№ 3(57) 2026
НАУКА і ТЕХНІКА СЬОГОДНІ
ISSN 2786-6025 Online
УДК 004.056.53:343.98:004.8

https://doi.org/10.52058/2786-6025-2026-3(57)-70-85

Габорець Ольга Андріївна доктор філософії, доцент, доцент кафедри оперативно-розшукової діяльності та інформаційної безпеки Навчально-наукового інституту підготовки фахівців для підрозділів кримінальної поліції імені Е.О. Дідоренка Донецького державного університету внутрішніх справ, м. Кропивницький, https://orcid.org/0000-0001-7791-6795

Лунгол Ольга Миколаївна кандидат педагогічних наук, доцент, завідувач кафедри оперативно-розшукової діяльності та інформаційної безпеки Навчально-наукового інституту підготовки фахівців для підрозділів кримінальної поліції імені Е.О. Дідоренка Донецького державного університету внутрішніх справ, м. Кропивницький, https://orcid.org/0000-0001-8128-0072

Тулінов Валентин Сергійович кандидат юридичних наук, доцент, заступник директора Навчально-наукового інституту підготовки фахівців для підрозділів кримінальної поліції імені Е.О. Дідоренка Донецького державного університету внутрішніх справ, м. Кропивницький, https://orcid.org/0000-0002-3972-348X

Волобоєва Злата Олегівна здобувач вищої освіти навчально-наукового інституту права та соціального менеджменту Донецького державного університету внутрішніх справ, м. Кропивницький, https://orcid.org/0009-0009-9760-5279

ІННОВАЦІЙНІ МЕТОДИКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ: ПРОТИДІЯ ФІШИНГУ В СТРУКТУРІ СУЧАСНОЇ КІБЕРЗЛОЧИННОСТІ

Анотація. У статті досліджено фішинг як базовий елемент структури сучасної організованої кіберзлочинності, що стрімко еволюціонує завдяки інтеграції соціоінженерних практик та новітніх технологій. Визначено, що сучасні фішингові атаки трансформувалися у високоприбуткову індустрію, зокрема через поширення моделі «фішинг як послуга» (Phishing-as-a-Service, PhaaS), що робить загрозу масовою та структурованою. Проаналізовано системний характер фішингу як домінантного початкового вектора кібератак. На основі емпіричного аналізу маніпулятивних повідомлень, поширюваних через цифрові канали комунікації, виокремлено ключові соціоінженерні прийоми (імітація авторитетного джерела, створення ефекту невідкладності). Доведено, що традиційні засоби захисту не здатні повною мірою протистояти

ISSN 2786-6025 Online

таким викликам, що зумовлює потребу правоохоронних органів та фахівців з інформаційної безпеки у симетричній технологічній відповіді. Обґрунтовано необхідність комплексного підходу до нейтралізації фішингових загроз із пріоритетним застосуванням інноваційних методик. Акцентовано увагу на ефективності впровадження алгоритмів штучного інтелекту та машинного навчання для предиктивного семантичного аналізу, використання платформ автоматизованого реагування (SOAR), методів поведінкової аналітики та передових OSINT-інструментів. Практичне значення результатів полягає у можливості їх використання для вдосконалення поліцейських практик, тактики розкриття кіберзлочинів та посилення загального контуру інформаційної безпеки цифрового суспільства.

Ключові слова: фішинг; організована кіберзлочинність; інноваційні методики; інформаційна безпека; штучний інтелект; машинне навчання; соціальна інженерія; Phishing-as-a-Service (PhaaS); кіберзахист.

Haborets Olha PhD, Docent, Associate Professor of the Department of Operational-Search Activity and Information Security of the Educational and Scientific Institute for the Training Specialists for Criminal Police Units named after E.O. Didorenko of Donetsk State University of Internal Affairs, Kropyvnytskyi, https://orcid.org/0000-0001-7791-6795

Lunhol Olha PhD, Docent, Head of the Department of Operational-Search Activity and Information Security of the Educational and Scientific Institute for the Training Specialists for Criminal Police Units named after E.O. Didorenko of Donetsk State University of Internal Affairs, Kropyvnytskyi, https://orcid.org/0000-0001-8128-0072

Tulinov Valentyn PhD, Docent, Deputy Director of the Educational and Scientific Institute for Training Specialists for Criminal Police Units named after E.O. Didorenko of Donetsk State University of Internal Affairs, Kropyvnytskyi, https://orcid.org/0000-0002-3972-348X

Voloboieva Zlata student of the Educational and Scientific Institute of Law and Social Management, Donetsk State University of Internal Affairs, Kropyvnytskyi, https://orcid.org/0009-0009-9760-5279

INNOVATIVE INFORMATION SECURITY METHODS: COUNTERING PHISHING IN THE STRUCTURE OF MODERN CYBERCRIME

Abstract. The article explores phishing as a fundamental element of the structure of modern organized cybercrime, which is rapidly evolving due to the

