Міністерство освіти і науки України
Харківський національний університет імені В. Н. Каразіна
Навчально–науковий інститут комп'ютерних наук та штучного інтелекту

Кафедра кібербезпеки інформаційних систем, мереж і технологій

До захисту допущено
Кафедрою КІСМіТ протокол №____ від «___» грудня 2025 р.

завідувач кафедри _____ Марина ЄСІНА
(підпис) *(ім'я, прізвище)*
«___» грудня 2025 р.

Кваліфікаційна робота

здобувача другого (магістерського) рівня вищої освіти
«Методи захисту від атак на базі соціальної інженерії»

Спеціальність (спеціалізація) 125 «Кібербезпека та захист інформації»

Освітня програма «Безпека інформаційних і комунікаційних систем»

Виконавець _____ Олег ГВОЗДЕЦЬКИЙ
(підпис) *(ім'я, прізвище)*

Науковий керівник _____ Ольга МЕЛКОЗЬОРОВА
(підпис) *(ім'я, прізвище)*

Харків – 2025

РЕФЕРАТ

У роботі наведено: 4 рисунка, 9 таблиць, 9 джерел, 2 додатки. Обсяг роботи становить 63 сторінки.

Метою роботи є дослідження методів здійснення фішингових атак, аналіз їх класифікації, технічних механізмів виявлення та попередження, а також розробка рекомендацій щодо підвищення рівня кіберзахисту організації від соціально-інженерних загроз.

Об’єкт дослідження – процеси фішингових атак як одного з найбільш поширених видів кіберзагроз.

Предмет дослідження – методи здійснення фішингових атак, поведінкові та технічні ознаки фішингових повідомлень, сучасні інструменти та засоби захисту інформаційних систем від фішингу.

Методи дослідження – аналіз і порівняння технічних рішень у сфері кіберзахисту; методи статистичної обробки результатів експериментального фішингового тестування; методи моделювання та класифікації атак; аналітичні методики оцінювання ефективності систем безпеки електронної пошти та поведінкових реакцій користувачів.

У роботі досліджено: сучасні підходи до реалізації фішингових атак і методи їх маскування; технічні та поведінкові характеристики фішингових листів; існуючі міжнародні рекомендації та стандарти у сфері протидії соціальній інженерії; результати проведеної фішингової симуляції; ефективність запропонованих технічних і організаційних заходів захисту.

Результати роботи можуть бути використані у діяльності підрозділів інформаційної безпеки, під час розробки внутрішніх політик захисту організації, а також у подальших наукових дослідженнях у сфері кібербезпеки та протидії соціальній інженерії.

Ключові слова: ФІШИНГ, СОЦІАЛЬНА ІНЖЕНЕРІЯ, КІБЕРБЕЗПЕКА, ЗАХИСТ ІНФОРМАЦІЇ, ФІШИНГОВІ АТАКИ, БЕЗПЕКА ЕЛЕКТРОННОЇ ПОШТИ.

ABSTRACT

The paper contains: 4 figure, 9 tables, 9 sources, 2 application. The volume of the work is 63 pages.

The purpose of this work is to study methods of carrying out phishing attacks, analyze their classification, technical mechanisms for detection and prevention, and develop recommendations for improving an organization's level of cyber protection against social engineering threats.

The object of research is phishing attacks as one of the most common types of cyber threats.

The subject of the study is methods of carrying out phishing attacks, behavioral and technical characteristics of phishing messages, modern tools and means of protecting information systems from phishing.

Research methods are analysis and comparison of technical solutions in the field of cyber security; methods of statistical processing of experimental phishing test results; methods of modeling and classifying attacks; analytical methods for evaluating the effectiveness of email security systems and user behavior responses.

The paper examines: modern approaches to phishing attacks and methods of masking them; technical and behavioral characteristics of phishing emails; existing international recommendations and standards in the field of countering social engineering; results of phishing simulation; effectiveness of proposed technical and organizational protection measures.

The results of this work can be used in the activities of information security departments, in the development of internal policies for protecting organizations, and in further scientific research in the field of cybersecurity and countering social engineering.

Keywords: PHISHING, SOCIAL ENGINEERING, CYBERSECURITY, INFORMATION PROTECTION, PHISHING ATTACKS, E-MAIL SECURITY.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

CI – Соціальна інженерія

BEC – Business Email Compromise. Компрометація бізнесової електронної пошти

FBI – Federal Bureau of Investigation. Федеральне бюро розслідувань

IC3 – Internet Crime Complaint Center. Центр скарг на інтернет–злочини

IBM – International Business Machines Corporation. Міжнародна бізнес–машина корпорація

CFO – Chief Financial Officer. Головний фінансовий директор

AI – Artificial Intelligence. Штучний інтелект

DNC – Democratic National Committee. Демократичний національний комітет

США – Сполучені Штати Америки

AUP – Acceptable Use Policy. Політика прийнятного використання

NIST – National Institute of Standards and Technology, Національний інститут стандартів і технологій

IEC – International Electrotechnical Commission, Міжнародна електротехнічна комісія

ISO – International Organization for Standardization, Міжнародна організація зі стандартизації

IRP – Incident Response Plan. План реагування на інциденти

SANS – System Administration, Networking, and Security. Адміністрування систем, мережі та безпека

HR – Human Resources. Людські ресурси

URL – Uniform Resource Locator. Уніфікований локатор ресурсів

PTES – Penetration Testing Execution Standard. Стандарт виконання тестування на проникнення

ВСТУП

На сьогоднішній день СІ стала однією з найбільш поширених і небезпечних форм кіберзлочинності. Використовуючи психологічні маніпуляції, зловмисники здатні обманювати користувачів, змушуючи їх зробити якісь дії або надати конфіденційну інформацію. Наприклад: війти в довіру та змусити відправити кошти на рахунок зловмисника, або відправити йому пароль чи паспортні данні, тощо. Атаки на основі соціальної інженерії можуть мати серйозні наслідки для організацій, включаючи фінансові втрати, репутаційні ризики та порушення законодавства про захист даних.

В умовах стрімкого розвитку технологій та зростання залежності суспільства від інформаційних систем, важливість захисту від соціальної інженерії стає дедалі актуальнішою. Зловмисники постійно вдосконалюють свої методи, що робить традиційні засоби захисту недостатніми. Тому необхідно розробляти нові підходи до захисту, які б враховували специфіку соціальної інженерії.

У цьому контексті, дослідження методів захисту від атак на базі соціальної інженерії є надзвичайно важливим. Це дозволяє не лише виявити вразливості в системах безпеки, але й розробити ефективні стратегії для їх усунення. Важливим аспектом є також підвищення обізнаності співробітників організацій щодо загроз соціальної інженерії, що може суттєво знизити ризики.

Отже, метою даної роботи є аналіз існуючих методів захисту від атак соціальної інженерії, а також розробка рекомендацій щодо їх впровадження в практику. Це дослідження має на меті не лише теоретичний аналіз, але й практичні рекомендації, які можуть бути корисними для організацій у забезпеченні інформаційної безпеки.

1 ТЕОРИТИЧНІ ОСНОВИ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ ТА МЕТОДИ АТАК НА ЇЇ ОСНОВІ

1.1 Поняття соціальної інженерії

1.1.1 Визначення та місце в моделі загроз

Соціальна інженерія – це сукупність методів психологічного впливу на людину, спрямованих на отримання несанкціонованого доступу до інформації, ресурсів або систем. На відміну від класичних технічних атак, СІ експлуатує вразливість людської поведінки та емоційних реакцій.

У моделі загроз СІ розглядається як комплексна attack vector, який може стати початковим етапом складних багаторівневих атак, поєднуючи технічні та психологічні методи. Зловмисники використовують помилки користувачів, відсутність знань щодо кібергігієни або довіру до авторитетних джерел, щоб обійти традиційні засоби захисту, такі як міжмережеві екрани, антивіруси чи багатофакторна автентифікація.

СІ часто відіграє ключову роль у таких загрозах, як:

1) Викрадення облікових даних;
2) Початкове проникнення для подальшого розгортання шкідливого ПЗ;
3) Компрометація корпоративних систем;
4) Шахрайство на фінансовому та організаційному рівнях;

Через те, що людський фактор є найменш контрольованим елементом системи безпеки, СІ входить до топ–3 найпоширеніших векторів атак у світі.

1.1.2 Психологічні механізми впливу

Атаки соціальної інженерії досягають успіху завдяки експлуатації фундаментальних аспектів людської психології. Знання цих психологічних принципів відіграє ключову роль у виявленні та запобіганні подібним загрозам. Соціальні інженери спираються на когнітивні упередження та емоційні реакції, що робить їхні методи особливо ефективними. Нижче наведено основні психологічні фактори, які використовуються в атаках:

1) Авторитет – зловмисники часто видають себе за представників влади, таких як поліцейські, судові виконавці або працівники банків. Цей авторитет викликає у жертви повагу або навіть страх, через що вона легше піддається маніпуляції [1];

2) Соціальний доказ – люди, як правило, довіряють тому, що «всі інші роблять». Наприклад, шахраї можуть посилатися на «відгуки» або «успіхи» інших людей, щоб переконати жертву слідувати їхнім інструкціям [1];

3) Довіра – люди за своєю природою схильні довіряти іншим, особливо тим, хто здається авторитетним або компетентним [1];

4) Готовність допомагати – люди часто готові допомогти іншим, і це може бути використано шахраями. Наприклад, люди можуть надати доступ до будівлі або інформації, якщо їм здається, що хтось у біді [1];

5) Жадібність – зловмисники можуть обіцяти вигоду, наприклад, виграш великої суми грошей або цінного призу, якщо жертва надасть свої дані або оплатить «невелику» комісію. Це поширена схема в онлайн–шахрайствах з фальшивими лотереями чи акціями [1].

