МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
МІЖНАРОДНИЙ ГУМАНІТАРНИЙ УНІВЕРСИТЕТ

МІЖНАРОДНА КОНФЕРЕНЦІЯ

ПЕРЕДОВІ ТЕХНОЛОГІЇ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНІЙ ІНЖЕНЕРІЇ

(ATICE'2025)

ОДЕСА, УКРАЇНА, 18 ЛИПНЯ 2025 Р.

МАТЕРІАЛИ КОНФЕРЕНЦІЇ

ОДЕСА

2025

MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE

INTERNATIONAL HUMANITARIAN UNIVERSITY

INTERNATIONAL CONFERENCE

ADVANCED TECHNOLOGY IN INFORMATION AND COMMUNICATION ENGINEERING

(ATICE'2025)

ODESA, UKRAINE, JULY 18, 2025

CONFERENCE PROCEEDINGS

ODESA

2025

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
МІЖНАРОДНИЙ ГУМАНІТАРНИЙ УНІВЕРСИТЕТ

ПЕРЕДОВІ ТЕХНОЛОГІЇ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНІЙ ІНЖЕНЕРІЇ

МАТЕРІАЛИ КОНФЕРЕНЦІЇ

Одеса, Україна, 18 липня 2025 р.

Видавничий дім
«Гельветика»
2025

MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE
INTERNATIONAL HUMANITARIAN UNIVERSITY

International Conference "Advanced Technology in Information and Communication Engineering" (ATICE'2025)

Odesa, Ukraine, July 18, 2025

Conference Proceedings

Видавничий дім
«Гельветика»
2025

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
МІЖНАРОДНИЙ ГУМАНІТАРНИЙ УНІВЕРСИТЕТ

Міжнародна конференція «Передові технології в інформаційно-комунікаційній інженерії» (ПТІКІ'2025)

Одеса, Україна, 18 липня 2025 р.

Матеріали конференції

Видавничий дім
«Гельветика»
2025

International Conference “Advanced Technology in Information and Communication Engineering” (ATICE’2025): Conference Proceedings. Odesa : International humanitarian university, 2025, 123 p.

DOI:

Міжнародна конференція «Передові технології в інформаційно-комунікаційній інженерії» (ATICE'2025): Матеріали конференції. Міжнародний гуманітарний університет, 2025. – Одеса: Видавничий дім «Гельветика», 2025. – 123 с.

ISBN 978-617-554-582-9

Збірка містить праці Міжнародної конференції з інформаційних систем, технологій захисту інформації, використання сучасних інформаційних технологій в управлінні системами за різними галузями народного господарства.

Матеріали публікуються в авторській редакції.

КОМІТЕТ МІЖНАРОДНИХ ЗВ'ЯЗКІВ

СТРЕЛКОВСЬКА І.В. – д.т.н., проф., Міжнародний гуманітарний університет, м.Одеса, Україна.

ГЛОБА Л. С . – д.т.н., проф., Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», м.Київ, Україна.

ВЧЕНИЙ СЕКРЕТАР

СОЛОВСЬКА І.М. – к.т.н., доц., Міжнародний гуманітарний університет, м.Одеса, Україна.

ГРИГОР'ЄВА Т.І. – к.т.н., доц., Міжнародний гуманітарний університет, м.Одеса, Україна.

ТЕХНІЧНО-ПРОГРАМНИЙ КОМІТЕТ

СТРЕЛКОВСЬКА І.В. – д.т.н., проф., Міжнародний гуманітарний університет, м.Одеса, Україна.

УРИВСЬКИЙ Л.О. – д.т.н., проф., Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», м.Київ, Україна.

ГЛОБА Л.С. – д.т.н., проф., Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», м.Київ, Україна.

СЕКЦІЇ

СЕКЦІЯ 1. ІНЖЕНЕРІЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

СТРЕЛКОВСЬКА І.В. – д.т.н., проф., Міжнародний гуманітарний університет, м.Одеса, Україна.

ГЛОБА Л.С. – д.т.н., проф., Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», м.Київ, Україна.

