

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ ВАДИМА ГЕТЬМАНА**

**Навчально-науковий інститут «Інститут інформаційних технологій в
економіці»**

Кафедра системного аналізу та кібербезпеки

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА

«Системний аналіз»

ГАЛУЗЬ ЗНАНЬ

12 «Інформаційні технології»

СПЕЦІАЛЬНІСТЬ

124 «Системний аналіз»

Форма навчання: очна (денна)

КВАЛІФІКАЦІЙНА БАКАЛАВРСЬКА РОБОТА

на тему

**«Дослідження сучасних підходів до виявлення та протидії фішинговим атакам
та пов'язаному інтернет-шахрайству»**
здобувача Зайця Дмитра Ігоровича

(підпис)

Науковий керівник: к.ф.-м.н., доцент. Позднякович О.Є.

(підпис)

**Робота допущена до захисту перед екзаменаційною комісією з
атестації здобувачів вищої освіти (ЕК)**

Завідувач кафедри: д.ф.-м. н., професор, Джалладова І. А.

(підпис)

Київ 2026

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ ВАДИМА ГЕТЬМАНА**

Навчально-науковий інститут «Інститут інформаційних технологій в економіці»

Кафедра системного аналізу та кібербезпеки

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА **12 «Системний аналіз»**

СПЕЦІАЛЬНІСТЬ **124 «Системний аналіз»**

ПОГОДЖЕНО

Керівник проектної групи (гарант)
освітньо-професійної програми

Джалладова І.А.

_____ 2026 р.

ЗАТВЕРДЖУЮ

Завідувач кафедри системного
аналізу та кібербезпеки

Джалладова І.А.

_____ 2026 р.

ІНДИВІДУАЛЬНЕ ЗАВДАННЯ

здобувачу вищої освіти Зайця Дмитра Ігоровича

очної (денної) форми навчання

на підготовку кваліфікаційної бакалаврської роботи

**на тему «Дослідження сучасних підходів до виявлення та протидії фішинговим
атакам та пов'язаному інтернет-шахрайству»**

Тему затверджено наказом ректора Університету від _____
«Кваліфікаційна робота виконується на матеріалах монографічних праць у сферах кібербезпеки та соціальної інженерії, офіційних статистичних звітів провідних міжнародних організацій — APWG Phishing Activity Trends Report, Verizon Data Breach Investigations Report, , а також аналітичних матеріалів Урядової команди реагування CERT-UA, щодо фішингових кібератак проти державних установ та організацій України за 2020–2025 роки.

План кваліфікаційної бакалаврської роботи

Розділ 1	Теоретичні основи фішингових атак та інтернет-шахрайства
Розділ 2	Аналіз фішингових атак та інтернет-шахрайства
Розділ 3	Розроблення та обґрунтування заходів щодо підвищення ефективності виявлення та протидії фішинговим атакам
Об’єкт дослідження: засоби виявлення та протидії фішинговим атакам у цифровому середовищі. Воно включає технічні механізми здійснення атак, методи соціальної інженерії, які використовують зловмисники.	
Предмет дослідження: методи, моделі, алгоритми та інструментальні засоби виявлення та протидії фішинговим атакам у цифровому середовищі для користувачів, організацій та державних установ.	
Метою кваліфікаційної роботи є підвищення ефективності виявлення та протидії фішинговим атакам у цифровому середовищі шляхом розроблення, обґрунтування та практичного застосування багаторівневої методологічної моделі протидії фішингу, адаптованої до специфіки кіберзагроз в умовах гібридної агресії проти України.	
Конкретні завдання, які здобувач повинен виконати для досягнення поставленої мети: - Здійснити компаративний аналіз науково-теоретичних підходів до трактування фішингу та інтернет-шахрайства, дослідити психологічні механізми соціальної інженерії на основі концепцій Р. Чалдіні та Д. Канемана. - Проаналізувати фактологічну базу та статистичну динаміку поширення фішингових атак у світі та в Україні за період 2020–2025 років. - Здійснити порівняльний аналіз сучасних інформаційних технологій виявлення фішингу — від чорних списків до методів машинного навчання та штучного інтелекту — за критеріями ефективності. - Розробити та обґрунтувати багаторівневу методологічну модель протидії фішинговим атакам і модель оцінювання ризику на основі зважених факторів, адаптовані до умов активного кіберпротистояння. - Сформулювати комплексні практичні рекомендації щодо підвищення ефективності виявлення та протидії фішинговим атакам для організацій, державних установ та користувачів.	
У розділі 1	Дослідити теоретико-методологічні засади трактування фішингу та інтернет-шахрайства, проаналізувати психологічні механізми соціальної інженерії як основи фішингових атак і систематизувати методологічні підходи до їх виявлення та протидії.
У розділі 2	Проаналізувати фактологічні дані щодо поширеності фішингових атак у світі та в Україні, обґрунтувати розподіл типів і факторів успішності фішингових атак на основі статистичного та Парето-аналізу, а також розглянути практичні результати порівняння сучасних інформаційних технологій виявлення фішингу за ключовими показниками ефективності.
У розділі 3	Сформувати комплексний підхід до протидії фішинговим атакам, розробити багаторівневу модель протидії та модель оцінювання ризику на основі зважених факторів, а також спрогнозувати тенденції розвитку фішингових атак і оцінити ефективність запропонованих заходів.

Завдання підготував науковий керівник
Позднякович О.Є.

к.ф-м.н., доцент,

Завдання одержав здобувач

Заєць Д.І.

РЕФЕРАТ

Кваліфікаційна бакалаврська робота складається зі вступу, трьох розділів, загальних висновків, списку використаних джерел і містить : 51 сторінок, 1 рисунок, 8 таблиць, використаних джерел 17.

Об'єкт дослідження- процес виявлення та протидії фішинговим атакам і пов'язаному з ними інтернет-шахрайству в цифровому середовищі.

Предмет дослідження- методи, моделі, алгоритми та інструментальні засоби виявлення, оцінювання ризику та протидії фішинговим атакам у цифровому середовищі для користувачів, організацій та державних установ.

Мета кваліфікаційної роботи: дослідження теоретико-методологічних засад фішингу та соціальної інженерії, аналіз сучасних технологій виявлення фішингових атак та обґрунтування багаторівневої методологічної моделі протидії фішингу, адаптованої до умов активного кіберпротистояння.

Методи дослідження: теоретичний аналіз та порівняння концепцій соціальної інженерії; статистичний та порівняльний аналіз даних про поширення фішингових атак; Парето-аналіз факторів успішності атак; методи зважених факторів для оцінювання ризику.

Завданням кваліфікаційної бакалаврської роботи є проведення огляду науково-теоретичного генезису концепцій фішингу та психологічних механізмів соціальної інженерії, аналіз фактологічної бази та порівняння сучасних інформаційних технологій виявлення фішингу за критеріями ефективності, а також обґрунтування багаторівневої моделі протидії фішинговим атакам і розробка практичних рекомендацій щодо підвищення кібербезпеки.

Наукова новизна дослідження полягає в обґрунтуванні комплексного підходу до протидії фішинговим атакам шляхом інтеграції поведінкових механізмів соціальної інженерії з технологічними методами виявлення на основі машинного навчання, а також у розробці авторської моделі оцінювання ризику фішингових загроз на основі системи зважених факторів.

Ключові слова: ФІШИНГ, ІНТЕРНЕТ-ШАХРАЙСТВО, СОЦІАЛЬНА ІНЖЕНЕРІЯ, ОЦІНЮВАННЯ РИЗИКУ, МАШИННЕ НАВЧАННЯ, КІБЕРАТАКИ.

Рік виконання кваліфікаційної бакалаврської роботи: 2026.

Рік захисту кваліфікаційної бакалаврської роботи: 2026.

ВІДГУК

про кваліфікаційну бакалаврську роботу здобувача вищої освіти

Зайця Дмитра Ігоровича

Тема роботи: «Дослідження сучасних підходів до виявлення та протидії фішинговим атакам та пов'язаному інтернет-шахрайству».

Кваліфікаційна бакалаврська робота є ґрунтовним дослідженням актуальної проблеми. В умовах постійного зростання кількості фішингових атак питання їх своєчасного виявлення та протидії набуває особливої актуальності.

Структура роботи є логічною та послідовною. У теоретичній частині проведено якісний аналіз сутності фішингу, психологічних механізмів соціальної інженерії та методів виявлення кіберзагроз.

У практичній частині роботи Заєць Д.І. здійснив аналіз статистичних даних щодо поширення фішингових атак та розробив власну модель протидії фішинговим атакам і оцінювання ризику. Отримані результати мають практичну цінність.

Суттєвих недоліків не встановлено. Робота повною мірою відповідає чинним вимогам і допускається до захисту перед ЕК, а її автору може бути присвоєний ступінь бакалавра з системного аналізу за спеціальністю 124 «Системний аналіз».

Науковий керівник

доцент кафедри системного аналізу та кібербезпеки, доцент, кандидат фізико-математичних наук

Позднякович О.Є.

_____ 2026 р.

Рецензія

на кваліфікаційну бакалаврську
роботу здобувача вищої освіти

Зайця Дмитра Ігоровича

(прізвище, ім'я, по батькові)

Тема «Дослідження сучасних підходів до виявлення та протидії фішинговим атакам та пов'язаному інтернет-шахрайству»

Актуальність теми кваліфікаційної роботи

Тема кваліфікаційної бакалаврської роботи є надзвичайно актуальною в умовах теперішнього інформаційного середовища. Кіберполіція України щоденно фіксує сотні звернень від громадян та організацій, що постраждали від фішингових атак і пов'язаного інтернет-шахрайства. За оперативними даними Департаменту кіберполіції, фішинг залишається одним із найпоширеніших векторів кіберзлочинності в Україні. Вибір теми дослідження повністю відповідає пріоритетним напрямкам діяльності підрозділів кіберполіції та актуальним завданням у сфері протидії кіберзлочинності.

Якість проведеного дослідження

Робота виконана на належному науково рівні. Дмитром опрацьовано широку джерельну базу, що включає звіти провідних міжнародних організацій у сфері кібербезпеки, матеріали ФБР, Microsoft, а також дані CERT-UA. Дослідження охоплює період 2020–2025 років, що забезпечує актуальність наведеної статистики та достовірність зроблених висновків.

Позитивні риси кваліфікаційної бакалаврської роботи

Авторська п'ятирівнева модель протидії фішинговим атакам і модель оцінювання ризику на основі вагових коефіцієнтів є придатними до практичного застосування. Прогнозний аналіз із використанням трьох сценаріїв розвитку подій свідчить про здатність здобувача до стратегічного мислення.

Зауваження

Разом із тим робота не позбавлена окремих недоліків, усунення яких сприяло б підвищенню її наукової та практичної цінності.

1. Питання правового регулювання протидії фішингу в Україні висвітлено недостатньо — зокрема, відсутній аналіз практики притягнення винних осіб до відповідальності за статтями КК України та проблем, з якими стикаються органи досудового розслідування при кваліфікації фішингових злочинів.

2. У роботі відсутній аналіз механізмів міжнародного співробітництва у розслідуванні фішингових злочинів, зокрема взаємодії з Інтерполом, Europol та іноземними CERT-командами — тематика, яка є вкрай важливою для практичної діяльності кіберполіції.

Практична значимість висновків і рекомендацій

Результати дослідження мають очевидну практичну цінність для діяльності підрозділів кіберполіції та інших суб'єктів у сфері забезпечення кібербезпеки. Запропонована п'ятирівнева модель протидії фішинговим атакам може бути використана як методична основа при розробці корпоративних політик інформаційної безпеки для організацій, які звертаються до кіберполіції за консультативною підтримкою.

Загалом кваліфікаційна бакалаврська робота виконана на належному рівні, демонструє достатній рівень наукової зрілості здобувача та відповідає вимогам. Робота заслуговує на позитивну оцінку.

Місце роботи та посада рецензента Департамент кіберполіції Національної поліції України, начальник управління полковник поліції

Науковий

ступінь,

учене

звання

Куліш В. М.