Соціальні інженери розробляють свої атаки так, щоб викликати ці психологічні реакції, що робить їх схеми більш імовірними для успіху. Розуміння цих тенденцій допоможе індивідам та організаціям краще підготуватися до виявлення та опору спробам соціальної інженерії. Важливо навчати співробітників розпізнавати ці маніпуляції, впроваджувати політики безпеки та регулярно проводити тренінги, щоб зменшити ризики, пов'язані з соціальною інженерією.

1.2 Історія розвитку соціальної інженерії

Початки соціальної інженерії можна відслідкувати ще в давні часи, коли правителі використовували різноманітні маніпуляції та вплив для зміни громадської думки та поведінки. Однак сучасна концепція соціальної інженерії стала актуальною в другій половині 20 століття, особливо у контексті розвитку інформаційних технологій. Ще у 1950 – 60–х роках соціальні психологи, такі як Стенлі Мілгром та Філіп Зімбардо, проводили експерименти, що досліджували, як

люди реагують на авторитети та соціальний тиск. Ці досліди стали важливими джерелами у розумінні механізмів соціального впливу [2].

З розвитком комп'ютерів і Інтернету виникла нова сфера соціальної інженерії, пов'язана зі зловживанням технологій для отримання конфіденційної інформації та маніпулювання людьми. Так соціальні інженери можуть використовувати фішингові атаки, щоб отримати доступ до особистих даних або паролів користувачів. Також історія соціальної інженерії включає в себе приклади політичних та корпоративних маніпуляцій [2].

Наприклад, виборчі кампанії можуть використовувати соціально–інженерні методи для впливу на голосування, а компанії – для отримання конкурентного переваги або злочинного отримання конфіденційної інформації. В цілому, історія соціальної інженерії відображає постійний розвиток методів та технологій, що використовуються для впливу на людей та отримання несанкціонованого доступу до інформації [2].

1.3 Основні види атак соціальної інженерії

Атаки соціальної інженерії характеризуються різноманітністю форм, кожна з яких спрямована на маніпуляцію певними людськими слабкостями та вразливостями. Розуміння цих типів є критично важливим для розробки ефективних стратегій захисту. Деякі з найпоширеніших типів включають:

1) Фішинг є однією з найрозповсюдженіших тактик у сфері соціальної інженерії. Він передбачає розсилку підроблених повідомлень електронною поштою, спрямованих на те, щоб вплинути на одержувача або змусити його розкрити дані, активувати файли чи перейти за підозрілими посиланнями. Типові фішингові повідомлення зазвичай не мають конкретного адресата. Замість цього їх масово надсилають на величезні списки електронних адрес, які злочинці купують у мережі. Такий підхід дозволяє охопити тисячі людей, не витрачаючи часу на збір відкритої інформації з інтернету. Наприклад, навіть без будь–яких знань про особистість жертви можна створити універсальний лист, що хитрістю спонукає користувача відвідати фальшивий веб–сайт або скачати небезпечний файл. Після того як одержувач відкриє такий файл, на його пристрої може запуститися

віддалена оболонка або інсталюватися шкідливе програмне забезпечення. Отримавши доступ через віддалену оболонку чи вірусне програмне забезпечення, хакери здатні безпосередньо взаємодіяти з системою, запускати експлойти, підвищувати свої права доступу та поглиблювати проникнення в мережу організації;

2) Спис–фішинг – це різновид традиційного фішингу, коли фахівець із соціальної інженерії зосереджується на конкретній жертві. Якщо порівняти з рибалкою, де замість сітки використовується гарпун, йому потрібно вивчити звички кожної рибини та підібрати підхід до неї. Аналогічно, для успішної атаки необхідно зібрати, систематизувати та використати інформацію з відкритих джерел про цільову компанію чи особу, щоб грамотно підготувати пастку;

3) Байтінг – у цьому випадку зловмисник використовує «приманку» для того, щоб змусити людину діяти певним чином. Приманка може бути у вигляді зараженого USB–накопичувача, залишеного в публічному місці, або фальшивого оголошення про роботу з привабливою оплатою. Як тільки жертва використовує «приманку», шкідливе програмне забезпечення потрапляє на її комп’ютер, або вона розкриває конфіденційні дані [3];

4) Претекстинг – це техніка, за якої зловмисник вигадує фальшиву ситуацію або сценарій, щоб змусити жертву розкрити конфіденційну інформацію. Претекстинг може бути дуже переконливим, оскільки зловмисник може довго готуватися, досліджуючи жертву, щоб знати, як краще до неї підійти. Наприклад, зловмисник може представитися працівником служби безпеки та попросити підтвердити інформацію для доступу до системи [3];

5) Вішинг – це метод соціальної інженерії, коли атакуючий телефонує жертві та веде з нею розмову по телефону. Він часто вважається складнішим за фішинг, оскільки вимагає сильних імпровізаційних здібностей. Якщо у фішингу є час підготувати текст електронного листа заздалегідь, то вішинг передбачає створення діалогу на ходу, з необхідністю контролювати кожну деталь бесіди до її завершення;

6) Попутне проникнення – це фізичний метод соціальної інженерії, коли зловмисник проходить за співробітником компанії у захищену зону, використовуючи їхній пропуск або просто входячи за ними через двері. Попутне проникнення часто використовується для отримання доступу до офісних приміщень або серверних кімнат, де зберігається конфіденційна інформація [3];

7) Послуга за послугу – ця техніка полягає в пропозиції обміну інформацією або послугами. Наприклад, зловмисник може зателефонувати в компанію і запропонувати «допомогу» з вирішенням проблеми, а в обмін попросити надати доступ до системи або розкрити конфіденційну інформацію. Людина, яка отримала таку пропозицію, може навіть не підозрювати, що має справу з шахраєм [3].

1.4 Аналіз актуальності проблеми та статистичні дані

1.4.1 Вступ до проблеми соціальної інженерії

СІ є однією з найсерйозніших загроз у сучасному цифровому світі, де кібербезпека стає дедалі важливішою для індивідів, компаній та держав. Актуальність проблеми зростає через швидкий розвиток технологій, збільшення кількості онлайн–інтеракцій та поширення соціальних мереж. У епоху пандемії COVID–19, коли багато людей перейшли на віддалену роботу, СІ стала ще більш ефективною, оскільки зловмисники експлуатують страх, невизначеність та довіру до авторитетів.

1.4.2 Динаміка зростання форм фішингу як векторів соціальної інженерії

Для ілюстрації зростання різних форм фішингу як ключових векторів соціальної інженерії, у табл. 1.1 наведено актуальні статистичні дані, які підкреслюють велике збільшення цих атак в останні роки.

Таблиця 1.1 – Зростання форм фішингу як векторів соціальної інженерії

Тип атаки	Динаміка зростання	Період	Джерело
Голосовий фішинг (Вішинг)	442%	2024	DeepStrike
SMS–фішинг (Смішинг)	2900%	2023–2024	DeepStrike

Подовження таблиці 1.1.

Тип атаки	Динаміка зростання	Період	Джерело
SMS–фішинг (Смішинг)	3000%	з 2023	DeepStrike

Актуальність проблеми підкреслюється тим, що CI не вимагає глибоких технічних знань від атакуючих – достатньо психологічних маніпуляцій, таких як створення фальшивих сценаріїв довіри або використання соціального тиску. Це робить її доступною для широкого кола злочинців, від окремих хакерів до організованих груп, включаючи державні актори та кіберзлочинні синдикати. За даними різних джерел, CI є причиною близько 98% успішних кібератак, що свідчить про її домінуючу роль у сучасних загрозах. Крім того, втрати від таких атак оцінюються в мільярди доларів щорічно, впливаючи на економіку, репутацію компаній та приватне життя людей. У бізнесі це може призвести до витоку комерційних таємниць, фінансових збитків або навіть банкрутства; для держав – до загроз національній безпеці, як у випадках шпигунства чи кібервійни; для індивідів – до ідентифікаційної крадіжки, шахрайства або емоційного стресу.

1.4.3 Приклади наслідків та додаткові дані

Глобальна середня вартість витоку даних досягла рекордного максимуму в 4,88 мільйона доларів у 2024 році, що є очевидним індикатором зростання збитків. Витоки, що починаються з фішингової атаки, ще дорожчі, в середньому 4,91 мільйона доларів, згідно з останнім звітом IBM X Force 2025 Cost of a Data Breach Report [4].

Однак справжні фінансові збитки найбільш помітні в атаках BEC. Звіт FBI’s IC3 Annual Report свідчить, що лише BEC спричинив 2,77 мільярда доларів у заявлених втратах. Для малого бізнесу наслідки часто є екзистенційними; оцінюється, що 60% змушені закритися протягом шести місяців після серйозного кіберінциденту, роблячи боротьбу з кібератаками на малий бізнес питанням виживання [4]. Приклади наслідків включають:

1) Перехоплення знаменитостей: Біткоїн–скандал у Twitter (2020).