ISSN 2786-6025 Online
integration of social engineering practices and the latest technologies. It is determined that modern phishing attacks have transformed into a highly profitable industry, in particular through the proliferation of the Phishing-as-a-Service (PhaaS) model, which makes the threat massive and structured. The systemic nature of phishing as a dominant initial vector of cyberattacks is analyzed. Based on an empirical analysis of manipulative messages disseminated through digital communication channels, key social engineering techniques (imitation of an authoritative source, creation of a sense of urgency) have been identified. It is proven that traditional protection tools are not fully capable of withstanding such challenges, which necessitates a symmetrical technological response from law enforcement agencies and information security specialists. The necessity of a comprehensive approach to neutralizing phishing threats with a priority application of innovative methods is substantiated. Emphasis is placed on the effectiveness of implementing artificial intelligence and machine learning algorithms for predictive semantic analysis, the use of automated response platforms (SOAR), behavioral analytics methods, and advanced OSINT tools. The practical significance of the results lies in the possibility of their application to improve police practices, cybercrime investigation tactics, and strengthen the overall information security contour of the digital society.

Keywords: phishing; organized cybercrime; innovative methods; information security; artificial intelligence; machine learning; social engineering; Phishing-as-a-Service (PhaaS); cyber defense.

Постановка проблеми. Стрімка цифровізація суспільних процесів зумовила якісну трансформацію кіберзагроз, серед яких фішинг посідає одне з провідних місць як домінантний початковий вектор більшості кібератак. На відміну від традиційних, хаотичних форм кіберзлочинності, фішинг у сучасному цифровому середовищі перетворився на високоприбуткову, чітко структуровану індустрію. Поширення тіньової бізнес-моделі «фішинг як послуга» (Phishing-as-a-Service, PhaaS) призвело до масовості та професіоналізації атак. Сьогодні організовані кіберзлочинні угруповання використовують фішинг не лише для викрадення фінансових активів, а й як базовий інструмент для отримання несанкціонованого доступу до корпоративних мереж, державних інформаційних ресурсів та об’єктів критичної інфраструктури.

Особливу загрозу становить поєднання фішингових технологій із можливостями соціальних мереж, месенджерів та передових інструментів OSINT. Це дає змогу зловмисникам автоматизувати збір даних, здійснювати високорівневу персоналізацію впливу та генерувати маніпулятивний контент за допомогою алгоритмів штучного інтелекту. За таких умов людський фактор залишається найбільш уразливою ланкою: атаки майстерно маскуються під легітимні сервіси та експлуатують когнітивні тригери користувачів. При цьому

ISSN 2786-6025 Online

традиційні (сигнатурні) засоби кіберзахисту та базові фільтри виявляються вкрай неефективними перед динамічними загрозами, які здатні миттєво адаптуватися до нових умов.

Водночас національна система протидії кіберзлочинності стикається з низкою проблем, пов'язаних із недостатньою інтеграцією предиктивного аналізу загроз та обмеженим використанням передових технологічних рішень у практичній діяльності правоохоронних органів та фахівців з інформаційної безпеки. Це зумовлює гостру потребу в ґрунтовному науковому осмисленні фішингу як складної багаторівневої системи та обґрунтуванні дієвих шляхів його нейтралізації шляхом упровадження інноваційних методик захисту.

За таких умов фішинг доцільно розглядати не просто як окремий різновид шахрайства, а як системний виклик, що вимагає симетричної технологічної та організаційної відповіді. Протидія сучасній організованій кіберзлочинності неможлива без переходу від реактивної моделі кіберзахисту до проактивної. Саме тому науковий пошук має бути зосереджений на інтеграції алгоритмів штучного інтелекту та машинного навчання (ML) для виявлення аномалій, упровадженні платформ автоматизованого реагування (SOAR) і методів поведінкової аналітики в нерозривному поєднанні з підвищенням загальної цифрової грамотності суспільства.

Аналіз останніх досліджень і публікацій. Проблематика протидії фішингу та організованій кіберзлочинності перебуває у фокусі постійної уваги багатьох вітчизняних науковців. Загальнотеоретичні та правові аспекти забезпечення інформаційної безпеки держави в умовах сучасних викликів розглядалися у ґрунтовних працях О. Тарасенко [1], О. Зіменка [2], І. Гончаренка [3], О. Пугачова [4] та ін. Водночас технологічний вимір протидії кіберзлочинам активно досліджується в площині технічних наук. Зокрема, трансформація фішингу у високоприбуткову тіньову бізнес-модель детально аналізується у дослідженнях М. Запорожченка [5], який одним із перших звернув увагу на вітчизняному рівні на феномен платформ «Phishing-as-a-Service» (PhaaS). Сучасні підходи до виявлення загроз за допомогою інноваційних технологій, таких як великі мовні моделі (LLM) та алгоритми машинного навчання для аналізу комунікацій у реальному часі, висвітлено в актуальних роботах Д. Ковальчука [6]. Важливим фактором залишається навчання фахівців з протидії загрозам цифрового простору [7 – 9].

