнаності. Це дозволяє проводити експерименти з мінімізацією ризиків для користувачів і без порушення чинних норм інформаційної безпеки. Водночас обмеженість GoPhish переважно електронною поштою як каналом атаки розглядається не як недолік, а як обґрунтоване спрощення, що дає змогу зосередитися на детальному аналізі одного з найпоширеніших векторів соціальної інженерії.

Потреба у багаторівневих механізмах захисту зумовлена комплексною природою соціотехнічних атак, що спрямовані на використання як технічних уразливостей інформаційних систем, так і психологічних особливостей користувачів. Багаторівневий підхід передбачає захист на рівні периметра, мережі, додатків та людини. Система AntiPhishing поєднує зовнішній шар інтеграції з GoPhish для збору даних, внутрішній шар аналізу у відповідних модулях risk_scorer.py та pattern_detector.py, а також шар візуалізації в modern_dashboard.py для відображення метрик ризику. За відсутності багаторівневої архітектури безпеки система залишається вразливою, оскільки подолання окремого захисного рівня дозволяє реалізувати атаку, тоді як інтеграція кількох рівнів підвищує загальну стійкість системи.

Запуск симуляції передбачає послідовне проходження наступних етапів: підготовку шаблонів атак у моделях models.py, налаштування клієнта для взаємодії з API GoPhish та ініціацію кампанії. У процесі моніторингу система збирає метрики, зокрема відсоток відкриттів листів, переходів за посиланнями, введення даних та звітування про підозрілі повідомлення, аналіз яких здійснюється через модулі risk_scorer.py та pattern_detector.py.

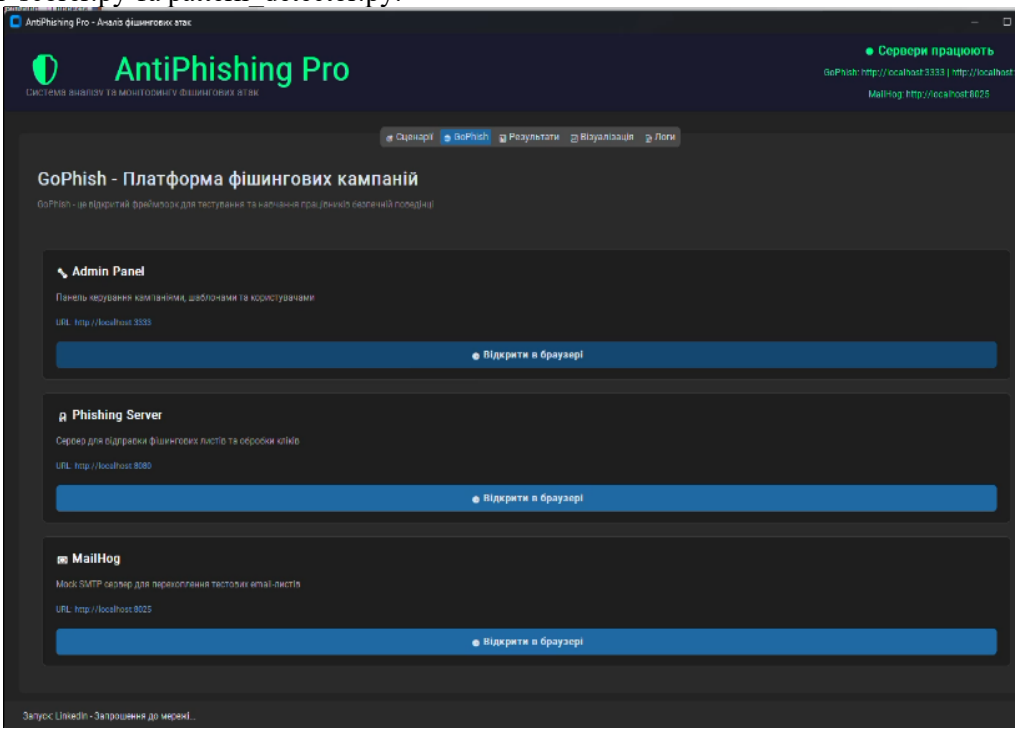

Рис. 2. Головне вікно AntiPhishing Pro – вкладка GoPhish

Розроблення сценаріїв фішингових атак потребує комплексного підходу, який інтегрує психологічні, технічні та організаційні компоненти з метою відтворення умов реальних загроз. Проектування сценаріїв у системі AntiPhishing (рис.3) забезпечує комплексний захист, поєднуючи

симуляцію з аналізом. Це дозволяє організаціям не лише тестувати вразливості, але й розробляти стратегії навчання. Сценарії фішингових атак базуються на моделях даних, визначених у модулі models.py, де описуються класи Campaign (фішингові кампанії з певними атрибутами), Event (події – реакція користувача) та User (класифікація користувачів за відділами, посадами, рівнями ризику тощо).