ГРИГОР'ЄВА Т.І. – к.т.н., доц., Міжнародний гуманітарний університет, м.Одеса, Україна.

СЕКЦІЯ 2. КОМП'ЮТЕРНІ НАУКИ ТА КОМП'ЮТЕРНА ІНЖЕНЕРІЯ

МІРОШНИК М.А. – д.т.н., проф., Міжнародний гуманітарний університет, м.Одеса, Україна.

СОЛОВСЬКА І.М. – к.т.н., доц., Міжнародний гуманітарний університет, м.Одеса, Україна.

РУСУ О.П. – к.т.н., доц., Міжнародний гуманітарний університет, м.Одеса, Україна.

СЕКЦІЯ 3. КІБЕРБЕЗПЕКА ТА ЗАХИСТ ІНФОРМАЦІЇ

ЛУНТОВСЬКИЙ А.О. – д.т.н., проф., Державна академія Саксонії «Беруфсакадемія», м. Дрезден, Німеччина.

ЙОНА Л.Г. – к.т.н., доц., Міжнародний гуманітарний університет, Одеса, Україна.

МАНЬКО Д.Г. – д.ю.н., проф., Міжнародний гуманітарний університет, м.Одеса, Україна.

СЕКЦІЯ 4. ЕЛЕКТРОННІ КОМУНІКАЦІЇ ТА РАДІОТЕХНІКА

УРИВСЬКИЙ Л.О. – д.т.н., проф., Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», м.Київ, Україна.

ЛЕМЕШКО А.В. – д.т.н., проф., Харківський національний університет радіоелектроніки, м. Харків, Україна.

ПЕДЯШ В.В. – к.т.н., доц., Міжнародний гуманітарний університет, м.Одеса, Україна.

СЕКЦІЯ 5. ІНФОРМАТИКА ТА ПРОГРАМУВАННЯ В ОСВІТІ

КУЧАЙ О.В. - д.п.н., проф., Національний університет біоресурсів і природокористування України.

ЖИГУЛІН О.А. – д.е.н., проф., Міжнародний гуманітарний університет, Одеса, Україна

ГОРБАЧОВ В.Е. – к.т.н., доц., Міжнародний гуманітарний університет, м.Одеса, Україна.

Разом із тим впровадження блокчейн-рішень не позбавлене викликів, зокрема проблем масштабованості, конфіденційності, регуляторних невизначеностей та людського фактора. Це підкреслює необхідність комплексного підходу, що має включати не лише технічні рішення, а й чітке правове регулювання, організаційні заходи та підвищення компетенцій користувачів.

Подальші дослідження у цьому напрямі мають бути зосереджені на поєднанні блокчейн-технологій з іншими інноваційними інструментами кіберзахисту — такими як штучний інтелект чи інтернет речей — для підвищення ефективності систем контролю даних і мінімізації ризиків. У довгостроковій перспективі це сприятиме зміцненню довіри до цифрових екосистем, зростанню прозорості процесів і посиленню кіберстійкості суспільства в цілому.

Література

1. Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System. 2008.
2. Swan M. Blockchain: Blueprint for a New Economy. 2015.
3. Yli-Huumo J., Ko D., Choi S., Park S., Smolander K. Where Is Current Research on Blockchain Technology? A Systematic Review. 2016.

Головатюк К.В.
студент факультету Кібербезпека, спеціальність 125
Міжнародний гуманітарний університет
kostya93.06@gmail.com
Науковий керівник Йона Л.Г.

ФІШИНГ ЯК ЗАГРОЗА КІБЕРБЕЗПЕЦІ

Анотація. *Розглядається фішинг як одна з найпоширеніших і найнебезпечніших кіберзагроз сучасності, зокрема в контексті гібридної війни проти України. Аналізуються різновиди атак — spear-phishing, фармінг, вішинг — та їх цілі: викрадення даних, інфікування пристроїв, маніпуляція користувачем. Підкреслюється роль соціальних мереж у поширенні фішингових схем, а також економічна зацікавленість зловмисників. Окремо надано рекомендації для захисту користувачів і приклади дій українських кіберфахівців у виявленні та блокуванні фішингових ресурсів.*

У сучасному світі кіберзагроз фішинг вийшов на одне з перших місць за масштабами та наслідками. Це форма атаки соціальної інженерії, коли зловмисники вводять жертву в оману з метою викрадення даних або інфікування пристроїв шкідливим ПЗ. Зазвичай використовується електронна пошта, фальшиві сайти, повідомлення у месенджерах або навіть телефонні дзвінки.