Незважаючи на значний масив наукових розвідок, стрімка еволюція організованої кіберзлочинності вимагає постійного оновлення методологічної бази. Більшість наявних праць зосереджується або суто на технічних алгоритмах (апаратно-програмний захист та класифікація веб-ресурсів), або на загальноправових механізмах. Натомість комплексний підхід, який органічно поєднує інноваційні технологічні методики, такі, як ШІ, машинне навчання,

ISSN 2786-6025 Online

автоматизований предиктивний аналіз, із практичними поліцейськими алгоритмами розкриття злочинів та нейтралізації фішингу в структурі сучасної кіберзлочинності, залишається недостатньо розкритим.

З огляду на вищезазначене, нагальною є потреба в розробці комплексних науково-практичних рекомендацій щодо застосування інноваційних методик правоохоронної протидії сучасним формам фішингу, що діють за моделлю «сервісу» та активно використовують технології штучного інтелекту.

Метою статті є комплексне наукове дослідження фішингу як базового елемента структури сучасної організованої кіберзлочинності, з'ясування його ролі та механізмів функціонування (зокрема поширення тіньової моделі Phishing-as-a-Service), а також обґрунтування ефективних шляхів нейтралізації фішингових атак на основі впровадження інноваційних методик інформаційної безпеки.

Досягнення поставленої мети передбачає не лише аналіз соціоінженерних механізмів маніпулятивного впливу, а й виявлення закономірностей технологічної еволюції фішингових кампаній. Окрім того, метою є оцінювання ролі людського фактора як ключової вразливої ланки цифрового середовища та визначення передових технологічних інструментів (алгоритмів штучного інтелекту, машинного навчання, систем автоматизованого реагування) для надійної компенсації цих ризиків у правоохоронній діяльності та сфері загального кіберзахисту.

Виклад основного матеріалу. У структурі сучасної організованої кіберзлочинності фішинг постає як одна з найбільш небезпечних та технологічно розвинених соціотехнічних загроз. Його еволюція свідчить про стрімкий перехід від хаотичних атак до системного тіньового бізнесу, що масово використовує модель «фішинг як послуга» (Phishing-as-a-Service, PhaaS). Особливість сучасного фішингу полягає в тому, що первинним об'єктом атаки є не програмно-апаратна інфраструктура, а безпосередньо людина як носій інформації та найуразливіша ланка будь-якої системи інформаційної безпеки.

В умовах тотальної цифровізації ефективність фішингових кампаній істотно зростає завдяки інтеграції зловмисниками інноваційних технологій, зокрема інструментів штучного інтелекту для автоматичної генерації таргетованого маніпулятивного контенту.

Використовуючи інформаційне перевантаження суспільства, дефіцит часу на перевірку джерел та емоційні тригери користувачів, кіберзлочинні угруповання створюють високоадаптивне середовище для маніпулятивного впливу. Це формує нагальну потребу у відході від застарілих реактивних засобів захисту та впровадженні інноваційних методик протидії, здатних компенсувати вразливість людського фактора предиктивними технологічними рішеннями.

ISSN 2786-6025 Online

За даними Системи виявлення вразливостей і реагування на кіберінциденти та кібератаки, що функціонує під егідою Державного центру кіберзахисту Державної служби спеціального зв'язку та захисту інформації України, протягом першого півріччя 2025 року було опрацьовано 535 кіберінцидентів та кібератак. Аналіз структури цих інцидентів свідчить, що фішинг і пов'язані з ним техніки соціальної інженерії залишаються домінуючим початковим вектором атак, зокрема через використання електронної пошти як основного каналу первинного доступу до інформаційних систем. Це підтверджує тезу про системний характер фішингу як інструменту проникнення та подальшої ескалації кіберзагроз.

У контексті гібридної війни фішинг набуває рис інструмента інформаційно-психологічних операцій, що реалізується через експлуатацію когнітивних тригерів. До таких тригерів належать страх за безпеку, очікування соціальної або гуманітарної допомоги, відчуття терміновості та апеляція до авторитету нібито офіційних джерел. Саме тому у фішингових повідомленнях періоду війни домінують наративи, пов'язані з соціальними виплатами, гуманітарними програмами, евакуацією населення, а також повідомленнями про надзвичайні події. Такі повідомлення спрямовані на швидке емоційне реагування користувачів і зниження рівня критичного аналізу отриманої інформації.

Емпіричні дані Оперативного центру реагування на кіберінциденти [11] засвідчують, що зловмисники дедалі частіше застосовують комбіновані вектори атак, поєднуючи фішинг, інфікування шкідливим програмним забезпеченням та використання фізичних носіїв або неліцензійного програмного забезпечення. Така багаторівнева модель ускладнює виявлення атак на ранніх етапах і свідчить про зростання професіоналізації кіберзлочинних угруповань, що діють у межах гібридних загроз.