Створення шаблонів розсилок електронною поштою розпочинається з ідентифікації ключових компонентів, спрямованих на використання когнітивних упереджень користувачів, зокрема відчуття терміновості та схильності довіряти авторитетним джерелам. У GoPhish шаблони формуються з використанням HTML-оформлення та текстових версій, при цьому тема повідомлення і його зміст відтворюють характер легітимної електронної кореспонденції.

Створення підроблених веб-сторінок, що імітують справжні сайти для збору даних, відбувається з використанням HTML/CSS, з елементами, що копіюють дизайн популярних сервісів, наприклад, форми входу в корпоративну систему.

Таблиця 1 ілюструє різноманітність сценаріїв, адаптованих до контексту організації.

Практична реалізація системи демонструє, що ефективність сценаріїв залежить від балансу між реалістичністю та етичністю. Система враховує фактор «свіжості» подій, тобто події за останні 30 днів мають вищу вагу, дозволяючи виявляти актуальні вразливості. Відповідні функції генерують статистику, наприклад, середній ризик по організації та топ вразливих користувачів, що в свою чергу забезпечує ітеративне вдосконалення, коли після кожної кампанії шаблони оновлюються на основі даних з бази.

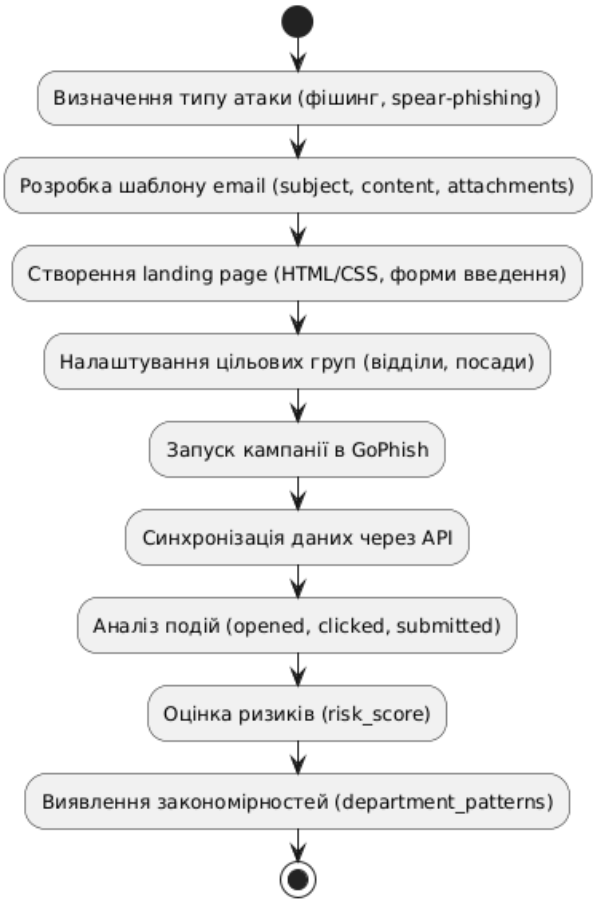

Рис. 3. Схема процесу проектування сценарію фішингової атаки в системі AntiPhishing

В процесі симуляції атаки (рис.4) збір даних здійснюється в автоматичному режимі: після запуску кампанії на платформі GoPhish система AntiPhishing виконує періодичні запити для отримання результатів. Моніторинг передбачає відстеження ключових показників у режимі реального часу, а подальший аналіз метрик у модулі pattern_detector.py дає змогу ідентифікувати характерні патерни, наприклад, підвищену вразливість окремих структурних підрозділів.

Таблиця 2

Приклади сценаріїв фішингових атак

Сценарій	Шаблон email	Підроблена сторінка	Цільова група	Очікувані події
Атака на крадіжку даних	Тема: "Термінове оновлення пароля". Вміст: Посилання на "службу безпеки"	Форма входу з полями логін/пароль, імітація корпоративного порталу	Бухгалтерія, менеджери	Opened Clicked Submitted
Spear-phishing на керівництво	Тема: "Конфіденційний документ". Вміст: Запит на підтвердження з вкладенням	Сторінка завантаження "документа" з формою верифікації	Керівники відділів	Sent Opened Reported
Фішинг через соціальні мережі	Тема: "Запрошення на конференцію". Вміст: Посилання на "реєстрацію"	Фальшива реєстраційна форма з особистими даними	IT-спеціалісти	Clicked Submitted
Тестова атака на всю організацію	Тема: "Щорічний аудит безпеки". Вміст: Запит на перевірку аккаунта	Сторінка з тестом на фішинг-обізнаність	Усі співробітники	Opened Reported

Рис. 4. Симуляція фішингової кампанії

В результаті аналізу метрик не лише фіксуються вразливості, але й на основі узагальнення результатів кількох кампаній формуються рекомендації щодо підвищення ефективності захисту, що забезпечує можливість довготривалого моніторингу рівня стійкості користувачів до атак.