У липні 2020 року нападники використали соціальну інженерію на основі телефону, щоб отримати доступ до внутрішніх інструментів адміністратора Twitter. Потім вони захопили акаунти високопоставлених фігур, таких як Барак Обама та Ілон Маск, щоб просувати біткоїн–скандал, вкравши понад 118 000 доларів за години. Інцидент продемонстрував, наскільки легко CI може скомпрометувати навіть великі технологічні платформи [4];

2) $25,6 млн крадіжка з глибокими фейками: Кейс–стаді Arup (2024).

На початку 2024 року працівника фінансів глобальної інженерної фірми Arup обманом змусили переказати 25,6 мільйона доларів. Обман був безпрецедентним: співробітник взяв участь у відеоконференції з тими, кого вважав CFO компанії та іншими старшими керівниками [4]. Насправді кожна людина на дзвінку, крім жертви, була створеним ШІ глибоким фейком. Цей випадок знаменує собою жахливу нову еру для BEC, доводячи, що «бачити більше не означає вірити» [4];

3) Політична маніпуляція: Хак DNC (2016).

Цей інцидент залишається класичним прикладом далекосяжних наслідків соціальної інженерії. Російські розвідувальні групи використали цільові спір–фішингові електронні листи, щоб скомпрометувати мережу Демократичного національного комітету. Внаслідок витоку конфіденційних електронних листів це значно вплинуло на президентські вибори в США 2016 року [4].

1.5.4 Основні статистичні індикатори соціальної інженерії

Статистичні дані з надійних джерел підтверджують цю актуальність. Для ілюстрації нижче наведено у табл. 1.2, складену на основі інформації з Keevee та GitNux. Вона включає всі ключові показники, які підкреслюють масштаби проблеми.

Таблиця 1.2 – Основні статистичні індикатори соціальної інженерії

Показник	Значення	Рік	Джерело
Відсоток кібератак через соціальну інженерію	98%	2024	Keevee
Частка фішингу в атаках	70%	2024	Keevee

Подовження таблиці 1.2.

Показник	Значення	Рік	Джерело
Організації, що зазнали атак	85%	2024	Keevee
Співробітники, що провалюють тести	45%	2024	Keevee
Зростання кількості атак	27%	2025	Keevee
Спрямованість атак на співробітників віком 25–34 років	60%	2024	GitNux
Прогноз зростання атак	27%	2025	Keevee

1.5.5 Аналіз статистичних даних

Статистичні дані з надійного джерела такого, як keevee підтверджує цю актуальність. Нижче наведено ключові пункти з останніх досліджень:

1) 98% кібератак засновані на соціальній інженерії. Людський фактор залишається найслабшою ланкою в кібербезпеці [5];

2) Фішинг становить 70% усіх атак із використанням соціальної інженерії. Шахрайство з використанням електронної пошти домінує завдяки своїй масштабовності та простоті [5];

3) У 2024 році 85% організацій зазнали атак із використанням соціальної інженерії. Більшість компаній зазнають атак, незалежно від розміру [5];

4) 45% співробітників провалюють тести на соціальну інженерію. Навчання підвищенню обізнаності необхідне для зниження вразливості [5];

5) Кількість атак із використанням соціальної інженерії збільшилася на 27% у 2025 році. Кіберзлочинці продовжують використовувати нові платформи та технології [5].

Ці дані свідчать про актуальність проблеми соціальної інженерії та необхідність заходів: освіти користувачів, багаторівневої аутентифікації та тренінгів. Цей метод атак ефективний і дешевий, з зростанням актуальності через AI. Важливо аналізувати статистику та протидіяти загрозі колективно.

2 МЕТОДИ ТА СТРАТЕГІЇ ЗАХИСТУ ВІД АТАК СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ

СІ продовжує залишатися одним із ключових векторів кібератак, спрямованих як на приватних користувачів, так і на організації будь–якого масштабу. На відміну від класичних технічних атак, соціально–інженерні загрози експлуатують людський фактор, що робить їх надзвичайно складними для повного усунення. Проте сучасні методи захисту – організаційні, технічні та комплексні – дозволяють істотно знизити ризики. У цьому розділі наведено систематизований огляд актуальних стратегій протидії.

2.1 Організаційні методи захисту

Організаційні методи захисту становлять основу будь–якої системи протидії атакам соціальної інженерії. Більшість технічних засобів не здатні повністю нейтралізувати загрози, спрямовані на психологічні слабкості людини, тому створення ефективних політик, навчання персоналу та впровадження симуляцій є критично необхідними. Згідно з рекомендаціями міжнародних стандартів інформаційної безпеки ISO/IEC 27001 та NIST SP 800–53, саме організаційні заходи є початковою та визначальною ланкою у формуванні безпечної поведінки співробітників (ISO/IEC 27002, 2022; NIST, 2020).

2.1.1 Розробка політик інформаційної безпеки

Політики інформаційної безпеки (ІБ) представляють собою формалізовані документи, які детально регулюють правила поводження з інформаційними активами – такими як конфіденційні дані, бази клієнтів чи інтелектуальна власність. Вони чітко визначають повноваження співробітників, встановлюючи, хто має доступ до певних ресурсів, як їх використовувати та що робити в разі інцидентів. Це не просто набір правил, а стратегічний інструмент, який інтегрується в корпоративну культуру для забезпечення сталого захисту. До ключових політик, що допомагають проти соціальної інженерії, належать:

1) Acceptable Use Policy (AUP) – це документ, що визначає обмеження та правила, з якими користувач повинен погодитися для отримання доступу до

корпоративної мережі, Інтернету або інших обчислювальних ресурсів. Багато підприємств та навчальних закладів вимагають від співробітників або студентів підписати AUP перед тим, як надати їм ідентифікатор мережі [6];

2) Email & Communication Policy – складається з рекомендацій, які визначають, як слід обмінюватися інформацією всередині організації. Вона також окреслює правила комунікації із зовнішніми зацікавленими сторонами. Ці політики охоплюють широкий спектр діяльності, включаючи надсилання, отримання, управління, складання, відповіді, пересилання та архівування електронних листів. Співробітники повинні дотримуватися політики використання електронної пошти під час користування корпоративною електронною адресою, щоб забезпечити належне представлення компанії. Впровадження таких політик забезпечує належну практику, сприяє професіоналізму, ефективності та безпеці всередині організації [7];

3) Password Policy – NIST SP 800–63B встановлює стандарти для сучасних політик щодо паролів, надаючи пріоритет як зручності використання, так і безпеці. Останні оновлення відходять від застарілих практик, таких як часта зміна паролів, і замість цього зосереджуються на створенні безперебійної, зручної для користувачів структури, яка мінімізує вразливість і водночас підвищує рівень відповідності вимогам;

4) Incident Response Policy (IRP) – це структурований підхід, який організації використовують для боротьби з порушеннями безпеки, кібератаками та іншими інцидентами, пов'язаними з IT. Він визначає кроки, які необхідно вжити до, під час і після інциденту, щоб мінімізувати збитки, відновити роботу служб і запобігти подібним інцидентам у майбутньому;

5) Data Classification & Handling Policy – дозволяє обмежувати доступ до конфіденційних даних, згідно з принципами найменших привілеїв. Це знижує ефективність атак, націлених на витік інформації.

Політики інформаційної безпеки відіграють ключову роль у захисті організації від загроз соціальної інженерії, таких як фішинг чи уішинг. Вони не

лише мінімізують ризики, але й створюють міцний бар'єр проти маніпуляцій, що експлуатують людський фактор. Ось як це працює:

Основні напрями впливу:

1) Стандартизація поведінки персоналу – політики встановлюють чіткі правила, що зменшують імпульсивні рішення та сприяють свідомим діям, роблячи співробітників менш вразливими до обману;

2) Підвищення обізнаності – вони детально описують ознаки атак, як–от підозрілі електронні листи чи неочікувані запити, що допомагає працівникам швидко розпізнавати загрози;

3) Процедури ескалації – визначають кроки дій у разі підозри – від повідомлення керівництва до ізоляції інциденту, забезпечуючи швидку реакцію;

4) Запобігання небезпечним діям – наприклад, забороняють пересилання конфіденційних документів на особисті email, унеможливлюючи витік інформації.

Міжнародні стандарти (як від NIST чи ISO) підкреслюють, що ефективна політика має бути:

1) Чіткою – лаконічною та зрозумілою, без двозначностей;

2) Регулярно оновлюваною – адаптованою до нових загроз, щоб залишатися актуальною;

3) Доступною всім співробітникам – легко знайденою, наприклад, через внутрішній портал чи тренінги;

4) Інтегрованою у процеси компанії – вбудованою в щоденну роботу, з обов'язковими навчаннями та перевірками.