Окрему увагу в аналізі фішингових атак слід приділити діяльності організованих кластерів кіберзагроз, які системно використовують фішинг як початковий етап кібератак. Згідно з класифікацією CERT-UA, у першій половині 2025 року найбільш активними були кластери UAC-0010, UAC-0050 та UAC-0202. Для цих угруповань характерним є застосування технік фішингу відповідно до класифікації MITRE ATT&CK, зокрема Spearphishing Attachment, що підтверджує використання цілеспрямованих фішингових повідомлень для компрометації облікових записів та подальшого отримання несанкціонованого доступу до систем.

Функціонування Системи виявлення вразливостей і реагування на кіберінциденти демонструє, що протидія фішингу в умовах гібридної війни не може обмежуватися виключно технічними заходами. Незважаючи на масштабний моніторинг кіберпростору, який охоплює десятки тисяч робочих станцій,

ISSN 2786-6025 Online

серверів і мережевих сенсорів, людський фактор залишається ключовою вразливістю. Саме через помилки користувачів, недостатній рівень цифрової грамотності та невміння розпізнавати маніпулятивні повідомлення зловмисники отримують початкову точку входу до інформаційних систем.



Рис. 1. Візуалізація глобальної кіберзагрозової активності в режимі реального часу за даними інтерактивної платформи Threat Map компанії Check Point Software Technologies (https://threatmap.checkpoint.com/)

У цьому контексті фішинг слід розглядати як індикатор стану інформаційної стійкості суспільства. Його масове поширення свідчить не лише про активність зловмисників, а й про структурні проблеми у сфері інформаційної культури, нормативно-правового регулювання та міжсекторальної взаємодії у сфері кібербезпеки. Дані офіційного державного моніторингу підтверджують, що без системної інтеграції технічних, правових і освітніх заходів фішинг залишатиметься ефективним інструментом гібридного впливу.

У межах дослідження фішингу в умовах гібридної війни важливим є не лише опис окремих інцидентів чи узагальнена характеристика загроз, а й систематичне спостереження за кіберландшафтом у масштабі, що виходить за межі однієї національної мережі або окремої організації. Для цього доцільно залучати інтерактивні аналітичні платформи, що надають дані про кіберінциденти у глобальному вимірі. Одним із таких ресурсів є Threat Map від Check Point Software Technologies (далі – Threat Map) (рис. 1.), який представляє

ISSN 2786-6025 Online

собою візуальний інформаційний щит глобальних кіберзагроз із миттєвим оновленням даних. Threat Map надає комплексну візуалізацію напрямків та інтенсивності атак у режимі реального часу, що дозволяє визначати основні тренди, розподіл атак за регіонами, а також типи загроз, що активізуються в певні часові періоди.

З наукової точки зору важливість використання Threat Map полягає у кількох ключових аспектах. По-перше, це емпіричне підтвердження системності загроз у кіберпросторі, зокрема фішингових кампаній як складової частини загальної картини атак. Threat Map дозволяє досліднику спостерігати, як змінюється інтенсивність кіберінцидентів у часі та просторі, які країни чи регіони стають епіцентрами активності, і яким чином ці індикатори корелюють із геополітичними або соціально-військовими подіями. Така кореляція є важливою, оскільки вона підтверджує, що зростання фішингових атак може бути не випадковим, а пов'язаним із певними етапами гібридної війни, ескалацією воєнних дій або інформаційних кампаній.

По-друге, Threat Map дозволяє виокремлювати структурні компоненти загроз, що мають важливе значення для наукового аналізу. Наприклад, інтерактивна карта розподілу атак дає змогу бачити не лише загальну кількість інцидентів, а й їхню спрямованість на певний сектор (урядові системи, корпоративні мережі, приватний сектор), що дозволяє визначити домінантні вектори атак. У контексті фішингу це дає інформацію про те, чи переважають загальні фішингові повідомлення, спрямовані на масову аудиторію, чи спостерігається тенденція до мішених фішингових атак (spear-phishing), що орієнтовані на конкретні групи або осіб. Такий рівень деталізації є критично важливим для формування адекватних стратегій захисту, оскільки різні типи фішингових атак потребують різних підходів реагування.

Третій аспект – можливість аналізу тенденцій у часовому вимірі, який дозволяє співставляти пік активності фішингу із визначеними подіями гібридної війни. Наприклад, у моменти загострення інформаційної напруги або після поширення гучних повідомлень у медіапросторі про військові дії або соціальні програми, спостерігається збільшення фішингової активності. Threat Map фіксує ці хвилі в реальному часі, що дозволяє робити висновки про динаміку загроз у відповідь на інформаційні стимули. Такий аналіз має важливе методологічне й практичне значення, оскільки він виходить за межі суто якісного опису фішингових кейсів і дозволяє досліджувати закономірності функціонування фішингу як системної інформаційної загрози.