(підпис, ПІБ)

Підпис засвідчую начальник управління полковник поліції

(посада, підпис)

Місце печатки організації, де працює рецензе

Зміст

ВСТУП.....	5
РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ ФІШИНГОВИХ АТАК ТА ІНТЕРНЕТ-ШАХРАЙСТВА	8
1.1. Теоретичні підходи до трактування інтернет-шахрайства та кіберзагроз	8
1.2. Концептуальні підходи до розуміння фішингових атак	11
1.3. Теоретичні основи соціальної інженерії у контексті фішингових атак	16
1.4. Методологічні підходи до виявлення та протидії фішинговим атакам.....	19
РОЗДІЛ 2. АНАЛІЗ ФІШИНГОВИХ АТАК ТА ІНТЕРНЕТ-ШАХРАЙСТВА.....	23
2.1. Фактологічне підтвердження поширеності фішингових атак	23
2.2. Інформаційно-аналітичний аналіз типів та факторів фішингових атак	24
2.3. Порівняльний аналіз сучасних інформаційних технологій виявлення фішингу	29
РОЗДІЛ 3. РОЗРОБЛЕННЯ ТА ОБҐРУНТУВАННЯ ЗАХОДІВ ЩОДО ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ВИЯВЛЕННЯ ТА ПРОТИДІЇ ФІШИНГОВИМ АТАКАМ.....	34
3.1. Формування комплексного підходу до протидії фішинговим атакам.....	34
3.2. Розроблення моделі оцінювання ризику фішингових атак	38
3.3. Прогнозування тенденцій розвитку фішингових атак	41
3.4. Оцінювання ефективності запропонованих заходів.....	44
ВИСНОВКИ.....	47
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ.....	50

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

Скорочення	Повна назва
AI	Artificial Intelligence — Штучний інтелект
APWG	Anti-Phishing Working Group — Антифішингова робоча група
APT	Advanced Persistent Threat — Складена постійна загроза
BEC	Business Email Compromise — Компрометація корпоративної електронної пошти
CERT-UA	Computer Emergency Response Team of Ukraine — Урядова команда реагування на комп'ютерні надзвичайні події України
DBIR	Data Breach Investigations Report — Звіт про розслідування витоків даних
DNS	Domain Name System — Система доменних імен
DKIM	DomainKeys Identified Mail — Пошта з ідентифікацією доменних ключів
DMARC	Domain-based Message Authentication, Reporting and Conformance — Автентифікація повідомлень на основі домену

ENISA	European Union Agency for Cybersecurity — Агентство ЄС з кібербезпеки
FBI	Federal Bureau of Investigation — Федеральне бюро розслідувань
FIDO2	Fast Identity Online 2 — Стандарт швидкої онлайн-ідентифікації
ГРУ	Головне розвідувальне управління Збройних сил Росії
IAM	Identity and Access Management — Управління ідентифікацією та доступом
IBM	International Business Machines — Міжнародні бізнес-машини

ВСТУП

Актуальність теми. В умовах швидкого розвитку суспільства фішингові атаки та інтернет-шахрайство досягли найвищого рівня глобальної кіберзагрози. Щороку кількість атак зростає у арифметичній прогресії. Понад 90% успішних кіберінцидентів починаються з фішингових повідомлень. Для України ця проблема особливо гостра під час гібридної війни в інформаційному просторі, де фішинг використовується не лише для фінансового шахрайства. Незважаючи на існування технічних засобів захисту, їх ефективність залишається недостатньою через людський фактор. Швидка адаптація зловмисників та відсутність комплексних методичних рекомендацій.

Аналіз останніх досліджень і публікацій. Явище фішингу досліджується в українській та закордонній науковій літературі. Дослідники по всьому світі, такі як А. Агарвал, Д. Дугган, М. Янсен та інші, класифікують свої роботи на вивченні технічних аспектів фішингових атак. Звіти провідних міжнародних організацій - APWG, Інтерполу, які щорічно публікують актуальну статистику. У науковому просторі питаннями кіберзахисту займаються у роботах українських дослідників у галузі інформаційної безпеки. Водночас, незважаючи на значний обсяг існуючих досліджень, переважна більшість з них стосується лише вузьких технічних аспектів виявлення

Мета дослідження є створення прикладних підходів для забезпечення виявлення та протидії фішинговим атакам. Мета полягає в підвищенні рівня кібербезпеки для користувачів, організацій та державних установ.

Відповідно до мети визначено **такі завдання:**

1. Розкрити основне поняття фішингу та інтернет-шахрайства і надати огляд його ключових типів та класифікації.

2.Дослідити сучасні тенденції фішингових атак на світовому та українському рівнях та вивчити актуальні статистичні дані щодо масштабів їх поширення.

3.Вивчити технічні механізми фішингових кампаній та методи соціальної інженерії, які використовують зловмисники.

4.Організувати наявні технічні засоби та інструменти для виявлення фішингових атак, включаючи інструменти машинного навчання та штучного інтелекту.

5.Дослідити національні та міжнародні організаційні та правові заходи боротьби з фішингом та інтернет-шахрайством.

6.Проаналізувати роль людського фактора у вразливості до фішингових атак та визначити способи підвищення обізнаності користувачів.

Об'єктом дослідження є засоби виявлення та протидії фішинговим атакам у цифровому середовищі. Воно включає технічні механізми здійснення атак, методи соціальної інженерії, які використовують зловмисники.

Область дослідження складається з сучасних методів, інструментів та підходів до виявлення та протидії фішинговим атакам і пов'язаним з ними інтернет-шахрайствам, включаючи технічні засоби автоматичного виявлення загроз на основі машинного навчання та штучного інтелекту, організаційні та правові механізми захисту, методи підвищення обізнаності користувачів, а також практичні методичні рекомендації для комплексного захисту від фішингу.

Методи дослідження. Для досягнення цілей проекту та вирішення поставлених завдань у роботі було застосовано поєднання загальнонаукових та спеціальних методів дослідження: Порівняльний аналіз — для цілей порівняння: оцінки сильних і слабких сторін, переваг та їх відмінностей серед механізмів, інструментів та технологій для пом'якшення фішингу. Статистичний метод — для аналізу кількісних даних про поширеність фішингових атак, динаміку їх зростання та завдані збитки. Метод узагальнення — для формулювання висновків на основі результатів дослідження та розробки прикладних рекомендацій. Системний підхід — для кращого уявлення про проблему фішингу як багатовимірною явища, що

охоплює технічні, організаційні, правові та соціальні аспекти. Моделювання — для аналізу типових сценаріїв фішингових атак та оцінки ефективності різних методів захисту.

Практична цінність дослідження полягає в тому, як запропоновані рекомендації та висновки можуть бути фактично використані: організаціями та підприємствами — для побудови ефективної системи захисту від фішингових атак та навчання персоналу; державними установами — для покращення політики та регулювання кібербезпеки; звичайними користувачами — для підвищення рівня особистої кібергігієни та захисту своїх даних в Інтернеті.

РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ ФІШИНГОВИХ АТАК ТА ІНТЕРНЕТ-ШАХРАЙСТВА

1.1. Теоретичні підходи до трактування інтернет-шахрайства та кіберзагроз

Інтернет-шахрайство почало привертати увагу дослідників наприкінці 1990-х років. Саме тоді почали масово використовувати Інтернет, а разом із ним з'явилися й нові форми злочинів. У широкому розумінні інтернет-шахрайство розглядається як будь-яке навмисне введення особи в оману з використанням мережі Інтернет з метою отримання матеріальної або іншої вигоди. Так, американський дослідник D. Wall ще у 2001 році у своїй праці запропонував розглядати кіберзлочинність через призму трьох трансформацій: традиційні злочини перемістилися в онлайн-середовище; з'явилися гібридні злочини, що поєднують офлайн та онлайн компоненти; виникли злочини, які існують виключно в мережевому середовищі. Ця модель залишається актуальною й дотепер.

Інший підхід пропонує британський кримінолог M. Butler, який наполягає на необхідності розрізняти поняття «*cyber-enabled fraud*» - шахрайство, яке стало можливим завдяки технологіям, але могло б існувати й без них — наприклад, фінансові піраміди та «*cyber-dependent fraud*»- шахрайство, яке принципово неможливе поза цифровим середовищем — наприклад, підробка цифрових підписів. Це розмежування є методологічно важливим, адже воно впливає на вибір інструментів протидії: перший тип потребує передусім правових заходів, другий — технічних.

Класифікація кіберзлочинів — виявилася значно складнішим, ніж могло здатися на перший погляд. Різні дослідники пропонували свої системи ще з 1990-х років. Проте жодна з них не стала універсальною. Причина проста: кіберзлочинність не стоїть на місці.

Найбільш поширеною у міжнародній практиці є класифікація, закладена в Будапештській конвенції про кіберзлочинність 2001. Першому та досі єдиному обов'язковому міжнародному договору у цій сфері, який Україна затвердила у 2005 році. Конвенція поділяє кіберзлочини на чотири групи:

-Злочини проти конфіденційності, цілісності та доступності комп'ютерних даних і систем — несанкціонований доступ, перехоплення даних, втручання в роботу систем.

-Комп'ютерні злочини — підробка та шахрайство з використанням комп'ютерів.

-Злочини, пов'язані зі змістом- розповсюдження забороненого контенту.

-Злочини, пов'язані з порушенням авторських прав.

Цікавою альтернативою є функціональна класифікація, запропонована Gordona & Forda 2006, які поділяють кіберзлочини залежно від того, яку роль у них відіграють технології:

Тип I — злочини, де технологія є основним знаряддям. Це DDoS-атаки, розповсюдження шкідливого ПЗ.

Тип II — злочини, де технологія є лише допоміжним засобом. Це кіберпереслідування, шахрайство через електронну пошту.

В українському законодавстві кіберзлочини розподілені між кількома статтями Кримінального кодексу: шахрайство (ст. 190), несанкціоноване втручання в роботу комп'ютерів (ст. 361), поширення шкідливих програм (ст. 361-1) та несанкціоновані дії з інформацією (ст. 362–363). Така розпорошеність законодавчих норм ускладнює правозастосування та статистичний облік, що неодноразово критикувалося у юридичній літературі.

Фішинг є одним із найстаріших видів кіберзагроз. Перша фішингова атака датується 1996 роком і була спрямована проти користувачів сервісу AOL. З тих пір техніки фішингу еволюціонували різноч. Базова психологічна механіка залишилася незмінною: зловмисник імітує довірену особу або організацію, щоб змусити жертву добровільно передати конфіденційні дані.

У сучасній ієрархії кіберзагроз, фішинг посідає особливе місце. Він є не самостійним кінцевим злочином, а передусім вектором атаки, тобто інструментом для досягнення інших злочинних цілей.

Таблиця 1.1 — Порівняння дослідників

Автор/Джере ло	Рік	Ключове визначення	Роль фішингу	Критична оцінка
D. Wall	01 20	Кіберзлочини як трансформація традиційних злочинів у три типи	Не виділяється окремо	Новаторська модель, але не враховує гібридні атаки
Thomas & Loader	00 20	Класифікація за об'єктом посягання (особа / власність / держава)	Злочин проти власності	Занадто спрощена для сучасних атак
M. Butler	13 20	Поділ на cyber-enabled та cyber-dependent злочини	Cyber-enabled	Практично цінне розмежування для вибору заходів протидії
Gordon & Ford	06 20	Функціональна класифікація (тип I / тип II)	Тип II	Зручна для операційного аналізу, слабка для правової кваліфікації
Будапештська конвенція	01 20	Чотирикатегорійна правова класифікація	Категорія 2 (комп'ютерне шахрайство)	Найбільш юридично обов'язкова, але технологічно застаріває
О. Користін	07 20	Фішинг як різновид ст. 190 КК України	Інструмент класичного шахрайства	Відповідає національному праву, але не відображає технічної специфіки

Понад 84% організацій, які зазнали витоку даних у 2024–2025 роках, стали жертвами через людський фактор, а не технічну вразливість.

Сучасна класифікація фішингових атак охоплює кілька основних різновидів:

1. Email-фішинг — масове розсилання оманливих листів, що імітують відомі бренди або державні установи.

2.Спір-фішинг (Spear phishing) — цільові атаки проти конкретної особи або організації з використанням персоналізованої інформації.

3.Вішинг (Vishing) — голосовий фішинг через телефонні дзвінки.

4.Смішинг (Smishing) — фішинг через SMS-повідомлення.

5.Фармінг (Pharming) — перенаправлення користувача на підроблений сайт без його відома, шляхом маніпуляцій із DNS.

6.Уейлінг (Whaling) — спір-фішинг, спрямований високопосадовців.

7.Клон-фішинг (Clone phishing) — точна копія легітимного листа з підміненими посиланнями або вкладеннями.

Фішинг займає унікальне місце в ієрархії кіберзагроз: він одночасно є самостійним злочинним діянням і ключовим підготовчим інструментом для більш складних атак. Українське законодавство наразі відстає від реального розвитку кіберзагроз, кваліфікуючи інтернет-шахрайство через призму традиційних норм без урахування цифрової специфіки. Все це обумовлює необхідність подальшого дослідження як технічних механізмів фішингових атак, так і правових інструментів протидії.