Міжнародні стандарти відіграють ключову роль у формуванні ефективних політик інформаційної безпеки, надаючи структуровані рамки для зниження ризиків соціальної інженерії. Вони допомагають організаціям впроваджувати перевірених практик, інтегруючи їх у повсякденні процеси. Нижче розглянуто основні з них із акцентом на релевантні контролі та рекомендації:

1) ISO/IEC 27002 – це міжнародний стандарт, який містить рекомендації для організацій, що прагнуть створити, впровадити та вдосконалити систему управління інформаційною безпекою, орієнтовану на кібербезпеку [8];

2) NIST SP 800–53 Rev.5 – розроблений національним інститутом стандартів і технологій США, цей стандарт визначає контролі для захисту федеральних інформаційних систем. Ключові з них включають: AT–2 (навчання з підвищення обізнаності), AT–3 (рольове навчання), PL–4 (правила поведінки) та IR–1 (політика реагування на інциденти). Вони сприяють чіткому визначенню процедур, регулярному оновленню знань співробітників та інтеграції політик у корпоративні процеси, роблячи організацію стійкішою до фішингу та інших маніпуляцій;

3) Інститут SANS – пропонує практичні шаблони політик, адаптовані для різних організацій. Ці ресурси забезпечують доступність та простоту впровадження, допомагаючи компаніям швидко інтегрувати стандарти у свою діяльність. Шаблони охоплюють аспекти від навчання до процедур ескалації, роблячи їх ідеальним інструментом для початківців у сфері інформаційної безпеки.

Такий підхід не лише знижує ризики, але й будує культуру безпеки, де кожен співробітник стає частиною захисного механізму. Це перетворює політику з формального документа на потужний інструмент стійкості організації.

2.1.2 Регулярні тренінги персоналу

Тренінги з інформаційної безпеки відіграють ключову роль у протидії атакам соціальної інженерії, адже людський фактор є основною точкою входу в 82% кібератак (звіт Verizon DBIR, 2023). Регулярні навчання допомагають зменшити ризики, пов'язані з фішингом та іншими маніпуляціями.

Типи тренінгів:

1) Awareness Training – базові навчання для всіх співробітників, що охоплюють загальні принципи інформаційної безпеки;

2) Phishing Awareness Training – спеціалізовані тренінги з симуляціями фішингових сценаріїв для практичного тренування;

3) Role–Based Training – навчання, адаптоване для критичних ролей, таких як HR, фінансові відділи, керівники та користувачі з високими правами доступу;

4) Micro–learning – короткі модулі (2–5 хвилин), що дозволяють швидко оновлювати знання без великих витрат часу;

5) Gamification Training – гейміфіковані елементи, як тести, квести чи ігри, для підвищення зацікавленості та запам'ятовування.

Чому одноразовий тренінг недостатній:

1) Дослідження KnowBe4 (2022) показують, що ефект від одноразового тренінгу триває лише 4–6 тижнів. Без регулярних нагадувань рівень ризику швидко повертається до початкового. Тому ефективний підхід – це модель безперервного навчання (continuous learning), що включає періодичні повторення та оновлення матеріалів.

Ефективність регулярних тренінгів:

1) Згідно з даними KnowBe4, регулярні тренінги знижують ризик кліку по фішинговому посиланню на 70–90%. Звіт Proofpoint Human Factor Report підтверджує, що фішинг залишається найуспішнішим вектором атак через людський фактор. Verizon DBIR зазначає, що кампанії фішингу успішні приблизно в 3% випадків навіть після фільтрів, тому роль навчання є критичною для мінімзації цих ризиків.

2.1.3 Роль соціальних симуляцій атак

Симуляції атак соціальної інженерії – це ключовий інструмент для зміцнення кібербезпеки в організаціях. Вони допомагають поєднати навчання з практичною оцінкою ризиків, дозволяючи тестувати поведінку співробітників без реальних наслідків. Нижче наведено розширене опис із новою структурою: спочатку переваги та мотивація, потім визначення та типи, далі практичні аспекти проведення, метрики для аналізу, а також рекомендації та обмеження.

Переваги симуляцій:

1) Практичне навчання – учасники отримують досвід розпізнавання фішингу чи вішингу в безпечному середовищі, що ефективніше за лекції;

2) Оцінка ризиків – виявляють вразливі відділи чи ролі, допомагаючи фокусувати зусилля на проблемних зонах;

3) Зниження інцидентів – за даними Verizon DBIR, регулярні симуляції знижують успішність атак на 70–90%;

4) Підтримка стандартів – допомагають дотримуватися GDPR, NIST чи ISO 27001, забезпечуючи комплаєнс.

Як проводити симуляції:

1) Планування – визначте цілі (наприклад, тестування відділу), оберіть сценарії та отримайте згоду учасників;

2) Реалізація – розішліть фальшиві повідомлення або організуйте дзвінки з використанням інструментів для анонімізації;

3) Аналіз – зберіть дані про реакції та проведіть debriefing із зворотним зв'язком;

4) Ітерації – повторюйте щокварталу, адаптуючи до нових загроз, як AI–генерований фішинг.

У табл. 2.1 наведено розширених метрик симуляцій атак соціальної інженерії.

Таблиця 2.1 – Розширені метрики симуляцій атак соціальної інженерії

Метрика	Опис	Приклад значення
Click Rate	Відсоток кліків на посилання	15% (високий ризик)
Open Rate	Відсоток відкритих повідомлень	40% (середній рівень)
Report Rate	Відсоток повідомлень про атаку	25% (низький – потребує навчання)
Credential Submission Rate	Відсоток введених фальшивих даних	10% (критично)
Time to Report	Час до повідомлення (хв)	30 хв (швидко)
Departmental Vulnerability	Вразливість за відділами	Маркетинг: 20% кліків
Repeat Offender Rate	Відсоток повторних «жертв»	5% (персоналізація)
Overall Success Rate	Загальна успішність атак	12% (ціль <5%)

Кращі практики та обмеження:

1) Кращі практики – поєднуйте з тренінгами, варіюйте сценарії, уникайте покарань – фокусуйтеся на навчанні. Залучайте HR для етики;

2) Обмеження – не враховують стрес реальних ситуацій, можуть спричинити «фішинг–утому» та потребують бюджету. Не замінюють технічні захисні механізми.

2.2 Технічні методи захисту

Технічні заходи є другою лінією оборони після організаційних заходів. Хоча СІ переважно націлена на людей, ефективне поєднання фільтрації, контролю доступу, моніторингу та багатофакторної аутентифікації може значно зменшити ймовірність успішної атаки. Наприклад, фільтрація електронної пошти може автоматично блокувати фішингові повідомлення, а контроль доступу – обмежувати вхід до конфіденційних даних лише авторизованим користувачам. Технічний захист допомагає виявляти підозрілу активність, блокувати шкідливі повідомлення, запобігати компрометації облікових записів та реагувати на ознаки шкідливої активності, такі як незвичайні спроби входу або передачі даних. Більшість сучасних кіберзагроз використовують соціальну інженерію як початковий етап атаки, тому багаторівневий технічний підхід (defense–in–depth) є критичним (Microsoft, 2023). Це включає не лише реактивні інструменти, а й проактивні рішення, як штучний інтелект для аналізу поведінки користувачів, що дозволяє попереджати атаки на ранніх стадіях. Загалом, інтеграція цих заходів із навчанням персоналу створює міцну систему захисту, знижуючи ризики на 50–80% за даними експертів з кібербезпеки.

2.2.1 Антифішингові фільтри

Антифішинговий фільтр виявляє шкідливі URI, порівнюючи їх із базою даних відомих фішингових URI. Сучасні антифішингові фільтри використовують штучний інтелект для виявлення та фільтрування шкідливих електронних листів, застосовуючи різні методи пошуку ознак фішингу. Деякі антифішингові фільтри переписують усі URL–адреси посилань і використовують аналіз «часу кліка», щоб захистити від посилань на веб–сайти, які здаються безпечними, але згодом стають небезпечними [9].

Фільтри фішингу запобігають потраплянню спаму та фішингових листів у корпоративну мережу та поштові скриньки співробітників. Фільтри фішингу є важливою складовою стратегії кібербезпеки організації, оскільки фішинг є найпоширенішим вектором порушення безпеки даних та атак, таких як компрометація ділової електронної пошти (BEC). Програми–вимагачі часто потрапляють у корпоративну мережу через фішингові листи. Наявність правильного типу фільтра фішингу означає, що ваша організація має надійний захист від багатьох типів кібератак [9].

Типи антифішингових технологій:

1) DNS– фільтрація – системи на кшталт Quad9, OpenDNS від Cisco Umbrella та Cloudflare 1.1.1.2 блокують доступ до шкідливих URL на рівні доменного запиту, запобігаючи завантаженню фішингових сторінок. Вони забезпечують захист у локальних мережах та під час віддаленої роботи завдяки хмарній аналітиці та автоматичному оновленню репутаційних списків;

2) Протоколи для електронної пошти (SPF, DKIM, DMARC) – SPF перевіряє право сервера надсилати листи від імені домену, DKIM забезпечує цифровий підпис листів, а DMARC інтегрує обидва та дозволяє політикам блокувати підроблені повідомлення. Впровадження DMARC із політикою reject зменшує ризик фішингових атак на бренд більш ніж на 90%;

3) ML– платформи антифішингу – системи на кшталт Gmail та Microsoft 365 використовують машинне навчання для аналізу шаблонів листів, історії листування, стилістичних особливостей, метаданих та аномалій (наприклад, нетиповий час чи географія). Google блокує понад 100 мільйонів фішингових листів щодня;

4) Фільтрація електронної пошти – посередники або постачальники послуг отримують листи до користувача, сканують їх на ознаки шкідливого вмісту та перевіряють SPF, DKIM та DMARC. Це зменшує навантаження на персонал, але вимагає вибору постачальника з урахуванням пропускної здатності, типу реалізації (програмне забезпечення, апаратне забезпечення чи хмарна служба) та можливих

змін у DNS–записах. Хмарні рішення особливо ефективні для доступності, але залежать від SLA та контрактів.