На основі даних Threat Map можна також оцінювати географічну диференціацію фішингової активності. Це особливо важливо в умовах гібридної війни, коли певні регіони можуть бути більш інтенсивно атаковані в різні періоди конфлікту. Такий просторовий аналіз є цінним для формування

ISSN 2786-6025 Online

політик захисту, оскільки дозволяє державним органам і приватним структурам коригувати свої оборонні стратегії залежно від актуальних загроз у конкретних географічних сегментах.

Емпіричне використання Threat Map у дослідженні фішингу також дозволяє розширити спектр наукових методів. Окрім якісного аналізу повідомлень або окремих кейсів, дослідник має можливість застосовувати кількісні методи, зокрема часові ряди, кореляційний аналіз та просторові статистичні моделі. Це сприяє підвищенню наукової обґрунтованості висновків та дозволяє формувати моделі прогнозування кіберзагроз з урахуванням гібридних факторів впливу.

Важливою функціональною перевагою Threat Map є його інтерактивність та візуальна доступність, що дозволяє не лише дослідникам, а й фахівцям практичного рівня оперативно виявляти зміни в поведінці кіберзагроз.

Наприклад, значні хвилі фішингових атак, що відображаються на карті, можуть служити сигналом для підвищення рівня пильності в організаціях або державних установах, а також слугувати підставою для негайного оновлення заходів захисту або інформаційних кампаній серед населення.

З огляду на зазначене, інтеграція даних Threat Map у наукове дослідження фішингу сприяє не лише моніторингу поточної кіберситуації, а й формуванню довгострокових стратегій нейтралізації загроз, що базуються на дедалі ширшому спектрі кількісних та якісних індикаторів. Такий підхід важливий для підвищення інформаційної стійкості суспільства в умовах гібридної війни, оскільки дозволяє поєднувати реальні дані з аналітичними конструкціями, що розкривають закономірності функціонування фішингу як складної системної загрози.

Важливим елементом аналізу фішингу в умовах гібридної війни є розгляд конкретних прикладів маніпулятивних повідомлень, що поширюються через месенджери та соціальні мережі. Саме такі приклади дозволяють простежити, яким чином соціальна інженерія адаптується до воєнного контексту та трансформується з інструменту індивідуального шахрайства в механізм масового інформаційно-психологічного впливу.

Одним із найбільш поширених різновидів є так званий фішинг гуманітарного або соціального типу, спрямований на соціально вразливі групи населення. Такі повідомлення, як правило, апелюють до базових потреб людини – безпеки, матеріального забезпечення та соціальної підтримки. У воєнний період ці потреби загострюються, що значно підвищує ефективність маніпулятивних комунікацій. Повідомлення даного типу зазвичай стилізуються під офіційні оголошення від імені відомих брендів, благодійних організацій або державних структур, використовують формалізовану лексику та імітацію адміністративних процедур.

ISSN 2786-6025 Online

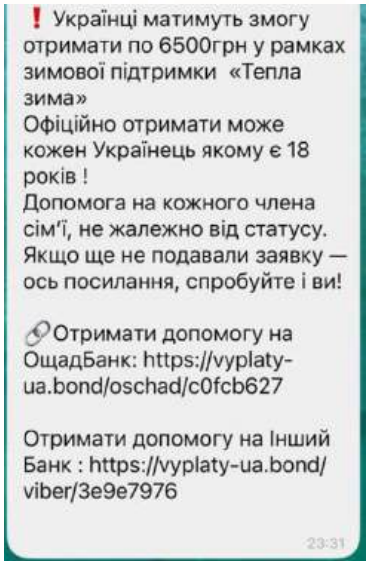

Рис. 2. Приклад фішингового повідомлення соціально-гуманітарного типу, спрямованого на експлуатацію теми фінансової допомоги населенню

Як ілюструє рис. 2, одним із найбільш поширених сценаріїв фішингових атак в умовах гібридної війни є використання соціально значущих наративів, пов'язаних із державною або гуманітарною підтримкою населення.

Повідомлення стилізоване під офіційне інформування та містить низку характерних ознак соціальної інженерії: апеляцію до соціальних гарантій, акцент на доступності фінансової допомоги для широких категорій громадян, а також заклик до негайної дії через перехід за гіперпосиланням.

Додатковим індикатором маніпулятивного характеру є час надходження повідомлення, оскільки воно було отримане у пізній період доби. Використання вечірнього або нічного часу є типовою тактикою фішингових кампаній, що ґрунтується на зниженні рівня когнітивної уваги користувача, підвищеній емоційній втомі та схильності до швидкого прийняття рішень без належної перевірки інформації.

У структурі повідомлення простежується застосування когнітивних тригерів довіри та терміновості. Зловмисники навмисно використовують формулювання, що імітують офіційну комунікацію, створюючи у користувача ілюзію легітимності джерела. Водночас застосування зовнішнього URL-посилання, яке не співвідноситься з офіційними державними доменами, є ключовим індикатором потенційної фішингової загрози.

Рис. 3 демонструє інший тип фішингових повідомлень, у яких класичні шахрайські механізми поєднуються з елементами дезінформації та психологічного тиску. Повідомлення побудоване за принципом шокового інформаційного впливу: використання емоційно насичених формулювань, маркерів терміновості та посилань на нібито оперативні джерела інформації.