Цей тип атаки побудований не лише на технічних уразливостях, а й на психологічному впливі. Атакуючі ретельно імітують комунікацію з надійним джерелом — банком, державною установою або знайомим контактом — аби викликати довіру та змусити користувача вчинити певну дію: перейти за посиланням, ввести паролі або завантажити заражений файл. Фішинг часто є першим етапом більш складної атаки, яка може завершитися повним контролем над пристроєм жертви або мережею організації.

Особливу небезпеку фішинг несе в умовах гібридної війни проти України, коли атаки націлені не лише на громадян, а й на інститути державної влади, критичну інфраструктуру, медіа та навіть благодійні організації [3].

У таких випадках фішинг є частиною цілеспрямованої інформаційно-психологічної операції, яка має на меті дестабілізувати суспільство, зірвати функціонування важливих державних механізмів або скомпрометувати осіб, дотичних до військових чи урядових процесів. Саме тому державні структури в Україні щодня фіксують сотні подібних атак, спрямованих на поширення дезінформації, крадіжку даних або зрив роботи критичних систем.

У межах адресних атак, зокрема spear-phishing, злочинці попередньо збирають інформацію про жертву, щоб повідомлення виглядало максимально переконливо. Часто використовуються прикріплені документи з шкідливими макросами у форматі Excel, як-от у випадках розгортання інструментарію Cobalt Strike проти українських користувачів, зафіксованих у 2023–2024 роках [2].

Spear-phishing, як цільова атака, значно ефективніший за масовий фішинг. Використання персоналізованих звернень, знань про коло контактів або посадову діяльність робить такі листи правдоподібними, іноді — навіть незаперечно достовірними на перший погляд. Це підвищує шанси користувача натиснути небезпечне посилання або завантажити інфікований файл, що відкриває доступ до внутрішніх систем організації.

Серед особливо небезпечних форм фішингу вирізняється також фармінг — автоматичне перенаправлення користувача на підроблений сайт через зміну файлу hosts або DNS-записів. Такий тип атаки особливо складно виявити та заблокувати, і на сьогодні не існує гарантованих способів повної протидії [2].

Фармінг небезпечний тим, що жертва навіть не підозрює, що її перенаправили на фальшиву копію знайомого ресурсу. Візуально все виглядає коректно: дизайн, логотип, структура сайту і навіть сертифікат безпеки можуть бути підроблені або вкрадені. Зловмисник отримує всі дані, які користувач вводить — логіни, паролі, банківську інформацію тощо. Через це такі атаки мають високий коефіцієнт успішності, особливо проти користувачів, які не звикли перевіряти URL-адресу чи цифрові сертифікати.

Відомі випадки вішингу — телефонних дзвінків з комп'ютерним голосом, що імітує службу безпеки банку. Жертву просять ввести 16-значний номер карти та інші персональні дані через клавіатуру телефону [2]. Атака може бути доповнена психологічним тиском, коли злочинець повідомляє про "негайне блокування рахунку".

Така схема працює завдяки автоматизованим дзвінкам (робо-дзвінкам), які можуть охопити десятки тисяч номерів за добу. Навіть невеликий відсоток довірливих користувачів може принести шахраям значні прибутки. Особливо небезпечно це для літніх людей, які менш обізнані з цифровими загрозами.

За підрахунками, 70% фішингових атак у соціальних мережах досягають своєї мети. Найпоширенішими платформами для атак є Facebook, LinkedIn та Telegram, де зловмисники поширюють фішингові посилання або використовують скрипти для перехоплення браузера (browser hooking) [2], [3].