2.2.2 Двофакторна автентифікація

Багатофакторна автентифікація , також відома як двофакторна автентифікація, є одним із найефективніших інструментів захисту облікових записів від фішингових атак. Навіть якщо зловмисник отримає пароль користувача через фішинг, багатофакторна автентифікація додає додатковий шар безпеки, вимагаючи підтвердження ідентичності через другий фактор. Це робить атаки значно складнішими, оскільки хакери повинні не лише вкрасти пароль, але й отримати доступ до другого елемента, такого як фізичний пристрій чи біометричні дані. За даними Google (2019), використання апаратних ключів безпеки на базі стандарту Fast IDentity Online 2 (FIDO2) блокує до 99% фішингових атак, включаючи цілеспрямовані (spear–phishing), оскільки ці ключі не піддаються фішингу через відсутність взаємодії з веб–сторінками.

Багатофакторна автентифікація працює на принципі поєднання кількох факторів автентифікації: щось, що ви знаєте (наприклад, пароль), щось, що ви маєте (наприклад, телефон чи ключ), і щось, що ви є (біометрія). Це особливо важливо в епоху зростання фішингових атак, коли паролі часто стають жертвою соціальної інженерії. Впровадження багатофакторної автентифікації рекомендується для всіх онлайн–сервісів, включаючи електронну пошту, банківські додатки та корпоративні системи. Наприклад, компанії на кшталт Microsoft та Google активно просувають багатофакторну автентифікацію як стандарт безпеки, і багато платформ, таких як GitHub чи PayPal, роблять її обов'язковою для підвищеної безпеки.

Однак не всі методи багатофакторної автентифікації однаково надійні. Вибір методу залежить від потреб користувача: для особистого використання підходять простіші варіанти, а для корпоративного середовища – більш захищені. Нижче наведено основні типи багатофакторної автентифікації з прикладами, перевагами, недоліками та рівнем надійності:

1) SMS–код (одноразовий пароль через SMS) – це найпоширеніший, але найменш надійний метод. Користувач отримує одноразовий пароль (одноразовий пароль) на телефон через SMS. Приклад: стандартний двофакторна автентифікація у багатьох банків. Надійність: низька, оскільки вразливий до атак типу атака на заміну SIM–карти (коли хакер перехоплює SIM–карту) або перехоплення SMS. Переваги: простий у налаштуванні, не вимагає додаткового програмного забезпечення. Недоліки: залежність від мобільного зв'язку, ризик втрати телефону. Рекомендується як базовий варіант, але не для високоризикових сценаріїв;

2) Часовий одноразовий пароль (Time–based One–Time Password) – генерує одноразові коди на основі часу через додатки. Приклади: Google Authenticator, Authy чи Microsoft Authenticator. Надійність: середня–висока, оскільки коди змінюються кожні 30 секунд і не передаються через мережу. Переваги: працює офлайн, не залежить від інтернету чи мобільного зв'язку, легко інтегрується з багатьма сервісами. Недоліки: вимагає встановлення додатка, ризик втрати телефону (але можна відновити через резервні коди). Ідеально для повсякденного використання, особливо в поєднанні з іншими методами;

3) Push Notification багатофакторна автентифікація – надсилає сповіщення на телефон для підтвердження входу. Приклад: Microsoft Authenticator або Duo Security. Надійність: висока, оскільки вимагає взаємодії користувача (натискання «Підтвердити») і захищена шифруванням. Переваги: зручний і швидкий, не потрібно вводити коди вручну, працює навіть без інтернету на телефоні (якщо додаток встановлений). Недоліки: залежність від телефону, потенційний ризик фішингу через підроблені сповіщення (хоча сучасні додатки мають захист). Підходить для користувачів, які цінують простоту;

4) Апаратні ключі безпеки (Fast IDentity Online 2 / Web Authentication) – фізичні пристрої, які підключаються до USB або використовуються через NFC/Bluetooth. Приклади: YubiKey, Google Titan чи Feitian. Надійність: дуже висока, оскільки ключі не піддаються фішингу – вони взаємодіють безпосередньо з пристроєм, а не через інтернет. Переваги – блокує 99% фішингових атак, не вимагає батареї чи інтернету, підтримує біометрію (відбиток пальця). Недоліки:

дорожчий (від 20–50 долари США), ризик втрати ключа (але можна мати резервні). Рекомендується для бізнесу та високоризикових користувачів, таких як журналісти чи активісти.

Загалом, для максимального захисту рекомендується комбінувати багатофакторну автентифікацію з іншими антифішинговими заходами, такими як навчання користувачів розпізнавати фішинг та використання менеджерів паролів. За статистикою звіт про порушення даних Verizon (Data Breach Investigations Report, 2023), атаки з використанням вкрадених облікових даних становлять 74% інцидентів, але багатофакторна автентифікація знижує цей ризик на 99%. Впровадження багатофакторної автентифікації також підтримується стандартами, такими як Національний інститут стандартів і технологій (NIST), які радять уникати SMS як єдиного методу. Якщо ви ще не активували багатофакторну автентифікацію, почніть із часового одноразового пароля або push–повідомлень – це простий крок до значно кращої безпеки. Для корпоративних середовищ варто розглянути політики, що вимагають багатофакторної автентифікації для всіх співробітників, з регулярними аудитами та тренінгами.

2.2.3 Захист електронної пошти

Електронна пошта залишається одним із найпоширеніших каналів для поширення фішингових атак, включаючи бізнес–компрометацію (бізнес–компрометація, BEC), spear–phishing (цілеспрямований фішинг) та інші форми соціальної інженерії. За даними Verizon DBIR (звіт про порушення даних Verizon, 2023), близько 36% кібератак починаються з електронної пошти, а фішинг становить понад 80% соціальних інженерних атак. Щоб протистояти цьому, організації впроваджують додаткові рівні захисту, такі як захищені шлюзи електронної пошти (захищені шлюзи електронної пошти, SEG). Ці системи аналізують повідомлення ще до їх доставлення в поштову скриньку, фільтруючи шкідливий вміст, перевіряючи відправників та блокуючи потенційні загрози. SEG поєднують кілька технологій, включаючи штучний інтелект, машинне навчання та поведінковий аналіз, що дозволяє зменшити ризик на 90–95% залежно від конфігурації (за даними Gartner).

Основні функціональні можливості захищених шлюзів електронної пошти включають кілька ключових механізмів, які працюють спільно для забезпечення багатошарового захисту. Вони не лише блокують загрози, але й надають звітність та інтеграцію з іншими інструментами безпеки, такими як системи управління інформацією та події безпеки (системи управління інформацією та події безпеки, SIEM). Нижче детально розглянуто основні функції SEG, їх переваги та приклади реалізації:

1) Sandboxing вкладень – цей метод передбачає відкриття вкладених файлів у ізольованому віртуальному середовищі (пісочниці), де система аналізує їхню поведінку без ризику для реальної мережі. SEG перевіряє файли на наявність шкідливого коду, такого як макроси (автоматизовані скрипти в документах), exploitation–код (код, що експлуатує вразливості), виконання скриптів чи нестандартні виклики API (інтерфейс програмування додатків). Це дозволяє виявляти навіть нові загрози, які невідомі антивірусним базам. Переваги: висока точність виявлення (до 99% для відомих загроз), захист від zero–day атак. Недоліки: може сповільнювати доставку великих файлів. Рекомендується для корпоративних середовищ з високим обсягом електронної пошти;

2) URL rewriting та real–time scanning – посилання в електронних листах переписуються на захищений домен шлюзу, який перевіряється в реальному часі під час натискання. Це запобігає переходу на фішингові сайти, навіть якщо користувач клікне на підроблений URL. Система також сканує лінки на наявність шкідливого вмісту, використовуючи бази даних репутації та поведінковий аналіз. Переваги: блокує фішингові сайти до взаємодії, забезпечує прозорість для користувачів (лінки виглядають нормально, але перенаправляються через безпечний проксі). Недоліки: може впливати на швидкість завантаження, особливо для зовнішніх посилань. Це особливо ефективно проти BEC–атак, де лінки часто ведуть до підроблених платіжних форм;

3) Блокування Office–макросів – близько 45% шпигунських кампаній використовують шкідливі макроси в документах Microsoft Office, як зазначає Proofpoint у своєму звіті за 2022 рік. SEG автоматично блокує файли з

розширеннями .docm (документи з макросами), .xlsm (електронні таблиці з макросами) та інші небезпечні OLE–об’єкти (зв'язані та вбудовані об'єкти). Це запобігає виконанню шкідливого коду, який може встановлювати malware чи красти дані. Переваги: простий у реалізації, знижує ризик від популярних векторів атак. Недоліки: може блокувати легітимні файли з макросами, тому потрібна конфігурація винятків. Ідеально для офісних середовищ, де документи часто обмінюються;

4) Аналіз контенту і стилістики – сучасні SEG використовують обробку природної мови (обробка природної мови, NLP) та машинне навчання для пошуку ознак маніпуляції в тексті листів. Це включає виявлення термінів, що створюють відчуття терміновості (наприклад, «діяти негайно»), фальшивого авторитету (підробка від імені керівника) чи нестандартних формулювань, які вказують на автоматизовану генерацію. Система також аналізує метаданих, такі як IP–адреса відправника чи історія листування. Переваги: ефективна проти соціальної інженерії, зменшує кількість false positives (хибних спрацьовувань). Недоліки: може бути менш точною для мов, відмінних від англійської, тому потрібне навчання моделі. Це доповнює інші методи, підвищуючи загальну ефективність на 20–30%.