ISSN 2786-6025 Online

Ключовою ознакою даного прикладу є перенаправлення користувача до зовнішнього каналу в месенджері, який позиціонується як джерело «актуальної інформації». У межах сучасних гібридних інформаційних операцій така схема може виконувати кілька функцій: залучення аудиторії до альтернативних інформаційних середовищ, формування інформаційної залежності та створення передумов для подальших фішингових або маніпулятивних впливів.

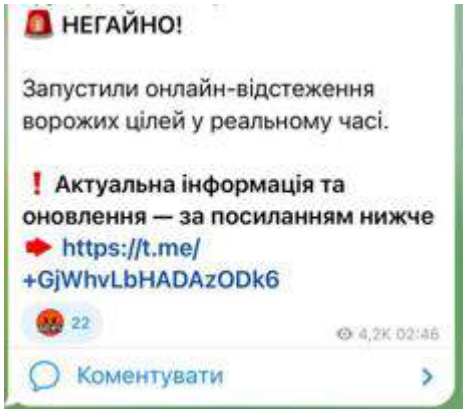

Рис. 3. Приклад маніпулятивного повідомлення з елементами фішингу та інформаційно-психологічного впливу, що поширюється через месенджери

З позиції інформаційної безпеки подібні повідомлення є прикладом гібридизації фішингу, коли первинною метою виступає не безпосереднє викрадення даних, а поступове зниження критичного сприйняття інформації та підрив довіри до офіційних каналів комунікації. Це дозволяє розглядати фішинг як складову ширших інформаційно-психологічних операцій у цифровому середовищі.

На рис. 4 представлено приклад фішингового повідомлення, що експлуатує тематику швидкого отримання кредитних коштів. Такі повідомлення є типовими для фінансово орієнтованого фішингу та спрямовані на користувачів, які можуть перебувати у стані фінансової невизначеності або психологічної вразливості.

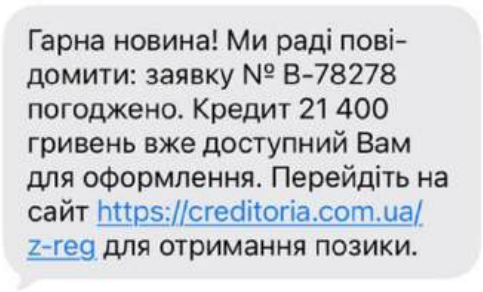

Рис. 4. Фішингове SMS-повідомлення як приклад експлуатації когнітивних тригерів користувача

ISSN 2786-6025 Online

Структура повідомлення містить характерні ознаки маніпулятивного впливу: повідомлення про нібито вже схвалену заявку, акцент на позитивному результаті («гарна новина»), а також заклик негайно перейти за посиланням для завершення процедури. Подібна комунікативна модель формує у користувача відчуття обмеженого часу для прийняття рішення, що знижує рівень критичного аналізу отриманої інформації.

Проведений аналіз наведених прикладів фішингових повідомлень дозволяє зробити висновок, що сучасний фішинг у контексті гібридної війни характеризується високим рівнем адаптивності до соціального та інформаційного середовища. Залежно від цільової аудиторії та ситуаційного контексту зловмисники комбінують різні комунікативні стратегії — від апеляції до соціальної підтримки й гуманітарної допомоги до використання шокового інформаційного контенту та фінансових стимулів.

Спільною рисою розглянутих прикладів є експлуатація когнітивних механізмів прийняття рішень користувача, зокрема ефекту терміновості, авторитетності джерела, страху втрати або бажання отримати вигоду. У таких умовах фішинг виступає не лише технічним інструментом компрометації даних, а й механізмом цілеспрямованого інформаційно-психологічного впливу, здатного змінювати поведінкові моделі користувачів у цифровому середовищі.

Важливо підкреслити, що розглянуті кейси демонструють трансформацію фішингу з індивідуальної шахрайської практики у системний елемент гібридних інформаційних операцій. Вплив таких повідомлень виходить за межі окремого користувача, оскільки їх масове поширення сприяє формуванню атмосфери інформаційної невизначеності, підвищенню рівня тривожності та зниженню довіри до легітимних каналів комунікації.

Таким чином, емпіричний аналіз підтверджує, що ефективність фішингових атак значною мірою визначається не технічними характеристиками повідомлення, а здатністю інтегруватися у соціальний контекст та використовувати психологічні особливості сприйняття інформації. Це зумовлює необхідність переходу від суто технічного розуміння фішингу до комплексного підходу, який поєднує кібербезпековий, інформаційно-аналітичний та когнітив-ний виміри дослідження.