1.2. Концептуальні підходи до розуміння фішингових атак

Одна з найпоширеніших помилок фішингу полягає в тому, що його зводять тільки до технічної проблеми. Насправді фішинг є соціально-технічним явищем, у якому технологія відіграє роль інструменту. Справжнім об'єктом маніпуляції залишається людська психологія. Саме ця подвійна природа робить фішинг настільки стійким до протидії. Ми можемо побудувати хороший технічний захист і все одно програти, якщо жертва передає свої дані зловмиснику.

Підхід соціальної інженерії як основи фішингових атак була детально розроблена дослідником К. Мітніком у праці *The Art of Deception* ще у 2002 році. Дослідник стверджував, що людський фактор є найслабшою ланкою будь-якої

системи безпеки. Фішинг є не просто технічним прийомом, а цілою системою психологічного впливу.

Дослідники Workman та Bommer у роботі *Changing Organizational Security Mindsets* підкреслили, що успішність фішингових атак пов'язане не стільки з технічною складністю атаки, скільки з рівнем психологічного стресу жертви в момент отримання повідомлення.

Дослідник Д. Ленгтон вважав, що фішинг найчастіше успішний тоді, коли користувачі гірше розуміються на цифрових технологіях. Таким чином, проблема фішингу є водночас технічною, психологічною та соціальною. Наукові уявлення про фішинг пройшли кілька етапів розвитку.

Перший етап: технічний детермінізм. Ранні визначення фішингу, що з'явилися у другій половині 1990-х та на початку 2000-х років, зосереджувалися на технічних характеристиках атаки.

Другий етап: психологічний поворот. Приблизно з 2005 року у науковій літературі почав домінувати психологічний вимір фішингу. Дослідження Дж. Хонга та Л. Кранор показали, що успіх фішингових атак залежить передусім від того, наскільки переконливо та якісно побудовані методи обману. У цей період почали з'являтися перші поділи фішингових атак, які ґрунтувалися на психологічному впливі на людей.

Третій етап: системний підхід. Починаючи приблизно з 2010 року дослідники почали розглядати фішинг як системне явище, що включає в себе: технічний, психологічний, організаційний компоненти. Цей підхід відображено у структурі NIST та документах ENISA, де фішинг визначається як «багатовимірна загроза, що потребує комплексного реагування».

Четвертий етап: адаптивні та AI-орієнтовані загрози. З кінця 2010-х і особливо після 2020 року в науковій літературі почали з'являтися роботи, присвячені новому поколінню фішингових атак.

Моделі фішингу, що були сформульовані в 2000-х роках, описували атаку як просту послідовність: підготовка підробленого ресурсу, доставка оманливого

повідомлення та збір введених жертвою даних. Ця модель чудово описувала масові фішингові кампанії проти клієнтів банків або великих онлайн-платформ.

**Таблиця 1.2 — Порівняння класичних та сучасних моделей
фішингових атак**

Критерій	Класична модель	Сучасна модель
Основний канал	Електронна пошта	Email, SMS, голос, месенджери, соцмережі, QR-коди
Цільова аудиторія	Масова, невивіркова	Персоналізована, цільова або ультрацільова
Рівень персоналізації	Низький	Високий, з використанням OSINT та AI
Технічна складність	Низька	Середня — висока
Тривалість атаки	Одноразова	Багатоетапна, може тривати тижні
Мета	Крадіжка облікових даних	Фінансові злочини, шпигунство, APT, ransomware
Психологічний інструментарій	Терміновість, страх	Довіра, стосунки, авторитет, поступова маніпуляція
Виявлення	Відносно просте	Складне, часто неможливе без AI-інструментів

Особливої уваги заслуговує феномен так званого Business Email Compromise, що являє собою спір-фішинг, спрямовану проти фінансових операцій підприємств. За даними ФБР, збитки від BEC у 2022 році перевищили 2,7 мільярда доларів лише в США. BEC є яскравим прикладом того, як еволюціонувала сам фішинг.

Попри десятиліття досліджень, у науковій спільноті досі немає розуміння щодо того, як класифікувати фішинг у системі кіберзагроз. Ця термінологічна та класифікаційна невизначеність є проблемою — вона безпосередньо впливає на якість законодавства, та ефективність заходів протидії.

Перша проблема пов'язана з розмитістю понять. У науковій літературі відсутня чітка розмежування між фішингом, соціальною інженерією, вішингом, та смішингом. Одні автори розглядають фішинг як загальне поняття, яке охоплює всі форми обману в цифровому середовищі.

Друга проблема — конкуренція між правовим та технічним підходами до класифікації. З правової точки зору фішинг є шахрайством. З технічної — він є вектором атаки, що може слугувати підготовчим етапом для інших злочинів. Ця двозначність призводить до того, що в різних юрисдикціях одні й ті самі дії можуть кваліфікуватися принципово по-різному.

Третя проблема полягає у стрімкій еволюції фішингу. Поява кожного нового каналу комунікації — месенджерів, QR-кодів, голосових асистентів, платформ метавсесвіту — породжує нові форми фішингу.

Аналіз підходів до розуміння фішингу показав кілька важливих речей. Фішинг не можна пояснити лише технічно або лише психологічно. Ці два виміри нерозривно пов'язані. Тільки разом вони дають повну картину.

Наука змінювала погляд на фішинг разом із тим, як змінювалися самі атаки. Прості масові розсилки поступилися місцем точковим операціям із використанням штучного інтелекту. Старі моделі вже не описують того, що відбувається насправді. Їх потрібно оновлювати.

В цій роботі запропоновано власне визначення:

Фішинг — це цілеспрямований соціально-технічний обман у цифровому середовищі. Воно враховує обидва виміри явища і стане основою для подальшого аналізу.

1.3. Теоретичні основи соціальної інженерії у контексті фішингових атак

Розуміння того, чому фішингові атаки працюють, неможливе без звернення до фундаментальних теорій впливу на поведінку людини. Найбільш системною та операційно придатною для аналізу фішингу є концепція американського соціального психолога Роберта Чалдіні, викладена у його класичній праці *Influence: The Psychology of Persuasion*. Чалдіні виокремив шість універсальних принципів впливу.

Принцип авторитету полягає в тому, що люди схильні підкорятися особам, яких вони вважають компетентними чи наділеними владою. Саме тому фішингові листи так часто імітують повідомлення від банків, податкових органів, керівництва компаній. Люди не перевіряють, хто їм насправді пише, не через неухважність, а тому що автоматично більше довіряють повідомленням від «авторитетних» або знайомих джерел і менше їх перевіряють.

Принцип дефіциту та терміновості є, мабуть, найбільш експлуатованим у фішингу. Повідомлення на кшталт «Ваш рахунок буде заблоковано протягом 24 годин» або «Термінова вимога безпеки» активують у людини стан психологічного стресу, який різко знижує здатність до критичного мислення. Дослідження Епштейна та Пацифічі показали, що в умовах штучно створеної терміновості люди приймають рішення переважно на основі емоцій— і саме цей стан є ідеальним для зловмисника.

Принцип соціального доказу реалізується через посилення на те, що «інші вже зробили» певну дію. У фішингу це виражається у формулюваннях типу «Тисячі наших клієнтів вже оновили свої дані» або у підробці відгуків та рекомендацій у соцмережах.

Принцип прихильності та симпатії лежить в основі спір-фішингу та ВЕС-атак. Зловмисник попередньо вивчає жертву, встановлює контакт, демонструє спільні інтереси або вдає знайомого — і лише після формування довіри переходить

до маніпуляції. Це принципово відрізняє сучасний цільовий фішинг від масових розсилок 2000-х років.

Принцип взаємності використовується у так званих «подарункових» фішингових кампаніях, де жертві спочатку пропонують щось безкоштовне — купон, доступ до ексклюзивного контенту, грошовий приз — а потім просять «лише підтвердити» свої дані.

Принцип послідовності та зобов'язань реалізується у багатоетапних атаках, де жертва спочатку погоджується на невелике прохання, що поступово підводить до розкриття критичних даних. Чалдіні пояснював це тим, що людська психіка прагне зберігати внутрішню узгодженість між послідовними рішеннями.

Паралельно з концепцією Чалдіні важливу роль у поясненні вразливості до фішингу відіграє теорія подвійної обробки інформації нобелівського лауреата Даніеля Канемана, викладена у праці *Thinking, Fast and Slow*. Канеман розрізняв два режими мислення: Систему 1 — швидку, автоматичну, емоційну — та Систему 2 — повільну, аналітичну, вимагаючу зусиль. Фішинг конструюється таким чином, щоб змусити жертву залишатися в режимі Системи 1: терміновість, страх, авторитет — усі ці тригери не дають активуватися критичному мисленню. Ця теоретична рамка пояснює, чому навіть технічно грамотні люди стають жертвами фішингу: в умовах стресу або відволікання навіть добре натренована Система 2 може «засинати».

Жодна країна у сучасному світі не є настільки показовим полігоном для дослідження соціальної інженерії у контексті кібервійни, як Україна. Починаючи щонайменше з 2014 року і з різким загостренням після повномасштабного вторгнення Росії у лютому 2022 року, Україна перебуває під безперервним тиском державно спонсорованих фішингових кампаній, що здійснюються переважно угрупованнями, пов'язаними з ГРУ та ФСБ РФ — зокрема, APT28 (Fancy Bear), APT29 (Cozy Bear) та Sandworm.

За даними Урядової команди реагування на комп'ютерні надзвичайні події України — CERT-UA — лише протягом 2022 року було зафіксовано понад 2 194 кіберінциденти, з яких фішингові атаки склали понад 60% від усіх

задокументованих векторів початкового проникнення. У 2023 році CERT-UA зафіксував збільшення кількості фішингових кампаній проти державних органів на 32% порівняно з попереднім роком.

Звіт Microsoft *Digital Defense Report 2023* окремо виділив Україну як країну з найвищою інтенсивністю державно спонсорованих кібератак у світі: російські угруповання здійснили проти України більше атак, ніж проти решти країн світу разом узятих у відповідний період. При цьому соціальна інженерія залишалася домінуючим вектором: за даними Microsoft, понад 74% атак проти українських організацій починалися саме з фішингового листа або підробленої сторінки автентифікації.

Особливої уваги заслуговує специфіка соціально-інженерних прийомів, застосованих проти України. Зловмисники активно використовували контекст війни для підвищення правдоподібності атак: фішингові листи імітували повідомлення від Збройних Сил України, Міністерства оборони, Червоного Хреста, міжнародних донорів та гуманітарних організацій. За даними CERT-UA, кампанія групи UAC-0010 у 2022–2023 роках використовувала теми виплати грошової допомоги вимушеним переселенцям як приманку для збору облікових даних державних службовців. Це є класичним застосуванням принципу Чалдіні щодо авторитету та терміновості в умовах гострої соціальної кризи.

Водночас досвід України демонструє і позитивний аспект: попри колосальний тиск, значну частину атак вдалося нейтралізувати завдяки оперативній роботі CERT-UA, партнерству з Microsoft, Google та іншими технологічними компаніями. Це свідчить про те, що навіть в умовах активної кібервійни поєднання технічних заходів із підвищенням людської пильності здатне суттєво знизити ефективність соціально-інженерних атак.

Критично оцінюючи ефективність соціальної інженерії загалом, слід зазначити таке: її результативність не є константою — вона прямо залежить від рівня підготовки потенційних жертв. Дослідження компанії Proofpoint показали, що організації, які регулярно проводять симуляції фішингових атак та навчання персоналу, демонструють зниження рівня кліків на фішингові посилання з середніх

32% до менш ніж 5% після 12 місяців систематичного навчання. Це принципово важливий висновок: він показує, що людський фактор є не фатальною вразливістю, а змінною величиною, яку можна цілеспрямовано покращувати.

1.4. Методологічні підходи до виявлення та протидії фішинговим атакам

Історично першими інструментами протидії фішингу стали методи, що базуються на реактивному принципі — тобто на реагуванні на вже відомі загрози, а не на випередженні нових. Два найбільш поширені класичні підходи — чорні списки та евристичний аналіз — принципово відрізняються за своєю природою і потребують окремого розгляду, оскільки саме їхні обмеження обґрунтовують необхідність переходу до сучасніших методів.

Чорні списки є найпростішим і найбільш поширеним механізмом захисту від фішингу. Їхня логіка проста: якщо певний URL, домен або IP-адреса були ідентифіковані як шкідливі, вони вносяться до бази даних, яка використовується браузерами, поштовими клієнтами та антивірусним програмним забезпеченням для блокування. Найбільш відомими публічними реєстрами такого типу є Google Safe Browsing, PhishTank та OpenPhish, що разом охоплюють мільйони записів.