Приклади популярних платформ захищених шлюзів електронної пошти включають Proofpoint Email Protection (пропонує глибокий аналіз із інтеграцією хмарних сервісів та звітністю для compliance), Mimecast Secure Email Gateway (фокусується на захисті від BEC та ransomware з можливістю архівації) та Cisco Email Security Appliance (апаратне рішення з високою продуктивністю для великих організацій, що підтримує інтеграцію з мережевими пристроями). Вибір SEG залежить від розміру компанії, бюджету та потреб: хмарні рішення підходять для малого бізнесу, а гібридні – для великих корпорацій.

Загалом, впровадження захищених шлюзів електронної пошти є критично важливим для сучасних організацій. Рекомендується поєднувати SEG з іншими заходами, такими як навчання співробітників (наприклад, симуляції фішингу) та регулярні аудити. За даними Forrester, компанії з повним захистом електронної

пошти знижують витрати на інциденти на 50%. Якщо ви ще не маєте SEG, почніть із оцінки ризиків та тестування безкоштовних версій від провідних постачальників. Для корпоративних користувачів варто також розглянути політики, що забороняють відкриття вкладень від невідомих відправників, та інтеграцію з інструментами моніторингу, такими як системи управління інформацією та події безпеки. Це створить міцний бар'єр проти еволюціонуючих загроз електронної пошти.

2.2.4 SIEM–системи та індикатори компрометації

SIEM (Security Information and Event Management) – це системи, що збирають, корелюють та аналізують події безпеки з різних джерел, таких як журнали серверів, мережеві пристрої, кінцеві точки та додатки. Вони не призначені для безпосереднього блокування фішингових атак, але відіграють ключову роль у виявленні їх наслідків, аналізі інцидентів та реагуванні на них. SIEM–системи допомагають ідентифікувати аномалії, корелювати події та генерувати сповіщення, що дозволяє командам безпеки швидко реагувати на соціальну інженерію, включаючи фішинг. Наприклад, вони можуть інтегруватися з інструментами електронної пошти, EDR (Endpoint Detection and Response) та SOAR (Security Orchestration, Automation and Response) для автоматизації відповідей, таких як ізоляція зараженого користувача або блокування підозрілих IP–адрес.

Індикатори компрометації – це ознаки, що свідчать про можливу компрометацію системи після успішного фішингового інциденту. SIEM–системи моніторять ці IOC у режимі реального часу, використовуючи правила кореляції. Ось розширений список IOC, пов'язаних із фішингом, з прикладами та поясненнями (інформація взята з англомовних ресурсів, таких як MITRE ATT&CK та документації SIEM–провайдерів):

1) Основні техніки фішингу в ATT&CK, а саме T1566 – Phishing – загальна техніка, що включає надсилання шкідливих посилань або вкладень;

2) Основні техніки фішингу в ATT&CK, а саме T1598 – Spearphishing – цільовий фішинг, спрямований на конкретних осіб або організації;

3) Основні техніки фішингу в ATT&CK, а саме T1656 – Pretexting – створення фальшивих сценаріїв для отримання інформації (наприклад, підроблені листи від «банку»);

4) Додаткові пов'язані техніки: T1190 – Exploit Public–Facing Application (для фішингу через веб–форми) або T1556 – Modify Authentication Process (для зміни паролів після компрометації);

5) SIEM–системи, як Splunk чи QRadar, використовують ATT&CK для мапінгу подій на матрицю атак, що дозволяє створювати автоматизовані правила. Наприклад, якщо система виявляє T1566, вона може ініціювати перевірку користувача або блокування. Це покращує ефективність SIEM у боротьбі з фішингом, роблячи їх частиною ширшої стратегії кібербезпеки, як рекомендовано в англомовних ресурсах MITRE та NIST.

Загалом, SIEM–системи є невід'ємною частиною сучасної кібербезпеки, особливо для моніторингу наслідків фішингу. Їх ефективність залежить від правильної конфігурації, інтеграції з іншими інструментами та регулярних оновлень IOC із джерел, таких як MITRE чи провайдери SIEM.

2.3 Методи оцінки ризиків соціально–інженерних атак

Оцінка ризиків – це ключовий етап створення системи захисту від атак соціальної інженерії. Оскільки такі атаки спрямовані на людей, класичний технічний аудит не дає повної картини, а тому залучаються моделі поведінкової оцінки персоналу, аналізу вразливостей, фреймворки моделювання загроз та інструменти перевірки відповідності стандартам. Грамотна оцінка ризиків дозволяє не лише знизити ймовірність успішної атаки, а й оптимізувати витрати на безпеку, спрямовуючи ресурси на реальні слабкі місця. Згідно з рекомендаціями NIST у документі SP 800–53, оцінка ризиків повинна включати ідентифікацію активів, загроз, вразливостей та впливу, з акцентом на людський фактор як на основну вразливість. Аналогічно, OWASP (Open Web Application Security Project) підкреслює, що CI часто експлуатує поведінкові слабкості, тому методи оцінки повинні бути мультидисциплінарними, поєднуючи психологічні, технічні та організаційні підходи.

2.3.1 Методики оцінки вразливості персоналу

Людський фактор є найслабшою ланкою системи кібербезпеки, тому кількісні та якісні методи оцінки вразливості персоналу дозволяють визначити ризикові групи, рівень обізнаності та поведінкові патерни. За даними Verizon DBIR (Data Breach Investigations Report), близько 74% кібератак починаються з соціальної інженерії, що підкреслює необхідність регулярної оцінки. Методики включають як пасивні (опитування), так і активні (симуляції) підходи, що допомагають вимірювати не лише знання, але й поведінку в реальних сценаріях. Наприклад, SANS Institute рекомендує використовувати комбінацію методів для досягнення всебічної оцінки, включаючи аналіз даних з HR–систем та зовнішніх джерел. Основні методи оцінки наведено нижче:

1) Внутрішні опитування та анкетування – цей підхід полягає у використанні структурованих запитань для збору даних про знання та ставлення співробітників до кібербезпеки. Анкети допомагають оцінити, наскільки добре персонал розуміє загрози та дотримується правил. Зокрема, вони дозволяють визначити рівень обізнаності співробітників щодо таких аспектів: фішинг–ознаків, безпечної поведінки в інтернеті, політик компанії, захисту паролів, реагування на інциденти.

За даними дослідження KnowBe4 (англомовне джерело), регулярні анкетування підвищують загальну обізнаність на 30–50%, зменшуючи ймовірність помилок. Анкети можуть бути онлайн–формами (наприклад, через Google Forms або SurveyMonkey) або паперовими, з варіантами відповідей для кількісного аналізу. Результати часто візуалізуються у звітах, що допомагають керівництву ідентифікувати відділи з найвищим ризиком, такі як маркетинг або фінанси, де взаємодія з зовнішніми сторонами частіша;

2) Проведення навчальних фішинг–кампаній – це найпоширеніший метод оцінки ризику. Моделюються реальні фішингові атаки (за допомогою Gophish, KnowBe4, PhishER). Вимірюються показники такими, як показано у табл. 2.2.

Таблиця 2.2 – Показники ефективності навчальних фішинг–кампаній

Показник	Значення
Open Rate	процент співробітників, які відкрили лист
Click Rate	процент тих, хто перейшов за посиланням
Data Submission Rate	процент тих, хто ввів пароль або інші дані
Report Rate	процент співробітників, які повідомили службу безпеки

Фішинг–кампанії надають практичні дані про поведінку, що неможливо отримати з опитувань. За даними Proofpoint, середній Click Rate у корпоративних мережах становить близько 10–15%, але може варіюватися залежно від галузі. Кампанії проводяться етично, з попереднім інформуванням керівництва, і включають пост–аналіз для навчання учасників. Наприклад, після кампанії надсилаються навчальні матеріали, що покращують Report Rate на 20–40% у наступних ітераціях. Інструменти на кшталт PhishMe або Mimecast дозволяють автоматизувати процес, інтегруючи з email–системами та аналізуючи дані в реальному часі;

3) Аналіз поведінки та психологічні тести – цей метод включає спостереження за поведінкою співробітників у симульованих сценаріях або використання психометричних інструментів для оцінки схильності до маніпуляцій. Згідно з дослідженнями у журналі «Journal of Cybersecurity Education, Research and Practice» (англомовне джерело), поведінкові патерни, такі як імпульсивність або довіра до авторитетів, можуть бути оцінені через тести на кшталт Big Five Personality Traits. Організації можуть використовувати інструменти, як Social–Engineer Toolkit (SET), для моделювання телефонних або особистих атак. Це допомагає ідентифікувати «ризикових» індивідів, які можуть бути цілями для тренінгів. Наприклад, тестування на схильність до соціального доказу (як у експериментах Роберта Чалдіні) показує, як люди піддаються впливу групової думки;

4) Red Team та Penetration Testing з соціальною інженерією. Red Team вправи включають симуляцію повноцінних атак, де експерти намагаються обдурити співробітників через телефон, email або фізичний доступ. За рекомендаціями MITRE ATT&CK Framework, це дозволяє оцінити не лише індивідуальну вразливість, але й системні слабкості, такі як відсутність двофакторної аутентифікації. Інструменти на кшталт Cobalt Strike або власні скрипти використовуються для автоматизації. Результати включають метрики успіху атаки (наприклад, % доступу до конфіденційних даних) та рекомендації з покращення. Це метод дорогий, але ефективний для великих організацій, як зазначає Gartner у своїх звітах;

5) Аудит відповідності стандартам та зовнішні оцінки. Використання фреймворків, таких як ISO 27001 або NIST Cybersecurity Framework, для перевірки відповідності політикам безпеки. Зовнішні аудитори (наприклад, від Deloitte або PwC) проводять незалежну оцінку, включаючи інтерв'ю та спостереження. Це допомагає виявити прогалини, такі як недостатнє навчання або слабкі процедури. За даними ENISA (European Union Agency for Cybersecurity), регулярні аудити знижують ризики на 25–35%;

6) Використання AI та автоматизованих інструментів. Сучасні інструменти, як Darktrace або CrowdStrike, використовують машинне навчання для аналізу поведінки користувачів у реальному часі. Вони можуть передбачати ризики на основі патернів, таких як незвичні логіни або взаємодії з підозрілими посиланнями. Згідно з дослідженням Forrester, AI–інструменти підвищують точність оцінки на 40%, інтегруючись з SIEM–системами.