Висновки. У результаті проведеного комплексного дослідження доведено, що фішинг у структурі сучасної організованої кіберзлочинності остаточно втратив ознаки локального шахрайства і трансформувався у високотехнологічну, чітко структуровану тіньову індустрію. Масштабування бізнес-моделі «фішинг як послуга» перетворило його на домінантний початковий вектор кібератак, що активно використовується злочинними угрупованнями для отримання несанкціонованого доступу до корпоративних, державних мереж та об’єктів критичної інфраструктури.

ISSN 2786-6025 Online

Емпіричний аналіз реальних маніпулятивних повідомлень та даних глобального моніторингу кіберзагроз (зокрема платформи Threat Map) засвідчив, що головною мішенню сучасних атак залишається людина як найуразливіша ланка системи інформаційної безпеки. Зловмисники майстерно експлуатують когнітивні тригери (страх, відчуття терміновості, очікування фінансової допомоги) та адаптують соціоінженерні сценарії до актуального соціально-політичного контексту. За таких умов традиційні, реактивні та сигнатурні засоби кіберзахисту виявляються критично неефективними.

Обґрунтовано, що єдиним дієвим шляхом нейтралізації цих загроз є перехід правоохоронних органів та суб'єктів забезпечення кібербезпеки до проактивної моделі захисту з пріоритетним застосуванням інноваційних методик. Ключовим елементом такої протидії є впровадження алгоритмів штучного інтелекту та машинного навчання для предиктивного семантичного аналізу комунікацій, використання систем автоматизованого реагування на кіберінциденти, методів поведінкової біометрії та передових інструментів OSINT.

Комплексне поєднання зазначених інноваційних технологічних рішень із заходами щодо підвищення рівня цифрової грамотності населення дозволить суттєво посилити спроможності правоохоронців у розкритті кіберзлочинів та сформувати надійний контур інформаційної стійкості суспільства.

Перспективи подальших досліджень у цьому напрямі доцільно зосередити на розробленні конкретних організаційно-тактичних рекомендацій для оперативних та слідчих підрозділів Національної поліції щодо використання інструментів штучного інтелекту під час документування та розслідування злочинів, вчинених із використанням PhaaS-платформ.

Література:

1. Тарасенко О. Удосконалення інструментарію забезпечення інформаційної безпеки держави. *СБУ в умовах війни в Україні: сучасні реалії та інноваційні стратегії забезпечення національної безпеки* : матеріали міжнар. наук.-практ. конф. (4–5 липня 2024 року). Київ : Алерта, 2024. С. 142–144.

2. Зіменко О. Є. Феномен інформаційного впливу у науковому середовищі: теорії, дефініції. *Бібліотекознавство. Документознавство. Інформологія*. 2022. № 1. С. 90–97.

3. Гончаренко І. Г. Кіберзагрози фінансового сектора в умовах війни. *Економіка та суспільство*. 2023. Вип. 50. URL: http://surl.li/tjtmk (дата звернення: 12.03.2026).

4. Пугачов О. І. Удосконалення державних механізмів забезпечення інформаційної безпеки України : дис. ... д-ра філософії : 281. Київ: Таврійський нац. ун-т ім. В. І. Вернадського, 2025. 248 с. URL: https://etnuir.tnu.edu.ua/bitstream/handle/123456789/462/dis_Puhachov.pdf (дата звернення: 05.03.2026).

5. Запорожченко М. Фішинг як послуга. *Cyber resilience strategies: risk management and business continuity*: proceedings of the national scientific and practical conference (Kyiv, February 23, 2023). Kyiv : Державний університет інформаційно-комунікаційних технологій, 2023. С. 47–49.

ISSN 2786-6025 Online

6. Ковальчук Д. Utilising large language models for automated real-time cyber threat analysis (Використання великих мовних моделей для автоматизованого аналізу кіберзагроз у реальному часі). *Вісник Черкаського державного технологічного університету*. 2025. Т. 30, № 1. С. 49–55.

7. Лунгол О. М. Удосконалення професійної підготовки майбутніх фахівців правоохоронної діяльності засобами інформаційних технологій. *Наука і техніка сьогодні*. 2022. № 7(7). С. 153–163.

8. Tsurkan O., Haborets O., Lunhol O. Innovative development of technologies in training future law enforcement specialists. *Science and technology today*. 2023. Issue № 12(12). P. 96–106.

9. Габорець О., Чернобров В. Social engineering as a means of influence on people consciousness. *Детермінанти посилення ролі освіти у повоєнному відновленні України: Березневий науковий дискурс 2023* : матеріали Міжнар. наук.-практ. конф. для освітян (м. Чернігів, 22 березня 2023 р.). Чернігів : ГО «Науково-освітній інноваційний центр суспільних трансформацій», 2023. С. 204–205.

10. Використання штучного інтелекту в кібербезпеці / О. М. Коваленко [та ін.]. *Інформатика та математичні методи в моделюванні*. 2025. Т. 15, № 1. С. 115–125.

11. Оперативний центр реагування на кіберінциденти оприлюднив річний звіт про роботу Системи виявлення вразливостей і реагування на кіберінциденти та кібератаки (СВВ) за 2025 рік. *Державний центр кіберзахисту Державної служби спеціального зв'язку та захисту інформації*. URL: https://scpc.gov.ua/uk/articles/402 (дата звернення: 13.03.2026).