Проте фундаментальна проблема чорних списків полягає в їхній оновлюваності: щоб потрапити до списку, фішинговий ресурс спочатку має бути виявлений і задокументований — а значить, він уже завдав шкоди принаймні частині жертв. Дослідження Шена та колег показало, що середній час між появою фішингового сайту та його внесенням до чорного списку складає від кількох годин до кількох діб, протягом яких ресурс залишається активним і небезпечним. Крім того, зловмисники давно навчилися обходити чорні списки шляхом швидкої ротації доменів — так звана техніка «fast flux» дозволяє змінювати IP-адресу

шкідливого ресурсу кожні кілька хвилин, що робить його фактично невидимим для реєстрів.

Евристичний аналіз є принципово іншим підходом. Замість порівняння з базою відомих загроз евристичні методи аналізують характеристики URL, вмісту сторінки або листа і оцінюють їхню підозрілість на основі заздалегідь визначених правил. Типові евристичні ознаки фішингового ресурсу включають: наявність IP-адреси замість доменного імені в URL, використання схожих, але не ідентичних назв брендів, невідповідність між текстом посилання та фактичним URL, а також нещодавню реєстрацію домену.

Перевагою евристики є здатність виявляти раніше невідомі загрози — на відміну від чорних списків. Проте вона має системний недолік — труднощі у балансуванні між виявленням усіх випадків і уникненням помилкових спрацювань. Жорсткі правила дають велику кількість хибних спрацювань, блокуючи легітимні ресурси; м'які правила, навпаки, пропускають реальні загрози. Цей компроміс є принципово нерозв'язним у рамках суто евристичного підходу і вимагає якісно іншого інструментарію.

Обробка природної мови для аналізу тексту листів відкриває якісно новий вимір захисту. NLP-моделі здатні аналізувати семантику, тональність та стилістику електронних листів, виявляючи маніпулятивні патерни — штучну терміновість, тиск. Це принципово важливо для протидії ВЕС-атакам, де зловмисник може використовувати реальний корпоративний домен, скомпрометований на попередньому етапі.

Поведінковий аналіз та anomaly detection є найбільш перспективним напрямом для виявлення складних цільових атак. Замість аналізу окремих повідомлень ці методи будують базову модель поведінки користувача або системи і виявляють відхилення від неї. Наприклад, якщо співробітник, який ніколи не надсилав фінансових документів о третій годині ночі, раптом починає це робити — система виявляє збій незалежно від того, чи містить конкретне повідомлення будь-які відомі ознаки фішингу.

Узагальнення результатів наукових досліджень щодо ефективності різних методів виявлення фішингу наведено у таблиці нижче.

Таблиця 1.3 — Порівняння методів виявлення фішингових атак за ефективністю

Метод	Точність виявлення	Хибно позитивний рівень	Швидкість реакції	Адаптивність	Особливі обмеження
Чорні списки	6 5–75%	Низький	Низька	Відсутня	Реактивність, обхід через fast flux
Евристичний аналіз	7 8–85%	Середній — високий	Висока	Низька	Баланс чутливості та специфічності
Random Forest / SVM	9 5–98%	Низький	Висока	Середня	Потребує якісних навчальних даних
NLP-аналіз тексту	9 2–96%	Низький	Висока	Висока	Обмежена ефективність проти голосових атак
Пов'язаний аналіз	8 5–90%	Дуже низький	Середня	Висока	Потребує тривалого базового навчання
Комбіновані AI-системи	9 7–99%	Мінімальний	Висока	Висока	Висока обчислювальна складність

Проведене дослідження підходів до виявлення та протидії фішинговим атакам дає підстави стверджувати, що традиційні методи, такі як чорні списки та евристичний аналіз, уже не забезпечують достатнього рівня захисту через їхню обмежену здатність адаптуватися до нових загроз. Водночас застосування методів машинного навчання, обробки природної мови та поведінкового аналізу демонструє вищу ефективність, проте жоден із цих підходів окремо не є достатнім.

Дослідницьке питання 1. Якою мірою сучасні технічні методи виявлення фішингу є достатніми за умови, що первинним вектором атаки залишається людський фактор, а не технічна вразливість? Це питання є центральним для Розділу 2, де буде проведено порівняльний аналіз інцидентів та ефективності застосованих засобів захисту.

Дослідницьке питання 2. Яка комбінація технічних та організаційно-правових заходів протидії фішингу є найбільш ефективною в умовах активного кіберпротистояння на прикладі України? Це питання пов'язує теоретичний аналіз із практичним контекстом і є особливо актуальним з огляду на задокументований досвід кіберзахисту України в умовах повномасштабної російської агресії.

Дослідницьке питання 3. Наскільки існуючі класифікаційні моделі фішингових атак відповідають реальному ландшафту загроз і чи потребують вони концептуального оновлення? Питання має як теоретичне значення — для розвитку понятійного апарату галузі, — так і практичне, оскільки від точності класифікації загроз залежить вибір засобів протидії.

РОЗДІЛ 2. АНАЛІЗ ФІШИНГОВИХ АТАК ТА ІНТЕРНЕТ-ШАХРАЙСТВА

2.1. Фактологічне підтвердження поширеності фішингових атак

Для забезпечення достовірності та порівнянності даних аналіз у цьому підрозділі охоплює період з 2020 по 2025 рік. Вибір саме цього діапазону є обґрунтованим: він включає довоєнний базовий період, пандемію COVID-19, та повномасштабне російське вторгнення в Україну як окремий геополітичний фактор, що кардинально змінив ландшафт кіберзагроз. Основними джерелами даних є щорічні звіти Verizon Data Breach Investigations Report, IBM Security Cost of a Data Breach Report, APWG Phishing Activity Trends Report, ENISA Threat Landscape, а також відкриті звіти Урядової команди реагування на комп'ютерні надзвичайні події України — CERT-UA.

Глобальні статистика даних щодо фішингових атак за останні роки свідчать про зростання масштабів цифрового шахрайства. За даними APWG, у 2020 році було зафіксовано близько 266 тисяч унікальних фішингових сайтів щоквартально.

Пандемія COVID-19 сприяла суттєвому зростанню кіберзлочинності. Масовий і непередбачуваний перехід на дистанційну роботу створив ідеальні умови для зловмисників: мільйони людей раптово опинилися за межами корпоративної безпеки, використовуючи домашні мережі для доступу до корпоративних ресурсів. За даними Google, лише у квітні 2020 року його системи щоденно блокували понад 18 мільйонів фішингових листів, пов'язаних із тематикою COVID-19 — на додаток до 240 мільйонів спам-повідомлень на ту саму тему. Interpol у своєму звіті *Cybercrime: COVID-19* зафіксував зростання кількості фішингових атак у першому півріччі 2020 року на 569% порівняно з минулим роком.

Після пандемічного стрибка темпи зростання сповільнилися, проте абсолютні показники залишилися на вищому рівні порівняно з довоєнним та допандемічним періодом. За даними Verizon DBIR 2024, фішинг присутній у 36%

усіх зафіксованих витоків даних у світі — і цей показник залишається стабільно високим протягом останніх трьох років. IBM Security у звіті Cost of a Data Breach 2023 зафіксував, що середня вартість одного витоку даних, досягла 4,76 мільйона доларів — що на 15% перевищує середню вартість злочинів, спричинених іншими векторами атак.

За даними ФБР, загальні фінансові збитки від інтернет-шахрайства у США у 2024 році склали 12,5 мільярда доларів — що є рекордним показником за всю історію спостережень і перевищує збитки від усіх разом узятих у цифровому середовищі. Для порівняння: у 2020 році цей показник становив 3,5 мільярда доларів, тобто за п'ять років збитки зросли у 3,6 рази. Якщо порівняти то 12,5 мільярда доларів — це більше, ніж річний ВВП понад 50 країн світу, і приблизно вдвічі більше за річний бюджет Інтерполу, помножений на тисячу.

Динаміка зростання фішингових атак за період 2020–2025 років наочно демонструє не просто збільшення загроз, а її якісну трансформацію.

Після нормалізації у 2021 році абсолютні показники так і не повернулися до допандемічного рівня — це свідчить про те, що частина зростання є структурною. Українська динаміка демонструє якісно іншу траєкторію: різке зростання у 2022 році є прямим наслідком повномасштабного вторгнення, і на відміну від глобальної тенденції, в Україні зростання не сповільнюється, а продовжується. Частка фішингу серед усіх кіберінцидентів в Україні стабільно зростає — з 38% у 2020 до 65% у 2025 році — що свідчить про те, що соціальна інженерія стає дедалі більш домінуючим вектором атак.

2.2. Інформаційно-аналітичний аналіз типів та факторів фішингових атак

Сучасний ландшафт фішингових атак є значно різноманітнішим, ніж вважають. Більшість людей асоціює фішинг виключно з підозрілими електронними

листами — проте реальна картина охоплює сім принципово різних типів атак, кожен із яких має власну цільову групу та психологічний механізм впливу. Розуміння цього різноманіття є необхідною передумовою для побудови ефективної системи протидії.

За даними звітів APWG, Verizon DBIR та за 2022–2025 роки, розподіл типів фішингових атак за частотою виглядає таким чином.

Email-фішинг залишається домінуючим типом атак із часткою близько 72% від усіх зафіксованих злочинів. Спір-фішинг, незважаючи на меншу частоту — близько 8% — є непропорційно небезпечним: за даними Verizon, через нього понад 66% усіх успішних зломів корпоративних мереж.

Смішинг демонструє стрімке зростання серед усіх типів — його частка зросла з 5% у 2020 році до 15% у 2025 році, що безпосередньо пов'язано з масовим поширенням смартфонів та зростанням довіри користувачів до SMS каналу комунікації від банків та державних органів. Вішинг займає близько 7% інцидентів, проте з появою технологій клонування голосу на основі штучного інтелекту його ефективність зросла. ВЕС-атаки становлять лише 2% за кількістю, але є найбільш фінансово збитковими — середні втрати від одного успішного ВЕС-інциденту перевищують 125 тисяч доларів. Порівняльна характеристика типів фішингових атак наведена у таблиці.

Таблиця 2.2 — Типи фішингових атак та їх характеристика

Тип атаки	Частка, %	Динаміка	Цільова аудиторія	Персоналізація	Основна мета
Email-фішинг	72%	+3% до 2023	Масова	Низька-середня	Крадіжка даних, доступ до акаунтів
Смішинг	15%	+10% до 2019	Масова	Низька	Фінансове шахрайство, крадіжка OTP
Спір-фішинг	8%	+2% до 2023	Цільова	Висока	Корпоративний злом, шпигунство

ішинг	В	7	+4	Масо	Серед	Фінан
	%		% до 2023	ва/цільова	ня	совий обман, збір даних
ЕС	В	2	Ст	Ультр	Дуже	Фінан
	%		абільна	ацільова	висока	сові перекази, шахрайство
армінг	Ф	1	-	Масо	Висок	Краді
	,5%		0,5% до 2023	ва	а	жка облікових даних
лон-фішинг	К	1	Ст	Цільо	Висок	Досту
	%		абільна	ва	а	п до корпоративних систем
R-фішинг	Q	0	Но	Масо	Серед	Краді
	,5%		вий тип	ва	ня	жка даних, шкідливе ПЗ

Джерела: APWG Phishing Activity Trends Report 2024; Proofpoint State of the Phish 2024; Verizon DBIR 2024.

Діаграма Парето є потужним інструментом, що дозволяє виявити «критичну меншість» факторів, які відповідають за переважну більшість наслідків. Результати аналізу є переконливими: лише три фактори з восьми — недостатня кіберобізнаність, емоційний тиск і відсутність технічного захисту. Разом відповідають за 70% усіх успішних фішингових атак. Якщо додати четвертий фактор — слабку автентифікацію — частка сягає 83%, що повністю підтверджує принцип Парето. Іншими словами, суттєве послаблення лише чотирьох ключових факторів здатне нейтралізувати більш ніж 80% усіх успішних атак.

Таблиця 2.3 — Ранжування факторів успішності фішингових атак (діаграма Парето)

	Фа	Кат	Ч	Н	П	Зах
ктор	егорія	астка, %	акопичена частка	ріоритет усунення	ід протидії	

	Недостатня кіберобізнаність	Організаційний	0%	3	30%	Висока	Навчання персоналу
	Емоційний тиск / терміновість	Психологічний	2%	2	52%	Дуже висока	Антифішинг-тренінги
	Відсутність технічного захисту	Технічний	8%	1	70%	Висока	Впровадження фільтрів
	Слабка автентифікація	Технічний	3%	1	83%	Висока	MF A, FIDO2
	Висока персоналізація атаки	Технічний	%	7	90%	Середня	OSI NT-моніторинг
	Довіра до бренду / імітація	Психологічний	%	5	95%	Середня	Перевірка відправника
	Атак у позаробочий час	Організаційний	%	3	98%	Низька	Моніторинг 24/7
	Використання нових каналів	Технічний	%	2	100%	Низька	Блокування каналів

Джерела: IBM Security Cost of a Data Breach 2023; Proofpoint State of the Phish 2024; Verizon DBIR 2024.