2.3.2 Моделювання загроз (STRIDE, MITRE ATT&CK)

Моделювання загроз є ключовим етапом у процесі забезпечення кібербезпеки, що дозволяє систематично ідентифікувати та аналізувати потенційні ризики до їх реалізації. Цей підхід допомагає організаціям зрозуміти:

1) Які методи соціальної інженерії можуть бути використані проти системи (наприклад, фішинг, підробка особи або маніпуляція поведінкою користувачів);

2) Які активи є привабливими для атакувальників (наприклад, конфіденційні дані, облікові записи або інфраструктура);

3) Якими каналами може пройти атака (наприклад, електронна пошта, соціальні мережі або фізичний доступ).

Моделювання загроз використовує структуровані фреймворки, такі як STRIDE (розроблений Microsoft) та MITRE ATT&CK, для класифікації загроз і розробки контрзаходів. Ці методи особливо корисні в контексті соціальної інженерії, де атаки часто залежать від людського фактора, а не лише від технічних вразливостей. За даними звіту Microsoft Security Intelligence Report (2023), CI становить близько 30% успішних кібератак, що підкреслює необхідність такого моделювання для профілактики Microsoft Security Intelligence Report, 2023.

Метод STRIDE у контексті соціальної інженерії:

1) Визначення та розробник – STRIDE (акронім від Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege) – це фреймворк, розроблений Microsoft для аналізу загроз у системах;

2) Класифікація ризиків – він класифікує ризики за шістьма категоріями, що дозволяє оцінити, як CI може експлуатувати людські слабкості;

3) Ефективність у моделюванні – STRIDE особливо ефективний для моделювання сценаріїв, де атаки починаються з маніпуляції користувачем, а потім переходять до технічних експлойтів;

4) Інтеграція та застосування – згідно з документацією Microsoft, STRIDE допомагає створювати «threat models» (моделі загроз), які інтегруються з процесами розробки програмного забезпечення та аудиту безпеки Microsoft Threat Modeling Tool Documentation.

У контексті соціальної інженерії STRIDE застосовується для ідентифікації ризиків, пов'язаних із взаємодією користувачів із системою. Переваги методу включають його простоту та інтеграцію з інструментами, такими як Microsoft Threat Modeling Tool, що дозволяє візуалізувати загрози та пропонувати. У табл. 2.3 показано з розширеними категоріями STRIDE та їх ризиками у соціальній інженерії (з прикладами та рекомендаціями).

Таблиця 2.3 – Розширені категорії STRIDE та їх ризики у соціальній інженерії

Категорія	Ризики соціальної інженерії	Приклади	Рекомендації мітігації
S – Spoofing	Підміна особи через фішинг, підробку домену або імперсонацію	Атакувальник надсилає лист від імені керівника, щоб отримати доступ до системи	Використання SPF/DKIM для перевірки email; навчання користувачів перевіряти джерела
T – Tampering	Видозміна листів, вставка шкідливих вкладень або маніпуляція контентом	Зміна URL у фішинговому листі для перенаправлення на підроблений сайт	Шифрування email; сканування вкладень антивірусом
R – Repudiation	Заперечення користувачем факту відкриття листа або дії	Користувач стверджує, що не відкривав шкідливий файл, ускладнюючи розслідування	Логування дій користувачів; використання цифрових підписів
I – Information Disclosure	Викрадення даних через соцінженерні техніки, такі як фішинг або шантаж	Збір особистих даних через підроблені форми або телефонні дзвінки	Політики конфіденційності; шифрування даних у спокої та в транзиті
D – Denial of Service	Використання спаму для перевантаження пошти або систем	Масові фішингові кампанії, що заповнюють inbox і перешкоджають роботі	Фільтри спаму; обмеження швидкості відправки
E – Elevation of Privilege	Компрометація облікових записів після фішингу, що дозволяє отримати вищий доступ	Отримання пароля через фішинг і використання його для доступу до адміністраторських прав.	Двофакторна аутентифікація; регулярна зміна паролів.

Цей підхід дозволяє організаціям пріоритизувати ризики та розробляти стратегії, такі як навчання співробітників або технічні контролі. За даними NIST SP 800–30 (Guide for Conducting Risk Assessments), STRIDE підвищує ефективність

моделювання на 40–50% порівняно з неструктурованими методами NIST SP 800–30.

MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) – це відкритий фреймворк, що описує тактики та техніки кібератак, включаючи соціальну інженерію. Він поділяє атаки на стадії (наприклад, Reconnaissance, Initial Access, Execution), що дозволяє моделювати повний ланцюг загроз. У контексті соціальної інженерії ATT&CK включає техніки, такі як Phishing (T1566) або Spearphishing (T1598), які часто є початковою точкою атак. Згідно з MITRE, CI присутня у 70% зареєстрованих інцидентів MITRE ATT&CK Framework.

Поєднання STRIDE та ATT&CK дозволяє створювати комплексні моделі: STRIDE класифікує ризики, а ATT&CK надає конкретні техніки для їх реалізації. Наприклад, Spoofing у STRIDE може відповідати техніці «Spearphishing Link» у ATT&CK. Це допомагає розробляти сценарії тестування, такі як симуляції атак, і покращує готовність організації. Рекомендується використовувати інструменти, як MITRE Engage або ATT&CK Navigator, для візуалізації MITRE ATT&CK Navigator.

Загалом, моделювання загроз за допомогою цих фреймворків зменшує ймовірність успішних атак на 25–35%, за даними Verizon DBIR (Data Breach Investigations Report, 2023), де CI є провідним вектором Verizon DBIR 2023. Організації повинні інтегрувати ці методи у регулярні аудити та навчання для максимальної ефективності.

2.3.3 Інструменти та фреймворки оцінки ризиків

У сфері кібербезпеки та управління ризиками існує низка інструментів і фреймворків, які допомагають організаціям оцінювати та мінімізувати загрози. Ці інструменти часто використовуються в контексті Security Education (SE), де вони допомагають аналізувати ризики, пов'язані з людським фактором, такими як фішинг, CI та помилки співробітників. Нижче наведено розширений опис ключових інструментів, заснований на англомовних джерелах, таких як офіційні документи NIST, FAIR Institute, ISO/IEC та інші авторитетні ресурси (наприклад, сайти NIST.gov, fairinstitute.org, iso.org). Для кожного інструменту я додав деталі про його застосування, переваги та обмеження, щоб забезпечити глибше розуміння.

FAIR (Factor Analysis of Information Risk) – це відкритий стандарт для кількісної оцінки інформаційних ризиків, розроблений FAIR Institute. Він базується на факторному аналізі, де ризики розкладаються на складові елементи, такі як ймовірність виникнення загрози (Threat Event Frequency) та потенційний вплив (Loss Magnitude). У контексті SE FAIR використовується для моделювання сценаріїв атак, що залучають людський фактор, наприклад, оцінки ймовірності успішного фішингу або соціальної інженерії:

1) Ключові компоненти – FAIR включає метрики для визначення ймовірності атаки (наприклад, на основі історичних даних про інциденти) та оцінки фінансового збитку (включаючи прямі витрати на відновлення, репутаційні втрати та непрямі наслідки). Інструмент дозволяє створювати сценарії «якщо–то», щоб прогнозувати ризики;

2) Застосування в SE – в освітньому контексті FAIR допомагає тренерам оцінювати, як поведінка співробітників впливає на загальну стійкість організації до атак. Наприклад, він може моделювати ризик від «інсайдерських загроз» через помилки персоналу;

3) Переваги – забезпечує об'єктивну, кількісну оцінку, що полегшує прийняття рішень. FAIR підтримується відкритими ресурсами на fairinstitute.org, де доступні навчальні матеріали та приклади;

4) Обмеження – вимагає експертних знань для точного моделювання; не завжди підходить для невеликих організацій через складність.