Завершальним етапом симуляції є збереження отриманих результатів у базі даних і формування звіту за допомогою модуля main.py, у якому подається узагальнена статистична інформація, зокрема середній рівень ризику для організації. Такий підхід забезпечує повний цикл – від проведення симуляції до інтерпретації результатів – і створює підґрунтя для розроблення та вдосконалення стратегій протидії соціотехнічним атакам.

Оцінка рівня загроз дозволяє не лише кількісно визначити ступінь ризику, але й сформувати обґрунтовані рекомендації для мінімізації вразливостей. Система AntiPhishing, інтегрована з платформою GoPhish, забезпечує автоматизовану обробку даних про взаємодію користувачів з симульованими фішинговими кампаніями на основі розрахунку балів ризику, враховуючи ваги подій та фактори свіжості. Це дозволяє виявити не тільки індивідуальні, але й групові вразливості.

Виявлення вразливих груп користувачів здійснюється через агрегацію даних по відділах та посадах, що реалізовано у відповідному модулі PatternDetector, який аналізує середні показники ризику, відсоток вразливих користувачів та тенденції змін. Відтак, наприклад, можна виявити підрозділи з підвищеним рівнем загроз, користувачі з яких мають часті взаємодії з фішинговими елементами, адже відповідно до [14] вразливість груп користувачів часто пов'язана з професійними ролями. Можливо також ідентифікувати осіб, які потребують пріоритетної уваги.

Вивчення типових помилок користувачів є ключовим елементом оцінки, оскільки дозволяє виявити поведінкові патерни, що сприяють успішності атак. AntiPhishing вивчає події, такі як відкриття листа, перехід за покликанням, введення даних. Дослідження показало, що в ході симуляції фішингової атаки 72% вразливих користувачів здійснювали перехід за покликанням протягом перших 5 хвилин після отримання листа, що вказує на імпульсивність реакції та узгоджується з [15], де наголошено на ролі когнітивних упереджень при виконанні рутинних дій.

На основі оцінки рівня загроз система генерує рекомендації, адаптовані до типу цілі – користувача, відділу чи організації. Модуль Recommendation системи класифікує їх за категоріями (навчання, технічні заходи, процедурні) та пріоритетами (від низького до критичного).

Інтеграція отриманих рекомендацій у загальну політику безпеки компанії є завданням організаційного рівня. Він включає систематичне оновлення бази даних загроз та автоматизоване формування управлінських звітів.

Таким чином, оцінка рівня загроз та наявність рекомендації формують замкнений цикл: від симуляції до аналізу та корекції поведінки, забезпечуючи ефективний захист від фішингових атак.

5. Висновки і перспективи подальших досліджень.

Дослідження розробленої системи AntiPhishing, інтегрованої з платформою GoPhish, підкреслило, що ефективний захист від атак соціальної інженерії вимагає інтеграції автоматизованого моніторингу, оцінки ризиків та виконання рекомендацій з урахуванням людського фактору. Система забезпечує комплексний аналіз даних симуляцій, що сприяє зменшенню ризиків у організаціях.

Перспективи подальших досліджень включають інтеграцію сучасних методів штучного інтелекту для автоматичного створення та адаптації сценаріїв атак.

Внесок авторів

Наталія Коршун – концептуалізація дослідження, формування наукової ідеї та методологічних засад дослідження соціотехнічних атак; Андрій Бондарчук – методика дослідження, розроблення підходу до моделювання фішингових кампаній і побудови експериментального середовища; Павло Складанний – програмне забезпечення, архітектура системи AntiPhishing, інтеграція з платформою GoPhish, реалізація програмних модулів аналізу та моніторингу; Тетяна Крижанівська – збір і перевірка емпіричних даних, проведення симуляцій фішингових кампаній та формування експериментальної вибірки; Володимир Соколов – емпіричне дослідження, аналіз результатів симуляцій, інтерпретація отриманих метрик ризику та формування практичних рекомендацій.

Подяка, джерела фінансування

Дослідження здійснено в рамках реалізації науково-дослідної теми "Методи та моделі забезпечення кібербезпеки інформаційних систем переробки інформації та функціональної безпеки програмно-технічних комплексів управління критичної інфраструктури (реєстраційний номер 0122U200483 від 06.07.2022).

