МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
МІЖНАРОДНИЙ УНІВЕРСИТЕТ

ПЕРЕДОВІ ТЕХНОЛОГІЇ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНІЙ ІНЖЕНЕРІЇ

МАТЕРІАЛИ КОНФЕРЕНЦІЇ
(зимовий форум)

Одеса, Україна, 14 листопада 2025 р.

Одеса
2025

MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE
INTERNATIONAL UNIVERSITY

International Conference “Advanced Technology in Information and Communication Engineering” (ATICE’2025)

Odesa, Ukraine, November 14, 2025

Conference Proceedings
(winter forum)

Odesa
2025

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
МІЖНАРОДНИЙ УНІВЕРСИТЕТ

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

Одеса, Україна, 14 листопада 2025 р.

Матеріали конференції
(зимовий форум)

Одеса
2025

International Conference “Advanced Technology in Information and Communication Engineering” (ATICE’2025): Conference Proceedings (winter forum). Odesa : International university, 2025, 101 p.

DOI:

Міжнародна конференція «Передові технології в інформаційно-комунікаційній інженерії» (ATICE'2025): Матеріали конференції (зимовий форум). Одеса : Міжнародний університет, 2025, 101 с.

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.

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

ТЕХНІЧНО-ПРОГРАМНИЙ КОМІТЕТ

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

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

МІРОШНИК М.А. – д.т.н., проф., Міжнародний університет, м.Одеса, Україна.
СОЛОВСЬКА І.М. – к.т.н., доц., Міжнародний університет, м.Одеса, Україна.
РУСУ О.П. – к.т.н., доц., Міжнародний 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 університет, Одеса, Україна.
МАНЬКО Д.Г. – д.ю.н., проф., Міжнародний 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 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 університет, Одеса, Україна
ГОРБАЧОВ В.Е. – к.т.н., доц., Міжнародний університет, м.Одеса, Україна.

ЗМІСТ

Головатюк К.В.
студент факультету Кібербезпека, спеціальність 125
Міжнародний університет
kostya93.06@gmail.com
Науковий керівник Григор'єва Т.І.

ОПТИМІЗАЦІЯ ПРОЦЕСІВ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ПРИ АТАКАХ ФІШИНГУ ІЗ ЗАСТОСУВАННЯМ НЕЧІТКОЇ ЛОГІКИ

Анотація. *В роботі проведено аналіз основних каналів поширення фішингових атак та визначені ключові фактори, що впливають на рівень ризику. Запропоновано використання нечіткої логіки для оптимізації процесів виявлення, аналізу та протидії фішинговим атакам (email-phishing, smishing, vishing). Проведено дослідження статистичних даних про успішність різних каналів атак. Запропонована модель із застосуванням нечіткої логіки, яка дозволяє оцінити ризик загрози та адаптувати реакцію систем кібербезпеки відповідно до ступеня ризику.*

У сучасному цифровому світі фішинг займає одне з провідних місць серед кіберзагроз за масштабами та наслідками. Тому тема дослідження є актуальною. Фішинг - це форма атаки соціальної інженерії, коли зловмисники вводять жертву в оману з метою викрадення даних або інфікування пристроїв шкідливим програмним забезпеченням [1]. Найпоширенішими каналами для фішингу є електронна пошта, фальшиві сайти, повідомлення у месенджерах, SMS та телефонні дзвінки - інструменти, які дозволяють атакуючим імітувати комунікацію від банку, державної установи або знайомого контакту, щоб викликати довіру й змусити користувача виконати небезпечну дію: перейти за посиланням, ввести паролі чи завантажити файл.

Фішинг спирається не лише на технічні вразливості, а й на психологічний вплив: страх, терміновість, цікавість або соціальний тиск підвищують імовірність помилки користувача. Особливо небезпечним фішинг стає в умовах гібридної війни проти України, коли атаки цілеспрямовано спрямовуються на громадян, державні інститути, критичну інфраструктуру, медіа та благодійні організації [1]. У таких випадках фішинг може слугувати елементом інформаційно-психологічної операції з метою дестабілізації, компрометації осіб або зриву роботи важливих державних механізмів. Державні структури в Україні щодня фіксують сотні подібних атак, спрямованих на поширення дезінформації, крадіжку даних та ін.

Існують різні форми фішингу, кожна зі своїми механіками та ризиками.

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) [1], [2].

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 [3].

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, а також застосування технологічних заходів - фільтрів, антивірусів, моніторингу, оновлення DNS/сертифікатів.

Разом з тим традиційні підходи виявлення («атака/не атака») не завжди ефективні через невизначену та адаптивну природу фішингових кампаній. Тут корисніші гнучкі моделі оцінки ризику, зокрема підхід на основі нечіткої логіки, який дозволяє вводити ступені ризику і

оперувати нечіткими змінними: рівень довіри до відправника, схожість домену, персоналізація повідомлення, історія реакції користувача, канал доставки (e-mail, SMS, телефон) на їх підставі приймати гнучкі рішення - блокувати, попереджати чи передавати на ручну перевірку.