Соціальні мережі надають зловмисникам зручний інструмент для вивчення потенційних жертв, побудови фальшивих акаунтів, проведення атак під виглядом «друга» чи знайомого, а також широкого розповсюдження шкідливого контенту. Особливу загрозу становлять вкладення, які відкриваються в браузері без попереджень, або «опитування», що збирають персональні дані.

Важливу роль відіграє економічна мотивація атак. Згідно з аналітичними оцінками, масований фішинг може приносити прибуток до 14 тисяч доларів з мільйона листів, тоді як цільовий фішинг — до 150 тисяч доларів лише з тисячі надісланих повідомлень. У другому випадку успішність досягає 50% через високий рівень персоналізації атаки [2].

Це свідчить про комерціалізацію кіберзлочинності, де фішинг використовується не лише хакерами-одинаками, а й організованими групами з чіткою структурою, фінансуванням

і навіть розподілом ролей. У деяких випадках зловмисники пропонують послуги «фішинг як сервіс» (Phishing-as-a-Service), коли будь-хто може купити доступ до готових інструментів атаки.

Окрім фінансових втрат, наслідками фішингу є витік критично важливої інформації, зокрема даних облікових записів, конфіденційної кореспонденції, внутрішніх документів. Такі атаки часто є початковою ланкою для масових заражень шкідливим ПЗ, включно з бекдорами, кейлогерами та інструментами для повного контролю над інфраструктурою [2].

Таким чином, одна фішингова атака може відкрити ворота до повномасштабної компрометації системи. У разі втрати корпоративного доступу — це загрожує зривом операцій, фінансовими штрафами, репутаційними втратами та навіть кримінальною відповідальністю за порушення законодавства у сфері захисту персональних даних.

Урядова команда CERT-UA постійно фіксує нові фішингові сайти, які імітують державні портали. Наприклад, підроблений сайт portal.nazk.org.ua маскувався під офіційний реєстр декларацій portal.nazk.gov.ua. Громадянам рекомендується звертати увагу на домен .gov.ua, уникати відкриття підозрілих листів і не вводити дані без перевірки сайту [1].

Цей приклад ще раз доводить, наскільки легко зловмисники можуть імітувати навіть офіційні ресурси, якщо користувачі не звикли уважно перевіряти адреси сторінок. Саме тому особливої ваги набуває просвіта та цифрова гігієна населення.

Фішинг — це не просто технічний виклик, а глибоко психологічна та соціальна загроза, що базується на довірі, неуважності або стресі. В умовах гібридної війни він перетворюється на ефективну зброю в руках супротивника, здатну паралізувати роботу цілих установ чи підрозділів. Успішна протидія цій загрозі можлива лише за умов поєднання технологічних рішень (фільтрів, антивірусів, моніторингових систем) та людського чинника — навчання, пильності, обізнаності. Особливої важливості набуває тісна взаємодія між державними органами, приватними компаніями та громадянським суспільством, адже тільки спільними зусиллями можна забезпечити реальний захист у цифровій війні, що точиться сьогодні на кіберфронті України.

Література:

1. CERT-UA. Як убезпечитися від фішингового сайта? [Електронний ресурс]. – Режим доступу: https://cert.gov.ua/article/2808

2. Інформаційна безпека: проблеми правового забезпечення та технологічного супроводу. – К.: Інститут інформації, безпеки і права, 2022. – 358 с.

3. Бурячок А. І. Інформаційна безпека в умовах гібридної війни: фішинг як інструмент соціальної інженерії. // Науково-аналітичний вісник. – 2023. – №4. – С. 110–140.

4. Аналітичний звіт з питань кібербезпеки в Україні: загрози та протидія. – ХНТУ, 2024. – С. 330–345.

УДК: 004.056 : 004.4

Царенко Євгеній Валентинович
Здобувач другого (магістерського) рівня вищої освіти факультету кібербезпеки, програмної інженерії та комп'ютерних наук, спеціальність «Кібербезпека та захист інформації»
Міжнародний Гуманітарний Університет
i.am.zhenya.tsarenko@gmail.com
Науковий керівник
Йона Лариса Григорівна
к.т.н., доцент