References:

1. Tarasenko, O. (2024). Udoskonalennia instrumentariiu zabezpechennia informatsiinoi bezpeky derzhavy [Improvement of the state's information security toolkit]. *Proceedings of the International Scientific and Practical Conference "SBU v umovakh viiny v Ukraini: suchasni realii ta innovatsiini stratehii zabezpechennia natsionalnoi bezpeky" [SSU in the conditions of war in Ukraine: modern realities and innovative strategies for ensuring national security]*, 142–144. Kyiv: Alerta. [in Ukrainian].

2. Zimenko, O. Ye. (2022). Fenomen informatsiinoho vplyvu u naukovomu seredovyshchi: teorii, definitsii [The phenomenon of information influence in the scientific environment: theories, definitions]. *Bibliotekoznavstvo. Dokumentoznavstvo. Informolohiia [Library Science. Record Management. Informology]*, (1), 90–97. [in Ukrainian].

3. Honcharenko, I. H. (2023). Kiberzahrozy finansovoho sektora v umovakh viiny [Cyber threats to the financial sector in conditions of war]. *Ekonomika ta suspilstvo [Economy and Society]*, (50). Retrieved from http://surl.li/tjtmk [in Ukrainian].

4. Puhachov, O. I. (2025). *Udoskonalennia derzhavnykh mekhanizmiv zabezpechennia informatsiinoi bezpeky Ukrainy [Improvement of state mechanisms for ensuring information security of Ukraine]* (Doctor's thesis). Tavriiskyi natsionalnyi universytet imeni V. I. Vernadskoho, Kyiv. Retrieved from https://etnuir.tnu.edu.ua/bitstream/handle/123456789/462/dis_Puhachov.pdf [in Ukrainian].

5. Zaporozhchenko, M. (2023). Fishynh yak posluha [Phishing as a service]. *Proceedings of the National Scientific and Practical Conference "Cyber resilience strategies: risk management and business continuity"*, 47–49. Kyiv: Derzhavnyi universytet informatsiino-komunikatsiinykh tekhnolohii. [in Ukrainian].

6. Kovalchuk, D. (2025). Utilising large language models for automated real-time cyber threat analysis (Vykorystannia velykykh movnykh modelei dlia avtomatyzovanoho analizu

ISSN 2786-6025 Online
kiberzahroz u realnomu chasi) [Utilising large language models for automated real-time cyber threat analysis]. *Visnyk Cherkaskoho derzhavnoho tekhnolohichnoho universytetu [Bulletin of Cherkasy State Technological University]*, 30(1), 49–55. [in Ukrainian].

7. Lunhol, O. M. (2022). Udoskonalennia profesiinoi pidhotovky maibutnikh fakhivtsiv pravookhoronnoi diialnosti zasobamy informatsiinykh tekhnolohii [Improving the professional training of future law enforcement specialists by means of information technologies]. *Nauka i tekhnika sohodni [Science and Technology Today]*, (7), 153–163. [in Ukrainian].

8. Tsurkan, O., Haborets, O., & Lunhol, O. (2023). Innovative development of technologies in training future law enforcement specialists. *Science and Technology Today*, (12), 96–106. [in English].

9. Haborets, O., & Chernobrov, V. (2023). Social engineering as a means of influence on people consciousness. *Proceedings of the International Scientific and Practical Conference "Determinanty posylennia roli osvity u povoiennomu vidnovlenni Ukrainy: Bereznevyi naukovyi dyskurs 2023" [Determinants of strengthening the role of education in the post-war recovery of Ukraine: March scientific discourse 2023]*, 204–205. Chernihiv: HO "Naukovo-osvitnii innovatsiinyi tsentr suspilnykh transformatsii". [in Ukrainian].

10. Kovalenko, O. M., et al. (2025). Vykorystannia shtuchnoho intelektu v kiberbezpetsi [The use of artificial intelligence in cybersecurity]. *Informatyka ta matematychni metody v modeliuvanni [Informatics and Mathematical Methods in Modeling]*, 15(1), 115–125. [in Ukrainian].

11. Derzhavnyi tsentr kiberzakhystu Derzhavnoi sluzhby spetsialnoho zviazku ta zakhystu informatsii. (2025). *Operatyvnyi tsentr reahuvannia na kiberintsydenty opryliudnyv richnyi zvit pro robotu Systemy vyiavlennia vrazlyvostei i reahuvannia na kiberintsydenty ta kiberataky (SVV) za 2025 rik [The Cyber Incident Response Center has published the annual report on the operation of the Vulnerability Detection and Cyber Incident Response System (SVV) for 2025]*. Retrieved from https://scpc.gov.ua/uk/articles/402 [in Ukrainian].

Дата першого надходження статті до видання: 13.03.2026
Дата прийняття статті до друку після рецензування: 27.03.2026