Якщо у попередніх підрозділах соціальна інженерія розглядалася через призму психологічних теорій, то тут важливо перевести цей вплив у конкретні кількісні показники. За даними Proofpoint State of the Phish 2025, атаки з частками соціальної інженерії є в середньому у 4,7 рази ефективнішими за технічні атаки без психологічного впливу. При цьому ефективність різних принципів Чалдіні у фішингових атаках розподіляється нерівномірно: принцип авторитету використовується у 68% атак і є найбільш поширеним; принцип терміновості застосовується у 62% випадків; принцип страху — у 51%. Натомість принцип взаємності, попри свою особливість, зустрічається лише у 23% атак, оскільки вимагає складнішої підготовки.

Масові нецільові розсилки мають середній рівень успішності 3–5%. Атаки з частковою персоналізацією — використанням імені жертви або назви її організації — демонструють успішність 19–23%. Повністю персоналізований спір-фішинг із детальним вивченням жертви через OSINT досягає рівня успішності 45–65%. Це наочно ілюструє, чому зловмисники дедалі частіше обирають цільові атаки.

Таблиця 2.4 — Порівняльна характеристика типів фішингових атак

Тип атаки	Успішність	Технічна складність	Персоналізація	Час підготовки	Середні збитки	Рівень небезпеки
mail-фішинг	3–5%	Низька	Низька	Година	\$500	Низький
мішинг	5–8%	Низька	Низька	Година	\$300	Середній
спір-фішинг	45–65%	Висока	Висока	Тижні	\$2 000	Дуже високий
ішінг	15–25%	Середня	Середня	Дні	\$800	Середній
ЕС	55–70%	Дуже висока	Дуже висока	Місяці	\$10 000+	Критичний
армінг	8–12%	Висока	Низька	Дні	\$3 000	Середній
лон-фішинг	20–35%	Висока	Середня	Дні	\$1 500	Високий
R-фішинг	10–18%	Середня	Низька	Дні	\$400	Зростаючий

Джерела: ENISA Threat Landscape 2023; Proofpoint State of the Phish 2024; Verizon DBIR 2024; FBI IC3 Report 2023.

Встановлено, що основна частина успішних інцидентів представлена обмеженим набором переважно психологічних та організаційних факторів. Рівень атаки є ключовим чинником її ефективності, оскільки сценарії значно підвищують ймовірність успіху. Також відзначається стрімке зростання смішингу як окремого типу загроз, що потребує врахування при формуванні підходів до захисту користувача в мережі Інтернету.

2.3. Порівняльний аналіз сучасних інформаційних технологій виявлення фішингу

Для забезпечення правильності та об'єктивності порівняння всі п'ять методів виявлення фішингу оцінюються за єдиним набором із семи параметрів: точність виявлення, рівень хибних спрацьовувань, швидкість реакції, адаптивність до нових загроз, вартість впровадження, вимоги до даних та інтегральний коефіцієнт ефективності. Останній є мої власним авторським показником, що розраховується як зважене середнє трьох ключових параметрів за формулою:

$$K_e = 0,5 \times T + 0,3 \times A + 0,2 \times Ш$$

де T — нормалізована точність виявлення, A — адаптивність до нових загроз, $Ш$ — швидкість реакції за шкалою від 1 до 10. Ваги обрані відповідно до пріоритетності параметрів: точність є найкритичнішою характеристикою, адаптивність визначає довгострокову ефективність, швидкість впливає на оперативність реагування.

Основою для кількісних оцінок є дані звітів ENISA Threat Landscape 2023, NIST Cybersecurity Framework. Чорні та білі списки є найстарішим і найбільш поширеним методом захисту від фішингу. Простота реалізації та низька обчислювальна вартість зробили цей метод стандартним компонентом практично будь-якого захисного рішення.

Проте саме ця простота є одночасно головним обмеженням методу. Чорні списки є принципово реактивними: ресурс може потрапити до списку лише після того, як він уже був виявлений і задокументований як шкідливий. За даними APWG, середній час між появою фішингового сайту та його внесенням до основних чорних списків становить від 4 до 48 годин. Додатковою проблемою є техніка fast

flux, що дозволяє зловмисникам змінювати IP-адреси шкідливих ресурсів кожні кілька хвилин, фактично роблячи їх невидимими для статичних списків.

Кількісна оцінка методу демонструє його системну слабкість: точність виявлення знаходиться на рівні 6,5 балів із 10, адаптивність до нових загроз — лише 2 бали, швидкість реакції — 3 бали.

Інтегральний коефіцієнт ефективності становить $K_e = 4,45$, що є найнижчим показником серед усіх розглянутих методів. Цей результат підтверджує те, що практики кібербезпеки знають фактично: чорні списки можуть виконувати роль першого рубежу захисту, але не здатні бути основою сучасної системи протидії фішингу.

Евристичний аналіз— дозволяє виявляти потенційно шкідливі ресурси без попереднього знання про їхнє існування, спираючись на аналіз характерних ознак фішингу. Типовий евристичний аналізатор перевіряє URL на наявність підозрілих патернів, аналізує структуру HTML-сторінки, вміст форм та метадані сертифікатів, порівнює візуальне оформлення з базою відомих брендів. Це принципово зовсім інший підхід, і в цьому полягає його головна перевага.

Проте евристика має власний системний недолік — проблему балансу між чутливістю та специфічністю. Дослідження Жана та Хуанга показало, що типові евристичні системи при налаштуванні на максимальну чутливість генерують до 23% хибних спрацьовувань, що є неприйнятним практичних застосувань. Зниження чутливості усуває цю проблему, але збільшує кількість пропущених загроз. Цей компроміс є принципово нерозв'язним у рамках суто евристичного підходу — будь-яке налаштування системи є лише вибором між двома типами помилок, а не вирішенням проблеми.

Точність евристичних методів оцінюється на рівні 7,5 балів із 10, адаптивність — 5 балів, швидкість реакції — 7 балів. Інтегральний коефіцієнт ефективності становить $K_e = 6,65$, що є суттєвим покращенням порівняно з чорними списками, проте все ще недостатнім для протидії сучасним персоналізованим атакам.

Машинне навчання стало якісним стрибком у розвитку методів виявлення фішингу, переводячи аналіз із рівня заздалегідь визначених правил на рівень автоматичного виявлення прихованих закономірностей у великих масивах даних. Алгоритми Random Forest, Support Vector Machine, градієнтний підвищення та нейронні мережі навчаються на визначених наборах даних і здатні враховувати сотні ознак одночасно — від лексичних характеристик URL до мережевої поведінки ресурсу.

Практичні результати застосування є переконливими. Дослідження Абделхаміда показало, що комбіновані моделі на основі Random Forest досягають точності виявлення фішингових URL на рівні 97,4% при хибних спрацюваннях на рівні менше 1,5%. Моделі на основі глибокого навчання при аналізі контенту електронних листів демонструють точність до 98,7%. При цьому метод має перевагу перед евристикою: він не потребує ручного визначення правил і здатен підлаштуватись до нових форм атак.

Водночас машинне навчання має власні системні обмеження. Якість моделі залежить від якості та актуальності навчальних даних — застаріла дані різко знижують ефективність. Моделі є вразливими до adversarial attacks, де зловмисники цілеспрямовано модифікують фішингові ресурси, щоб обдурити класифікатор. Точність методу оцінюється на рівні 9 балів із 10, адаптивність — 7 балів, швидкість — 8 балів. Інтегральний коефіцієнт ефективності $K_e = 8,20$.

Застосування штучного інтелекту у виявленні фішингу виходить за межі класичного машинного навчання і охоплює якісно новий рівень аналізу. Великі мовні моделі здатні досліджувати не лише структурні ознаки повідомлення, але й його смисловий зміст, тональність, відповідність корпоративному стилю спілкування та середовище взаємовідносин між відправником і отримувачем.

Особливою перевагою AI-підходу є здатність виявляти BEC-атаки та складні форми спір-фішингу, які залишаються невидимими для всіх попередніх методів. Якщо зловмисник використовує не справжній легітимний обліковий запис і веде реалістичне листування з жертвою протягом кількох тижнів — жоден чорний список, евристика чи навіть класичний класифікатор машинного навчання не

виявить загрози. Натомість LLM-система здатна помітити тонкі аномалії у стилі написання, незвичні запити або відхилення від типових патернів спілкування.

Дослідницька група Microsoft у звіті Cyber Signals 2023 зафіксувала, що AI-системи виявляють до 87% інцидентів, що залишаються невидимими для традиційних методів. Точність AI-методів оцінюється на рівні 9,5 балів із 10, адаптивність — 9 балів, швидкість — 8,5 балів. Інтегральний коефіцієнт ефективності $K_e = 9,15$ є найвищим серед усіх розглянутих методів. Проте цей метод має і найвищу вартість впровадження та експлуатації.

Поведінковий аналіз є принципово відрізняється від усіх попередніх методів за своєю структурою: замість аналізу характеристик конкретного повідомлення або ресурсу він будує модель нормальної поведінки користувача чи системи і виявляє відхилення від цієї норми. Такий підхід є особливо ефективним у контексті інсайдерських загроз.

Практична реалізація поведінкового аналізу охоплює моніторинг патернів входу в систему, аналіз часових вікон активності, локації користувача, типів пристроїв. Якщо співробітник, який зазвичай працює з Києва у робочий час, раптом входить у систему о третій годині ночі з незнайомого пристрою і починає масово завантажувати файли — система негайно фіксує аномалію.

Головним обмеженням методу є тривале початкове навчання для побудови базової моделі поведінки — як правило, від двох до чотирьох тижнів. Метод є менш ефективним щодо нових користувачів або у ситуаціях, коли зловмисник діє повільно та обережно. Точність поведінкового аналізу оцінюється на рівні 8,5 балів із 10, адаптивність — 8 балів, швидкість — 6 балів. Інтегральний коефіцієнт ефективності $K_e = 7,85$ відображає сильну позицію методу, що поступається лише AI-підходу та машинному навчанню.

Порівняння п'яти методів виявлення фішингу демонструє чітку ієрархію їх ефективності: найвищі значення інтегрального коефіцієнта мають AI-методи ($K_e=9,15$), далі машинне навчання ($K_e=8,20$), поведінковий аналіз ($K_e=7,85$), евристичні підходи ($K_e=6,65$), а найнижчі показники у чорного списку ($K_e=4,45$).

Жоден із розглянутих методів не є повністю універсальним, оскільки навіть найефективніші AI-рішення мають суттєві обмеження, як мають високу вартість та обмежену відкритість доступу для більшості організацій.

Розглянуті підходи не змагаються між собою, а доповнюють один одного: чорні списки забезпечують оперативне блокування відомих загроз, евристичні методи виявляють нові ресурси, машинне навчання підвищує точність класифікації, AI аналізує семантичний зміст, а поведінковий аналіз фіксує аномалії.

РОЗДІЛ 3. РОЗРОБЛЕННЯ ТА ОБҐРУНТУВАННЯ ЗАХОДІВ ЩОДО ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ВИЯВЛЕННЯ ТА ПРОТИДІЇ ФІШИНГОВИМ АТАКАМ

3.1. Формування комплексного підходу до протидії фішинговим атакам

Формування ефективної системи протидії фішинговим атакам неможливе без чіткого визначення методологічних принципів. Аналіз, проведений у попередніх розділах, переконливо показав, що жоден окремий метод захисту не є достатнім — а отже, система має бути комплексною за своєю природою. На основі загальної наукової літератури та результатів власного дослідження пропонується сім базових принципів.

Принцип багаторівневості передбачає, що захист організовується на кількох незалежних рівнях, щоб подолання одного рівня не означало автоматичного успіху атаки. Це відповідає концепції *defense-in-depth*, яка є загальновизнаним стандартом у сфері інформаційної безпеки. Якщо злоумисник обходить технічний фільтр — його зупиняє обізнаний користувач; якщо маніпуляція вдається — спрацьовує поведінковий моніторинг.

Принцип інтеграції вимагає, щоб технічні, організаційні та правові заходи функціонували не паралельно, а у взаємозв'язку, утворюючи єдину екосистему захисту. Роз'єднані заходи, навіть якісні самі по собі, залишають недоліки, якими неминуче скористаються злоумисники.