Наприклад, статистичні показники свідчать, що успішність різних каналів варіює: у 2024 році приблизно 8-9 кліків на 1000 email-листів, smishing демонструє значно вищу середню «успішність» (приблизно 8% у деяких дослідженнях), а vishing - близько 6-7% у симульованих тестах. На підставі таких даних нечітка модель може присвоювати каналу більшу вагу (наприклад, SMS як «високий ризик») і комбінувати її з показниками персоналізації й схожості домену, формуючи кінцевий рівень ризику.

В роботі запропоновано побудова математичної моделі оцінки ризику з використанням нечіткої логіки. Для оцінки ризику фішингової атаки пропонуються такі змінні для застосування моделі на основі нечіткої логіки:

A - схожість домену (низька/середня/висока);

B - персоналізація повідомлення (низька/середня/висока);

C - історія реакції користувача (обережний/сумнівний/необережний);

D - канал (email/SMS/телефонний дзвінок).

Рівень загрози (E) будемо визначати за допомогою функції:

$$E = f(A, B, C, D).$$

Наприклад, якщо (D = SMS) і (B = висока) і (A = середня/висока) → ризик загрози (E) = високий, або якщо (D = телефон) і (C = необережний) → ризик загрози (E) = середній-високий.

Роботизований контакт (бот-дзвінок або SMS-авторозсилка) має провести тестування реакції адресату. За результатами цього тестування нечітка модель має визначити «ступінь зацікавленості». Якщо ступінь перевищує встановлений поріг, то має підключитися живий оператор. Якщо ступінь менша за поріг, процес завершується або ставиться на паузу. Процес оптимізації пропонується реалізувати через мінімізацію цільової функції ризику.

Таким чином, на практиці побудована модель дозволить автоматично блокувати або попереджати про повідомлення з високим ризиком, передавати сумнівні випадки на ручну перевірку, оптимізувати розподіл ресурсів (що дозволяє операторам концентруються на високоризикових контактах, а не на масових низькоризикових потоках).Запропонована модель дозволяє системі безпеки адаптуватися до змін у загрозах, наприклад, якщо зростає персоналізація в SMS-кампаніях, то система безпека підвищує вагу показника B).

Застосування нечіткої логіки може покращує точність виявлення фішингових атак у ситуаціях невизначеності та робить захист пропорційним рівню ризику. Однак технічні системи самі по собі не вирішать проблему повністю: необхідна тісна взаємодія між державними органами, приватним сектором і громадянським суспільством, постійний обмін інформацією про індикатори компрометації, а також регулярне навчання користувачів.

Фішинг - це комплексна загроза на стику технологій, психології та економіки злочинності. Ефективна протидія потребує одночасно інвестицій у технології, впровадження адаптивних моделей оцінки ризику і системну роботу з підвищення цифрової обізнаності населення - тільки так можна знизити ймовірність успішних атак і мінімізувати їхні наслідки в умовах сучасної кібернетичної війни.

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.

Висновки

1. Проведений аналіз показав, що фішинг залишається однією з найпоширеніших і найнебезпечніших кіберзагроз сучасності. Основними каналами поширення є електронна

пошта, SMS, соціальні мережі та телефонні дзвінки, які поєднують технічні прийоми зі способами психологічного впливу на користувача.

2. Запропоновано підхід до оцінювання ризику фішингових атак із використанням нечіткої логіки, який дозволяє гнучко враховувати такі параметри, як схожість домену, рівень персоналізації повідомлення, історія реакцій користувача та канал доставки. Це дає можливість системам кібербезпеки адаптувати реакцію до рівня загрози, зменшуючи навантаження на аналітиків і підвищуючи точність виявлення атак.

3. В роботі побудовано математичну модель із застосуванням нечіткої логіки, яка дозволяє оцінити ризик загрози та адаптувати реакцію системи кібербезпеки відповідно до ступеня ризику.

4. Реалізація нечіткої моделі в процесах моніторингу та реагування сприятиме оптимізації використання ресурсів, скороченню часу реагування на інциденти й зниженню кількості успішних атак. Поєднання технологічних засобів, обміну даними між установами та підвищення цифрової грамотності користувачів є ключовими умовами ефективної протидії фішингу в умовах сучасної кібервійни.

Література.

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

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

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

Проценко М.М.

здобувач вищої освіти третього (аспірантського рівня)

спеціальності 123 – Комп'ютерна інженерія

Науковий керівник: Мірошник М. А.

доктор технічних наук, професор

Міжнародний університет

місто Одеса, Україна

ПОРІВНЯЛЬНЕ ДОСЛІДЖЕННЯ МЕТОДІВ ТЕСТУВАННЯ БЕЗПЕКИ LLM-КОДУ: SAST, DAST, GRAPH-BASED ТА СИНТЕЗ ГІБРИДНОГО ПІДХОДУ

Анотація. *У сучасному програмуванні великі мовні моделі (LLM) широко застосовуються для автоматичної генерації коду, однак дослідження 2025 року показують, що такий код нерідко містить вразливості безпеки [1]. Традиційні методи тестування – статичний аналіз безпеки (SAST) та динамічне тестування (DAST) – не завжди справляються з цими викликами. SAST-інструменти сканують вихідний код до його виконання, але генерують багато хибних спрацювань і не розуміють повної семантики застосунку. DAST-підходи перевіряють програму під час роботи, виявляючи лише явні проблеми та пропускаючи приховані дефекти, особливо у складних системах.*