Декларація про штучний інтелект

Під час підготовки цієї роботи автори використовували програму штучного інтелекту Grammarly Pro для виправлення граматики тексту та систему Strike Plagiarism для пошуку можливих проявів плагіату. Після використання цих інструментів автори переглянули та відредагували зміст за потреби і несуть повну відповідальність за зміст публікації.

Конфлікт інтересів

Автори заявляють про відсутність конфлікту інтересів та підтверджують, що під час підготовки цієї роботи не існувало жодних комерційних, фінансових чи інших взаємовідносин, які могли б бути розцінені як такі, що здатні вплинути на результати дослідження або їх інтерпретацію. Робота виконана відповідно до принципів академічної доброчесності, етичних норм проведення наукових досліджень та вимог редакційної політики щодо запобігання конфлікту інтересів.

Список використаної літератури

1. Wang, Z., Sun, L., & Zhu, H. (2020). Defining social engineering in cybersecurity. *IEEE Access, 8*, 85094–85115. https://doi.org/10.1109/access.2020.2992807

2. Wang, Z., Zhu, H., Liu, P., & Sun, L. (2021). Social engineering in cybersecurity: A domain ontology and knowledge graph application examples. *Cybersecurity, 4*(1). https://doi.org/10.1186/s42400-021-00094-6

3. Siddiqi, M., Pak, W., & Siddiqi, M. (2022). A study on the psychology of social engineering-based cyberattacks and existing countermeasures. *Applied Sciences, 12*(12), 6042. https://doi.org/10.3390/app12126042

4. Salahdine, F., & Kaabouch, N. (2019). Social engineering attacks: A survey. *Future Internet, 11*(4), 89. https://doi.org/10.3390/fi11040089

5. Akyesilmen, N., & Alhosban, A. (2024). Non-technical cyber-attacks and international cybersecurity: The case of social engineering. *Gaziantep University Journal of Social Sciences, 23*(1), 342–360. https://doi.org/10.21547/jss.1346291

6. Aldawood, H., & Skinner, G. (2020). An advanced taxonomy for social engineering attacks. *International Journal of Computer Applications, 177*(30), 1–11. https://doi.org/10.5120/ijca2020919744

7. Chen, F., Wu, T., Nguyen, V., & Rudolph, C. (2025). SoK: Large language model-generated textual phishing campaigns—End-to-end analysis of generation, characteristics, and detection. *arXiv*. https://doi.org/10.48550/arXiv.2508.21457

8. Khadka, K., Ullah, A. B., Ma, W., & Martinez Marroquin, E. (2024). A survey on the principles of persuasion as a social engineering strategy in phishing. *arXiv*. https://doi.org/10.48550/arXiv.2412.18488

9. Schmitt, M., & Flechais, I. (2024). Digital deception: Generative artificial intelligence in social engineering and phishing. *Artificial Intelligence Review*. https://doi.org/10.1007/s10462-024-10973-2

10. Santosa Pohan, D., Irfan, D., Fitriyani, I. N., Hasibuan, Y. I. M., & Chayani, I. (2025). Simulation and detection of phishing attacks on student academic emails using social engineering techniques. *International Journal of Health Engineering and Technology, 2*(4). https://doi.org/10.55227/ijhet.v2i4.283

11. Marchenko, V. V., Chaikivskyi, V. V., & Pryima, O. O. (2024). Method for increasing personnel awareness of information security using the GoPhish software application. *Systemy i tekhnolohii zviazku, informatyzatsii ta kiberbezpeky, 1*(6), 116–126. https://doi.org/10.58254/viti.6.2024.09.116

12. Bokhonko, O., & Lysenko, S. (2025). Models of social engineering attacks. *Measuring and Computing Devices in Technological Processes, 1*, 432–444. https://doi.org/10.31891/2219-9365-2025-81-55

13. Haidur, H. I., Hakhov, S. O., Marchenko, V. V., & Haidur, K. V. (2024). Conceptual model for detecting phishing attacks based on support vector machine methods. *Suchasnyi zakhyst informatsii, 2*, 24–33. https://doi.org/10.31673/2409-7292.2024.020003

14. The human factor in cybersecurity: Understanding psychology, training efficacy, and error reduction strategies. (2025). *ResearchGate*. https://www.researchgate.net/publication/387971383

15. Kim, S. (n.d.). Cognitive biases in social engineering attacks: Implications for user training. *Journal of Cybersecurity Research, 9*(2), 150–165.

16. Sokolov, V. Yu., & Kurbanmuradov, D. M. (2018). Methodology for counteracting social engineering at information activity objects. *Cybersecurity: Education, Science, Technique, 1*(1), 6–16.

Надійшла до редакції: 03.12.25
Прийнята до друку: 17.03.26
Опубліковано: 30.03.26