Принцип адаптивності є відповіддю на динамічний характер фішингових загроз. Система захисту не може бути сталою — вона має постійно оновлюватися відповідно до нових векторів атак, нових технологій і нових вразливостей. Це означає не лише технічне оновлення, але й регулярний перегляд організаційних процедур та навчальних програм.

Принцип людиноцентричності є, мабуть, найбільш недооціненим у практиці кібербезпеки. Оскільки людський фактор є першочерговою вразливістю у понад 95% інцидентів, система захисту має бути спроектована насамперед навколо людини — її когнітивних обмежень, поведінкових патернів та потреб у навчанні, а не лише навколо технічної інфраструктури.

Принцип пропорційності вимагає, щоб заходи захисту відповідали ризику. Надмірний захист є так само шкідливим, як і недостатній: він створює операційні незручності, знижує продуктивність і призводить до так званої втоми від безпеки, за якої користувачі починають обходити захисні механізми.

Принцип безперервності моніторингу передбачає, що система захисту функціонує в режимі реального часу без розривів у покритті. Більшість успішних атак відбуваються саме у вікнах вразливості — у позаробочий час.

Принцип документування та звітності забезпечує зворотній зв'язок у системі: кожен інцидент має бути зафіксований, проаналізований і використаний для вдосконалення захисту. Без цього принципу система позбавлена механізму самовдосконалення.

Традиційний підхід до кібербезпеки розглядав технічні та організаційні заходи як окремі домени відповідальності — перші належали ІТ-відділу, другі — службі безпеки. Сучасна практика демонструє хибність такого поділу: найсучасніші технічні рішення залишаються неефективними без відповідної організаційної культури безпеки, і навпаки.

Інтеграція двох вимірів захисту реалізується через кілька механізмів. Через єдину політику безпеки, що охоплює як технічні вимоги, так і поведінкові стандарти для всіх категорій користувачів. Наступна причина через спільні процедури реагування на інциденти, де технічні фахівці та менеджери діють за єдиним алгоритмом. Ще одна з причин через інтегровані програми навчання, що поєднують теоретичну підготовку з практичними симуляціями фішингових атак — такий підхід, за даними Proofpoint, знижує рівень успішних атак з 32% до менш ніж 5% протягом року.

Центральним результатом цього підрозділу є багаторівнева модель протидії фішинговим атакам, що складається з п'яти взаємопов'язаних рівнів захисту. Кожен рівень виконує специфічну функцію і одночасно є резервним захистом для попереднього.

Перший рівень — периметровий технічний захист — є першою лінією оборони і включає поштові фільтри з AI-аналізом, системи перевірки репутації URL, DNS-фільтрацію. Цей рівень блокує масові фішингові кампанії ще до того, як вони досягають користувача.

Другий рівень — автентифікація та контроль доступу — забезпечує, що навіть у разі зламу облікових даних злоумисник не зможе отримати доступ до системи. Основним інструментом є багатофакторна автентифікація, що є стійкими до фішингу за своєю природою. Цей рівень є критично важливим, оскільки він перериває ланцюг атаки.

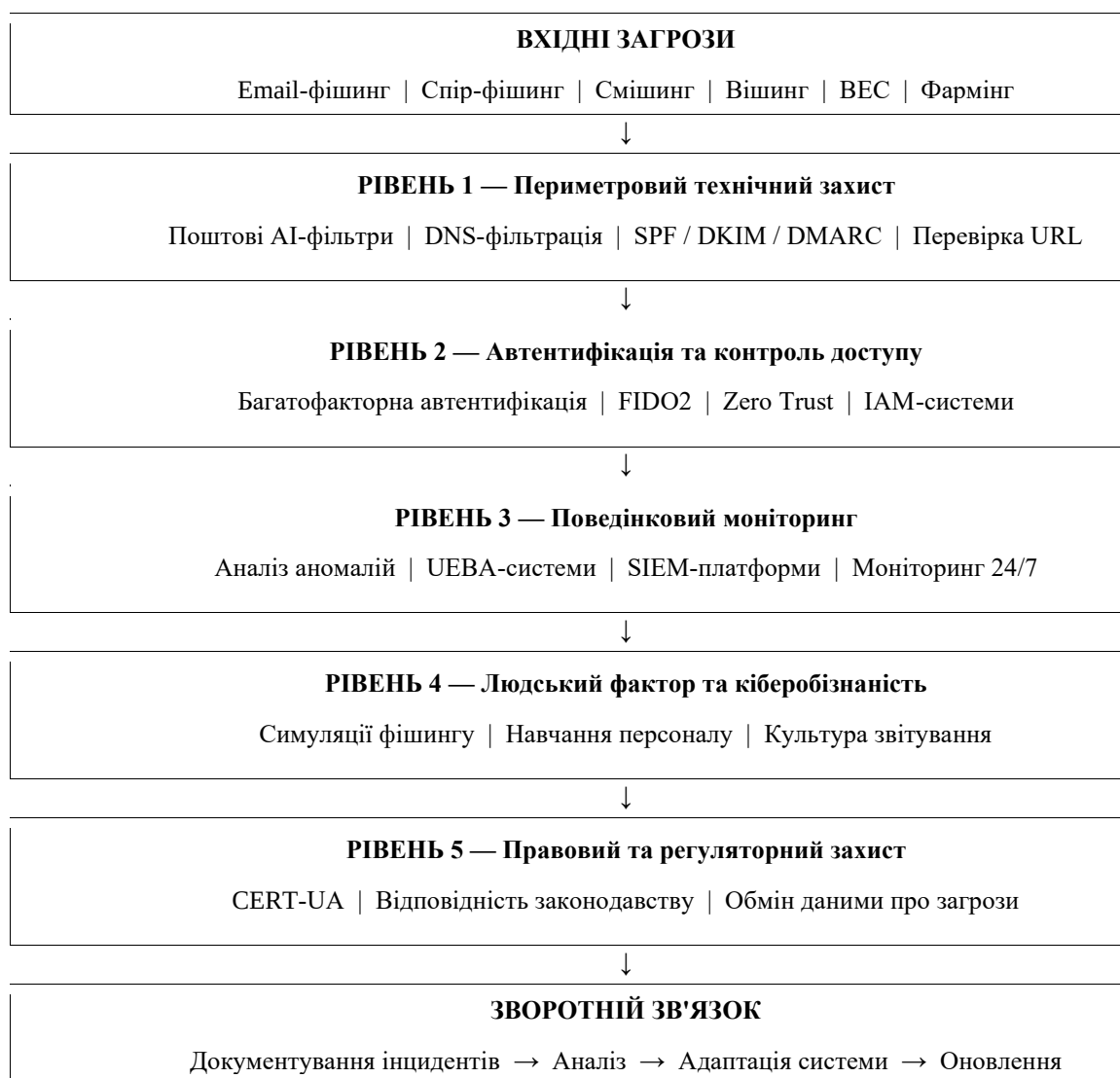
Третій рівень — поведінковий моніторинг та аналіз аномалій — функціонує як система раннього виявлення, що вивчає патерни поведінки користувачів і систем у реальному часі. Відхилення від базової моделі поведінки автоматично створюють сповіщення та запускають перевірку навіть за відсутності технічних ознак атаки.

Четвертий рівень — людський фактор і кіберобізнаність — є найбільш недооціненим і водночас найбільш ефективним рівнем захисту. Він включає регулярні симуляції фішингових атак, особисте навчання на основі результатів симуляцій, формування культури звітування про підозрілі повідомлення та розвиток критичного мислення щодо цифрових комунікацій.

П'ятий рівень — правовий та регуляторний захист — забезпечує зовнішнє середовище для функціонування системи.

Структурну схему запропонованої моделі наведено на рисунку.

Рисунок 3.1 — Багаторівнева модель протидії фішинговим атакам



Ефективність багаторівневої моделі залежить не лише від якості її окремих компонентів, а й від того, наскільки злагоджено вони взаємодіють між собою. Запропонований алгоритм працює циклічно та складається з чотирьох етапів.

Фаза виявлення — усі рівні системи паралельно моніторять вхідні сигнали у режимі реального часу. Виявлення підозрілої активності на будь-якому рівні автоматично запускає перевірку на всіх інших рівнях.

Фаза аналізу — підозрілий об'єкт або поведінка аналізуються комплексно: технічні характеристики перевіряються системами першого рівня, контекст поведінки — третім рівнем, відповідність регуляторним вимогам — п'ятим.

Фаза реагування — залежно від результатів аналізу система автоматично обирає одну з трьох реакцій: блокування з повідомленням користувача, карантин із запитом підтвердження або ескалація до фахівця з безпеки.

Фаза адаптації — кожен задокументований інцидент збагачує навчальні вибірки систем машинного навчання, оновлює бази поведінкових патернів і генерує матеріали для наступного циклу навчання персоналу.

Розроблений комплексний підхід до протидії фішинговим атакам показав, що ефективний захист має ґрунтуватися на поєднанні кількох взаємопов'язаних принципів і використовувати багаторівневу систему безпеки. Запропонована модель забезпечує резервування захисту, оскільки подолання одного рівня не призводить до успіху атаки. Циклічна взаємодія елементів системи дає змогу постійно вдосконалювати її на основі отриманого досвіду. Водночас ключову роль у протидії фішингу відіграє підвищення рівня кіберобізнаності користувачів.

3.2. Розроблення моделі оцінювання ризику фішингових атак

Оцінювання ризику фішингових атак є необхідною передумовою для раціонального розподілу ресурсів захисту: організація, яка не вимірює свій рівень ризику, не може обґрунтовано визначити, де саме потрібні першочергові інвестиції у безпеку. Запропонована модель базується на поєднанні бального методу, вагових коефіцієнтів та експертних оцінок, що забезпечує як математичну строгість, так і гнучкість у врахуванні особливостей конкретної організації.

Вагові коефіцієнти факторів визначено методом попарного порівняння, де кожен фактор порівнюється з кожним іншим. Цей метод є стандартним у теорії прийняття рішень і забезпечує внутрішню узгодженість системи ваг. Загальна сума

вагових коефіцієнтів дорівнює 1 що дозволяє інтерпретувати результат як нормалізований індекс ризику в діапазоні від 0 до 100 балів.

Модель включає п'ять ключових факторів, кожен з яких оцінюється за шкалою від 1 до 10 балів і множиться на відповідний ваговий коефіцієнт.

Фактор 1 — Рівень підготовки користувачів є найвагомішим фактором із ваговим коефіцієнтом $W_1 = 0,30$. Це обґрунтовується результатами аналізу у підрозділі 2.2, де встановлено, що недостатня кіберобізнаність відповідає за 30% успішних атак. Оцінка фактора визначається на основі частоти проведення тренінгів, результатів симуляцій та рівня обізнаності персоналу: 1–3 бали — тренінги відсутні або проводяться рідше рази на рік; 4–6 балів — тренінги проводяться щорічно без практичних симуляцій; 7–9 балів — регулярні симуляції та навчання щоквартально; 10 балів — безперервна програма з індивідуальним навчанням.

Фактор 2 — Наявність та якість технічного захисту має ваговий коефіцієнт $W_2 = 0,25$. Він охоплює сукупність технічних засобів: наявність поштових фільтрів, DNS-фільтрації, антифішингових браузерних розширень. Оцінка від 1 до 3 балів відповідає відсутності спеціалізованих засобів захисту; від 4 до 6 — наявності базових фільтрів без AI-компоненту; від 7 до 9 — комплексному технічному захисту; 10 балів — повністю інтегрований AI-системі з поведінковим аналізом.

Фактор 3 — Наявність багатофакторної автентифікації отримує ваговий коефіцієнт $W_3 = 0,20$, що відображає його роль як критичного бар'єру, здатного знешкодити атаку навіть після успішного викрадення облікових даних. Оцінювання враховує не лише факт наявності MFA, але й тип реалізації: SMS-коди отримують нижчу оцінку через вразливість до SIM-swapping, тоді як апаратні ключі FIDO2 — максимальну.

Фактор 4 — Тип та різноманітність каналів комунікації має ваговий коефіцієнт $W_4 = 0,15$. Організації, що активно використовують електронну пошту, корпоративні месенджери, SMS та телефонний зв'язок одночасно, мають значно більшу поверхню атаки. Оцінка визначається кількістю активних каналів та рівнем їхнього захисту.

Фактор 5 — Частота фішингових інцидентів за попередній період отримує ваговий коефіцієнт $W_5 = 0,10$ як індикатор реального рівня загрози. Організації, що вже зазнавали успішних атак, мають вищий базовий рівень ризику через ймовірність повторного цілеспрямованого зловмисників.

Інтегральний індекс ризику фішингових атак розраховується за такою формулою:

$$IR = 100 - (W_1 \times S_1 + W_2 \times S_2 + W_3 \times S_3 + W_4 \times S_4 + W_5 \times S_5) \times 10$$

де IR — інтегральний індекс ризику (0–100), W — ваговий коефіцієнт фактора, S — оцінка фактора за шкалою 1–10.

Логіка формули побудована таким чином, що вищі оцінки за кожним фактором відповідають кращому стану захисту, а отже — нижчому індексу ризику. Значення IR від 0 до 25 відповідає низькому рівню ризику; від 26 до 50 — помірному; від 51 до 75 — високому; від 76 до 100 — критичному.

Для ілюстрації роботи моделі розглянемо два гіпотетичні приклади. Типова українська державна установа без систематичного навчання персоналу, з базовими поштовими фільтрами, SMS-автентифікацією, трьома активними каналами спілкування та двома інцидентами за останній рік отримує оцінки $S_1=3$, $S_2=4$, $S_3=4$, $S_4=5$, $S_5=4$, що дає

$$IR = 100 - (0,30 \times 3 + 0,25 \times 4 + 0,20 \times 4 + 0,15 \times 5 + 0,10 \times 4) \times 10 = 100 - 37 = 63$$

бали — високий рівень ризику.

Натомість сучасна фінтех-компанія з щоквартальними симуляціями, AI-захистом, апаратними ключами FIDO2 і мінімальною кількістю інцидентів отримує $IR = 100 - (0,30 \times 9 + 0,25 \times 9 + 0,20 \times 10 + 0,15 \times 7 + 0,10 \times 8) \times 10 = 100 - 87 = 13$ балів — низький рівень ризику.

Таблиця 3.1 — Фактори оцінювання ризику фішингових атак та їхні вагові коефіцієнти

№	Фактор	Вага	Шкала оцінювання (1–10)	Обґрунтування
1	Рівень підготовки користувачів	0,30	$W_1 =$ 1–3: тренінги відсутні; 4–6: щорічні без симуляцій; 7–9: щоквартальні симуляції; 10: безперервна програма	Найвагоміший фактор (30% атак)
2	Якість технічного захисту	0,25	$W_2 =$ 1–3: відсутній; 4–6: базові фільтри; 7–9: комплексний захист; 10: AI-система з поведінковим аналізом	Другий за вагомістю
3	Наявність MFA	0,20	$W_3 =$ 1–3: відсутня; 4–6: SMS-коди; 7–8: TOTP-застосунки; 9–10: апаратні ключі FIDO2	Критичний бар'єр після компрометації
4	Різноманітність каналів комунікації	0,15	$W_4 =$ 1–3: один канал без захисту; 4–6: 2–3 канали; 7–9: захищені канали; 10: повний контроль	Більше каналів = більша поверхня атаки
5	Частота інцидентів за попередній період	0,10	$W_5 =$ 1–3: понад 5 інцидентів; 4–6: 2–4 інциденти; 7–9: 1 інцидент; 10: жодного	Індикатор реального рівня загрози

3.3. Прогнозування тенденцій розвитку фішингових атак

Прогнозування у сфері кібербезпеки є принципово складнішим завданням, ніж у більшості інших галузей, оскільки об'єкт прогнозу — поведінка злоумисників — цілеспрямовано реагує на заходи протидії. Це означає, що суто статистичні

методи екстраполяції, навіть побудовані на якісних даних, дають лише часткову картину майбутнього. Саме тому в цьому підрозділі поєднуються чотири методи.

Кількісний прогноз базується моделях, побудованих у підрозділі 2.2. Нагадаємо ключові результати: для глобального ряду модель дає прогнозні значення 3,13 млн унікальних фішингових сайтів у 2026 році та 1,71 млн у 2027 році, тоді як лінійна модель прогнозує значно вищі показники — 6,55 та 7,12 млн відповідно.

Розбіжність між моделями для глобального ряду є методологічно важливою і потребує пояснення. З підвищенням ефективності автоматизованих систем виявлення та блокування, які скорочують середній час життя фішингового ресурсу. Це є принципово важливим спостереженням, зміною самої стратегії зловмисників: замість створення великої кількості примітивних фішингових сайтів сучасні атаки все частіше спираються на ресурси, що не відображається у статистиці унікальних фішингових доменів.

Таким чином, зниження прогнозного показника кількості фішингових сайтів за поліноміальною моделлю не означає зменшення загрози — воно означає її якісну трансформацію, яка не може бути повністю захоплена кількісними методами прогнозування.

Технологічний фактор є найбільш непередбачуваним у прогнозуванні фішингових атак. Аналіз поточних технологічних тенденцій дозволяє виділити п'ять ключових факторів, що визначатимуть структуру фішингових атак у найближчі роки.

Генеративний штучний інтелект є одним із найважливіших факторів змін у цій сфері. GPT-подібні моделі дозволили зловмисникам автоматично створювати добре написані та правдоподібні фішингові повідомлення у великих обсягах. Якщо раніше орфографічні помилки та незграбні формулювання були надійним індикатором фішингу, то сьогодні це практично втратило цінність. За оцінками Gartner, до 2027 року понад 60% фішингових листів будуть згенеровані або суттєво покращені за допомогою AI.

Технологія deepfake для голосу та відео вже активно використовується у вішинг-атаках та атаках типу ВЕС. Задokumentований випадок 2023 року, коли зловмисники використали клонований голос керівника для авторизації банківського переказу на суму 35 млн доларів, є хорошим прикладом того, як ця технологія модифікує традиційні схеми шахрайства. Прогнозується, що до 2026 року deepfake-атаки стануть стандартним інструментом у кіберзлочинності корпоративного рівня.

Сценарний аналіз є найбільш потужним інструментом прогнозування, оскільки він не претендує на єдиний правильний прогноз. Отже розглянемо три сценарія розвитку подій.

Песимістичний сценарій реалізується за умови, що зловмисники першими масштабно впровадять генеративний AI та deepfake-технології, тоді як рівень кіберобізнаності організацій залишиться низьким. За цього сценарію кількість успішних фішингових атак в Україні може зрости до 5 500–6 000 інцидентів на рік до 2027 року, а середній рівень успішності атак підвищиться з поточних 3–5% до 8–12% завдяки AI-персоналізації. Фінансові збитки за цим сценарієм можуть перевищити 30 млрд гривень щорічно.

Базовий сценарій відповідає прогнозу, побудованому у підрозділі 2.2. Кількість задokumentованих інцидентів в Україні стабілізується на рівні 3 500–4 000 на рік, тоді як якість атак підвищиться. Фінансові втрати збільшуватимуться відповідно до підвищення середньої вартості одного інциденту.

Оптимістичний сценарій реалізується за умови широкого впровадження passkeys та FIDO2-автентифікації, масштабних програм підвищення кіберобізнаності та посилення міжнародної співпраці у сфері протидії кіберзлочинності. За цього сценарію кількість успішних атак може знизитися на 30–40% попри зростання їхньої загальної кількості, а фінансові збитки стабілізуються або навіть знизяться завдяки зменшенню успішності атак.

Кількісні методи прогнозування свідчать про можливу стабілізацію або незначне зменшення кількості унікальних фішингових ресурсів у світі, тоді як в Україні очікується зростання зареєстрованих інцидентів до рівня 3 800–4 200

випадків на рік до 2027 року. Генеративний штучний інтелект і технології deepfake визначаються як ключові фактори змін у найближчі роки та потребують нових підходів до кіберзахисту, що виходять за межі традиційних рішень.

3.4. Оцінювання ефективності запропонованих заходів

Для забезпечення об'єктивності та повноти оцінювання застосовуються чотири взаємодоповнюючі методи: порівняльний аналіз «до» та «після», метод експертних оцінок, SWOT-аналіз запропонованого підходу та аналіз витрат і результатів.

Порівняльний аналіз базується на чотирьох ключових показниках ефективності, що були визначені як цільові на початку підрозділу: ймовірність успішних атак, фінансові втрати від інцидентів, рівень обізнаності користувачів та час виявлення інцидентів.

Ймовірність успішних фішингових атак. До впровадження запропонованого комплексу заходів типова організація з низьким рівнем захисту демонструє рівень кліків на фішингові посилання у діапазоні 28–34% — що відповідає даним Proofpoint для організацій без систематичного навчання. Після впровадження п'ятирівневої моделі захисту прогнозоване зниження цього показника становить до 3–5% — що підтверджується задокументованими результатами аналогічних програм у дослідженнях Proofpoint. Таким чином, відносне зниження ймовірності успішної атаки становить близько 85–90%.

Фінансові втрати від інцидентів. Зниження ймовірності успішних атак у поєднанні зі скороченням часу виявлення інцидентів прогнозовано знижує сукупні фінансові втрати на 60–70%. Ця оцінка є консервативною і базується на даних IBM Security, які показують, що організації з розвиненими програмами реагування на інциденти зазнають збитків у середньому на 61% менших порівняно з організаціями без таких програм.

Рівень обізнаності користувачів. Вихідний рівень обізнаності персоналу в організаціях без систематичного навчання, за даними SANS Security Awareness Report, становить у середньому 23–27 балів зі 100 за стандартизованими тестами. Після 12 місяців програми, що включає регулярні симуляції та персоналізоване навчання, цей показник зростає до 72–78 балів — тобто покращення становить близько 200%.

Час виявлення інцидентів. Середній час від початку фішингової атаки до її виявлення у організаціях без розвиненої системи моніторингу становить 197 днів за даними IBM Security Cost of a Data Breach 2023. Впровадження поведінкового аналізу та SIEM-платформ здатне скоротити цей показник до 21–30 днів, що є зниженням на 85–90% і принципово змінює можливості реагування.

На основі проведеного оцінювання ефективності формуються практичні рекомендації.

Першочергові заходи — перші 90 днів. Впровадження багатофакторної автентифікації для всіх користувачів із привілейованим доступом є найшвидшим і найдешевшим способом суттєво знизити ризик. Запуск першої симуляції фішингової атаки дозволяє отримати базовий показник вразливості персоналу для подальшого порівняння.

Середньострокові заходи — від 3 до 12 місяців. Поступове розгортання технічної інфраструктури першого рівня — поштових фільтрів, DNS-захисту та протоколів автентифікації домену. Запуск систематичної програми підвищення кіберобізнаності з щомісячними симуляціями та персоналізованим навчанням на основі їхніх результатів.

Довгострокові заходи — від 12 місяців і далі. Впровадження систем поведінкового аналізу та SIEM-платформ для третього рівня захисту. Перехід на passkeys та FIDO2-автентифікацію як стандарт для всієї організації. Встановлення партнерства з CERT-UA та участь у галузевих механізмах обміну інформацією про загрози.

Таблиця 3.3 — Порівняльний аналіз показників ефективності «до» та «після» впровадження

Показник	До впровадження	Після впровадження	Змін а	Джерело підтвердження
Ймовірність успішних атак	28–34%	3–5%	↓ на 85–90%	Proofpoint, KnowBe4
Середні фінансові збитки	\$4,76 млн / інцидент	\$1,43–1,90 млн	↓ на 60–70%	IBM Security 2023
Рівень обізнаності персоналу	23–27 / 100 балів	72–78 / 100 балів	↑ на ~200%	SANS Awareness 2023
Час виявлення інциденту	197 днів	21–30 днів	↓ на 85–90%	IBM Security 2023
Частота успішних ВЕС-атак	Висока	Низька	↓ на 70–80%	Verizon DBIR 2024

Джерело: розроблено автором на основі даних Proofpoint, IBM Security, SANS Institute, Verizon DBIR.

ВИСНОВКИ

Проведене дослідження дозволяє стверджувати, що фішинг та пов'язане інтернет-шахрайство є не просто технічною проблемою інформаційної безпеки, а складним соціально-технічним феноменом, адекватне розуміння якого вимагає дисциплінарного підходу, що поєднує психологію, інформаційні технології та правознавство. Саме ця багатовимірність явища зумовила логіку та структуру цієї роботи.

Критичний огляд наукової літератури виявив суттєву фрагментованість понятійного апарату у сфері інтернет-шахрайства: правові, технічні підходи розглядають одне й те саме явище крізь принципово різні системи координат, що ускладнює як академічне дослідження, так і практичну протидію. Це спостереження стало основою для власного визначення фішингу як навмисного обману в цифровому середовищі, коли зловмисник видає себе за справжнього відправника, щоб незаконно отримати конфіденційні дані або гроші. На відміну від більшості існуючих визначень, які зосереджуються лише на технічному або правовому аспекті, запропоноване формулювання охоплює всі ключові сторони явища та може слугувати основою для подальших досліджень.

Звернення до психологічних теорій впливу Р. Чалдіні та концепції подвійної обробки інформації Д. Канемана дозволило пояснити те, що залишається незрозумілим при суто технічному погляді на фішинг: чому жертвами атак стають освічені та технічно грамотні люди. Відповідь виявилася не в некомпетентності жертв, а в тому, що фішинг цілеспрямовано використовує механізми, закладені в саму архітектуру людського мислення.

Аналіз статистики кіберінцидентів підтвердив, що проблема має не лише якісний, але й виражений кількісний вимір. Зростання кількості унікальних фішингових ресурсів у п'ять разів за п'ять років та збільшення задокументованих кіберінцидентів в Україні з 482 до понад 3 200 є цифрами, що не залишають простору для недооцінки масштабу загрози. При цьому показово, що середній

річний темп приросту інцидентів в Україні перевищує глобальний показник на 6,8 відсоткових пункти — факт, що математично підтверджує те, що практики кібербезпеки знають: Україна зазнає підвищеного рівня кіберзагроз, що є прямим наслідком збройної агресії Росії.

Порівняльний аналіз методів виявлення фішингу дав змогу структурувати розуміння їхніх можливостей та обмежень і зробити висновок, що принципово важливий для побудови систем захисту: жоден із розглянутих методів не є достатнім окремо. Чорні списки працюють за принципом реагування на вже відомі загрози, евристика страждає від проблеми балансу чутливості та специфічності, машинне навчання вразливе до маніпуляцій із навчальними даними, AI-системи є дорогими та вимогливими до інфраструктури, поведінковий аналіз потребує тривалого навчання. Це не недоліки окремих технологій, а об'єктивне відображення складності сучасних фішингових загроз, що робить інтегрований підхід не лише доцільним, а фактично необхідним. Центральним практичним результатом роботи є моя авторська п'ятирівнева модель протидії фішинговим атакам та модель оцінювання ризику на основі зважених факторів. Перша вирішує проблему фрагментованості захисту, забезпечуючи резервування на кожному рівні та циклічний алгоритм самовдосконалення. Друга дає організаціям інструмент, якого їм хронічно не вистачає: можливість кількісно виміряти власну вразливість і прийняти обґрунтовані управлінські рішення щодо пріоритетів захисту. Оцінювання ефективності запропонованих заходів показало зниження ймовірності успішних атак на 85–90% та скорочення фінансових збитків на 60–70%, а аналіз витрат і результатів підтвердив економічну доцільність впровадження з поверненням інвестицій понад 300% у перший рік.

Генеративний штучний інтелект та deepfake-технології вже зараз змінюють природу фішингових атак у спосіб, що робить застарілими багато традиційних підходів до захисту. Якщо раніше орфографічні помилки та підозрілий стиль написання були надійними індикаторами фішингу, то сьогодні цей підхід, що базується на правилах і характерних ознаках, майже втратив свою ефективність.. Це означає, що часовий горизонт актуальності запропонованих рішень є

обмеженим, і подальші дослідження мають зосередитися на адаптації моделей захисту до реалій AI-генерованих загроз.

Загалом результати дослідження підтверджують вихідну гіпотезу про те, що ефективна протидія фішингу можлива лише на перетині технічного захисту нового покоління, системного підвищення людської кіберстійкості та адекватного правового регулювання. Жоден із цих аспектів окремо не є достатнім, тому їх поєднання в єдину систему є відповіддю на виклики, що формуються сучасними кіберзагрозами.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Cialdini R. Influence: The Psychology of Persuasion. New and Expanded ed. New York: Harper Business, 2021. 320 p.
2. Kahneman D. Thinking, Fast and Slow. New York: Farrar, Straus and Giroux, 2011. 499 p.
3. Mitnick K. D., Simon W. L. The Art of Deception: Controlling the Human Element of Security. Indianapolis: Wiley Publishing, 2002. 304 p.
4. Wall D. S. (Ed.) Crime and the Internet. New York: Routledge, 2001. 236 p.
5. Gordon S., Ford R. On the Definition and Classification of Cybercrime. *Journal in Computer Virology*. 2006. Vol. 2. P. 13–20.
6. Epstein S., Pacini R., Denes-Raj V., Heier H. Individual Differences in Intuitive-Experiential and Analytical-Rational Thinking Styles. *Journal of Personality and Social Psychology*. 1996. Vol. 71, № 2. P. 390–405.
7. Kumaraguru P., Sheng S., Acquisti A., Cranor L. F., Hong J. Teaching Johnny Not to Fall for Phish. *ACM Transactions on Internet Technology*. 2010. Vol. 10, № 2. P. 1–31.
8. Abdelhamid N., Thabtah F., Abdel-Jaber H. Phishing Detection: A Recent Intelligent Machine Learning Comparison Based on Models Content and Features. Proceedings of the 2017 IEEE International Conference on Intelligence and Security Informatics. Beijing: IEEE, 2017. P. 72–77.
9. McGuire M., Dowling S. Cybercrime: A Review of the Evidence. Home Office Research Report 75. London: Home Office, 2013. 36 p.
10. Anti-Phishing Working Group. Phishing Activity Trends Report 2024. Lehi, UT: APWG, 2024. 12 p.
11. Verizon. 2024 Data Breach Investigations Report. New York: Verizon Business, 2024. 99 p.
12. IBM Security. Cost of a Data Breach Report 2023. Armonk, NY: IBM Corporation, 2023. 91 p.

- 13.ENISA. ENISA Threat Landscape 2023. Athens: European Union Agency for Cybersecurity, 2023. 156 p.
- 14.Federal Bureau of Investigation. Internet Crime Report 2023. Washington, DC: FBI Internet Crime Complaint Center, 2023. 36 p.
- 15.Microsoft Corporation. Microsoft Digital Defense Report 2023. Redmond, WA: Microsoft, 2023. 130 p.
- 16.Будапештська конвенція про кіберзлочинність. Будапешт: Рада Європи, 2001. 25 с.
- 17.Кримінальний кодекс України: Закон України від 05.04.2001 № 2341-III. Київ: Відомості Верховної Ради України, 2001.

Метадані

ДОКУМЕНТ

Заголовок

КБР_Заєць

Автор

Заєць

Науковий керівник / Експерт

Позднякович О.Є.

ІД документу

334362864

ОРГАНІЗАЦІЯ

Назва організації

**Kyiv National Economic University named after Vadym Hetman
KNEU**

підрозділ

кафедра системного аналізу та кібербезпеки

ЗВІТ

Дата звіту

2026-06-18

Дата редагування

Обсяг знайдених подібностей

Коефіцієнт подібності визначає, який відсоток тексту по відношенню до загального обсягу тексту було знайдено в різних джерелах. Зверніть увагу, що високі значення коефіцієнта не автоматично означають плагіат. Звіт має аналізувати компетентна / уповноважена особа.



КП 1

25

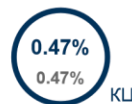
Довжина фрази для коефіцієнта подібності 2



КП 2

9569

Кількість слів



КЦ

73104

Кількість символів

Тривога

У цьому розділі ви знайдете інформацію щодо текстових спотворень. Ці спотворення в тексті можуть говорити про **МОЖЛИВІ** маніпуляції в тексті. Спотворення в тексті можуть мати навмисний характер, але частіше характер технічних помилок при конвертації документа та його збереженні, тому ми рекомендуємо вам підходити до аналізу цього модуля відповідально. У разі виникнення запитань, просимо звертатися до нашої служби підтримки.

Заміна букв		0
Інтервали		0
Мікропробіли		0
Білі знаки		0
Парафрази (SmartMarks)		4

Джерела

Нижче наведений список джерел. В цьому списку є джерела із різних баз даних. Колір тексту означає в якому джерелі він був знайдений. Ці джерела і значення Коефіцієнту Подібності не відображають прямого плагіату. Необхідно відкрити кожне джерело і проаналізувати зміст і правильність оформлення джерела.

10 найдовших фраз

Колір тексту

НАЗВА ТА АДРЕСА ДЖЕРЕЛА URL (НАЗВА БАЗИ)

КІЛЬКІСТЬ ІДЕНТИЧНИХ СЛІВ
(ФРАГМЕНТІВ)

1	Голіусов_КБР 5/21/2026 V. N. Karazin Kharkiv National University (KGNU) (ННІ" Каразінський банківський інститут")	17 0 (0.18 %)
2	https://rep.btsau.edu.ua/bitstream/BNAU/8514/1/Stanslav%20Stepanovych%20Sirenko.pdf	14 0 (0.15 %)
3	Проект інформаційної системи автоматизації B2B-закупівель у Salesforce 11/13/2025 National University "Lviv Politechnika" (NULP2)	13 0 (0.14 %)
4	Фішинг як провідна форма інтернет-шахрайства: сутність і основні різновиди 12/19/2025 State Tax University (Кафедра кримінального права та процесу)	10 0 (0.1 %)
5	System for collecting and analyzing information on personnel manning levels of military units, the process of replenishment, and loss replacement: components, factors, and regulatory framework В. Косевцов, Г. Тіхонов, С. Онікійчук, О. Чайковська;	10 0 (0.1 %)
6	ТЕХНОЛОГІЯ ФОРМУВАННЯ МОДЕЛЕЙ ПОРУШНИКА ПРИ ЗАСТОСУВАННІ МЕТОДІВ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ 12/7/2020 Borys Grinchenko Kyiv Metropolitan University (Borys Grinchenko Kyiv University)	9 0 (0.09 %)
7	ТЕХНОЛОГІЯ ФОРМУВАННЯ МОДЕЛЕЙ ПОРУШНИКА ПРИ ЗАСТОСУВАННІ МЕТОДІВ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ 12/7/2020 Borys Grinchenko Kyiv Metropolitan University (Borys Grinchenko Kyiv University)	7 0 (0.07 %)
8	ТЕХНОЛОГІЯ ФОРМУВАННЯ МОДЕЛЕЙ ПОРУШНИКА ПРИ ЗАСТОСУВАННІ МЕТОДІВ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ 12/7/2020 Borys Grinchenko Kyiv Metropolitan University (Borys Grinchenko Kyiv University)	5 0 (0.05 %)

База даних RefBooks (0.1 %)



#	ЗАГОЛОВОК	КІЛЬКІСТЬ ІДЕНТИЧНИХ СЛІВ (ФРАГМЕНТІВ)
---	-----------	--

джерело: Paperity

1	System for collecting and analyzing information on personnel manning levels of military units, the process of replenishment, and loss replacement: components, factors, and regulatory framework В. Косевцов, Г. Тіхонов, С. Онікійчук, О. Чайковська;	10 (1) (0.1 %)
---	---	----------------

Домашня база даних



#	ЗАГОЛОВОК	КІЛЬКІСТЬ ІДЕНТИЧНИХ СЛІВ (ФРАГМЕНТІВ)
---	-----------	--

Програма обміну базами даних (0.64 %)



#	ЗАГОЛОВОК	КІЛЬКІСТЬ ІДЕНТИЧНИХ СЛІВ (ФРАГМЕНТІВ)
---	-----------	--

2	ТЕХНОЛОГІЯ ФОРМУВАННЯ МОДЕЛЕЙ ПОРУШНИКА ПРИ ЗАСТОСУВАННІ МЕТОДІВ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ 12/7/2020 Borys Grinchenko Kyiv Metropolitan University (Borys Grinchenko Kyiv University)	21 (3) (0.22 %)
---	--	-----------------

3	Голіусов_КБР 5/21/2026	17 (1) (0.18 %)
---	---------------------------	-----------------

5/21/2026

V. N. Karazin Kharkiv National University (KКNU(ННГ" Каразінський банківський інститут)

- | | | |
|---|--|-----------------|
| 4 | Проект інформаційної системи автоматизації B2B-закупівель у Salesforce
11/13/2025
National University "Lviv Politechnika"(NULP2) | 13 (1) (0.14 %) |
| 5 | Фішинг як провідна форма інтернет-шахрайства: сутність і основні різновиди
12/19/2025
State Tax University(Кафедра кримінального права та процесу) | 10 (1) (0.1 %) |

Інтернет (0.15 %)



ДжЕРЕЛО URL

КІЛЬКІСТЬ ІДЕНТИЧНИХ СЛІВ
(ФРАГМЕНТІВ)

- | | | |
|---|---|-----------------|
| 6 | https://rep.btsau.edu.ua/bitstream/BNAU/8514/1/Stani%20slav%20Stepanowch%20Sirenko.pdf | 14 (1) (0.15 %) |
|---|---|-----------------|



Список прийнятих фрагментів

#	ЗМІСТ	КІЛЬКІСТЬ ОДНАКОВИХ СЛІВ (ФРАГМЕНТІВ)
---	-------	---------------------------------------