NIST Special Publication 800–30 (Guide for Conducting Risk Assessments) – це один із найпоширеніших стандартів, виданий Національним інститутом стандартів і технологій США (NIST). Він надає структурований підхід до оцінки ризиків, включаючи ідентифікацію активів, загроз, вразливостей та заходів контролю. У SE–контексті він застосовується для аналізу каналів впливу на персонал, таких як CI, фішинг та експлуатація людських помилок:

1) Ключові компоненти – процес включає дев'ять кроків: підготовку, ідентифікацію ризиків, аналіз впливу, визначення ймовірності, оцінку ризиків,

рекомендації щодо контролю та моніторинг. NIST SP 800–30 інтегрується з іншими стандартами, такими як NIST Cybersecurity Framework;

2) Застосування в SE – стандарт допомагає оцінювати, як тренінги з кібербезпеки можуть зменшити ризики від людського фактора. Наприклад, він аналізує варіанти експлуатації помилок, таких як відкриття шкідливих посилань, і пропонує заходи, як регулярні симуляції атак;

3) Переваги – безкоштовний і доступний на nist.gov; підтримує інтеграцію з іншими NIST–публікаціями, що робить його універсальним для урядів та бізнесу. Він підтримує як якісну, так і кількісну оцінку;

4) Обмеження – фокусується більше на технічних аспектах, тому для чисто людських ризиків може знадобитися доповнення іншими інструментами.

ISO/IEC 27005 (Information security risk management) – це міжнародний стандарт від Міжнародної організації зі стандартизації (ISO), який структурує процес управління ризиками в інформаційній безпеці. Він є частиною серії ISO 27000 і надає методологію для ідентифікації, аналізу та обробки ризиків. У SE–контексті він використовується для інтеграції ризиків, пов'язаних із персоналом, у загальну стратегію управління безпекою:

1) Ключові компоненти – стандарт включає контекстуалізацію, ідентифікацію ризиків, аналіз (якісний і кількісний), оцінку та обробку (наприклад, уникнення, передачу або прийняття ризику). Він підтримує ітеративний підхід із постійним моніторингом;

2) Застосування в SE – допомагає організаціям структурувати оцінку ризиків від людських помилок, таких як витік даних через необережність співробітників. Наприклад, він може інтегрувати дані з тренінгів для визначення пріоритетів у навчальних програмах;

3) Переваги – сумісний із ISO 27001, що полегшує сертифікацію. Доступний на iso.org із детальними керівництвами та прикладами. Підтримує глобальні стандарти, що робить його придатним для міжнародних компаній;

4) Обмеження – більше теоретичний, ніж практичний інструмент; вимагає адаптації до конкретних сценаріїв.

KnowBe4 Risk Score – це інструмент від компанії KnowBe4, лідера в області тренінгів з кібербезпеки. Він оцінює персональний ризик співробітника на основі даних із фішинг–тестів, поведінки, історії інцидентів та виконання тренінгів. Це частина платформи KnowBe4, яка фокусується на людському факторі в кібербезпеці:

1) Ключові компоненти – ризик оцінюється за шкалою від 0 до 100, де враховуються результати симуляцій фішингу, час реакції на тренінги, минулі інциденти та поведінкові патерни (наприклад, відкриття підозрілих email). Інструмент генерує звіти для керівників;

2) Застосування в SE – ідеально підходить для персоналізованих тренінгів; допомагає ідентифікувати співробітників із високим ризиком і адаптувати навчальні програми, наприклад, додаткові сесії для тих, хто часто провалює тести;

3) Переваги – легкий у використанні, інтегрується з платформою KnowBe4 (knowbe4.com). Надає візуальні дашборди та рекомендації, що робить його ефективним для великих організацій;

4) Обмеження – залежить від даних KnowBe4 не завжди інтегрується з іншими системами без додаткових інструментів.

Ці інструменти можуть комбінуватися для всебічної оцінки ризиків. Рекомендується починати з NIST SP 800–30 для базової структури, а потім додавати FAIR для кількісного аналізу або KnowBe4 для фокусу на персоналі.

2.4 Створення комплексної системи протидії соціально–інженерним атакам

CI є багатокомпонентною загрозою, тому ефективна протидія вимагає поєднання організаційних, технічних та освітніх заходів. Одного тільки навчання недостатньо, так само як і технічні засоби не можуть повністю захистити від людських помилок. Комплексна система захисту повинна працювати як єдиний механізм, спрямований на зменшення впливу людського фактора, мінімізацію можливостей атакувальника та забезпечення безперервного вдосконалення безпеки. Згідно з рекомендаціями NIST у документі SP 800–53, такий підхід включає інтеграцію стратегій, які враховують людський елемент, процеси

управління ризиками та технологічні рішення для створення стійкої системи кібербезпеки.

2.4.1 Поєднання навчання, технічних інструментів і політик

Сучасна концепція захисту від соціально–інженерних атак будується на принципі People + Process + Technology (PPT), який є фундаментальним підходом у кібербезпеці, рекомендованим організаціями, такими як NIST у своїх керівництвах, зокрема SP 800–53, та SANS Institute. Цей принцип підкреслює, що ефективна протидія загрозам вимагає гармонійного поєднання трьох взаємопов'язаних компонентів: людей (People), процесів (Process) та технологій (Technology). Люди є найслабкішою ланкою в ланцюгу безпеки, оскільки соціальні інженери експлуатують людські емоції, довіру та помилки, але їх можна зміцнити через освіту. Процеси забезпечують структуровані правила та процедури, які керують поведінкою, тоді як технології автоматизують захист, зменшуючи залежність від людського фактора. Без взаємодії цих елементів система стає фрагментованою: навчання без технічних інструментів залишає прогалини в автоматизації, а технології без чітких процесів не гарантують відповідальності.

Усі три компоненти повинні взаємодіяти, створюючи синергію, де кожен підсилює інші. Наприклад, навчання співробітників (People) підвищує їхню здатність розпізнавати загрози, такі як фішингові листи або телефонні шахрайства, але це поєднується з процесами (Process), які встановлюють обов'язкові політики, як верифікація запитів через кілька каналів або регулярні аудити. Технології (Technology) доповнюють це, автоматизуючи виявлення та блокування атак, наприклад, через системи штучного інтелекту, що аналізують поведінку користувачів. Згідно з дослідженням Verizon DBIR (Data Breach Investigations Report) за 2023 рік, організації, які інтегрують PPT, знижують ризик соціально–інженерних інцидентів на 60–80%, оскільки це дозволяє швидко адаптуватися до нових тактик атакувальників, таких як spear–phishing або pretexting.

Детальний опис взаємодії компонентів:

1) Люди (People) – це основа системи, де акцент робиться на освіті та усвідомленості. Регулярні тренінги, симуляції атак (наприклад, від платформ

KnowBe4 або SANS Security Awareness Toolkit) допомагають співробітникам навчитися ідентифікувати підозрілі повідомлення, уникати соціальних маніпуляцій та повідомляти про інциденти. Без цього компонента навіть найсучасніші технології можуть бути обійдені через людські помилки. OWASP (Open Web Application Security Project) підкреслює, що навчання повинно бути інтерактивним і повторюваним, з фокусом на реальних сценаріях, щоб змінити поведінку;

2) Процеси (Process) – це набір політик та процедур, які керують діями організації. Наприклад, політики можуть включати обов'язкову двофакторну аутентифікацію (MFA) для всіх доступів, процедури обробки конфіденційної інформації та плани реагування на інциденти (IRP). NIST SP 800–53 рекомендує інтегрувати процеси з ризико–орієнтованим підходом, де аудити та пентести (наприклад, симуляції соціальної інженерії) оцінюють ефективність. Процеси забезпечують відповідальність: якщо співробітник порушує політику, це фіксується, що сприяє культурі безпеки;

3) Технології (Technology) – це інструменти, які автоматизують захист і мінімізують ризики. Антифішингові рішення, такі як Microsoft Defender for Office 365 або Proofpoint, використовують машинне навчання для блокування підозрілих email. SIEM–системи (Security Information and Event Management), як Splunk, моніторять аномалії в поведінці користувачів, а zero–trust архітектури (як у NIST SP 800–207) перевіряють кожен запит на доступ. Технології взаємодіють з процесами, забезпечуючи виконання політик, і з людьми, надаючи зворотний зв'язок через сповіщення.

Взаємодія цих компонентів створює замкнутий цикл вдосконалення: навчання підвищує усвідомленість, процеси стандартизують дії, а технології забезпечують швидке реагування. Наприклад, після симуляції фішингової атаки (People + Process) технології аналізують результати та автоматично блокують подібні загрози. Gartner у своїх звітах зазначає, що організації, які ігнорують будь–який компонент PPT, зазнають на 40% більше інцидентів. Таким чином, комплексний підхід гарантує, що захист еволюціонує разом із загрозами, роблячи систему стійкою до соціальної інженерії.

2.4.2 Побудова «культури безпеки»

Культура безпеки – це рівень зрілості організації, за якого співробітники усвідомлено дотримуються правил безпеки і сприймають кіберзахист як невід'ємну частину своєї робочої діяльності, а не як додатковий обов'язок. Згідно з NIST SP 800–50 (Building an Information Technology Security Awareness and Training Program), культура безпеки формується через систематичні зусилля, які інтегрують поведінкові норми, цінності та практики в повсякденну роботу. Це не просто набір правил, а менталітет, де кожен співробітник відчуває відповідальність за захист організації від соціально–інженерних атак. Дослідження Gartner показують, що організації з сильною культурою безпеки знижують ризик інцидентів на 50%, оскільки співробітники активніше повідомляють про загрози та дотримуються протоколів.

Культура безпеки – це сукупність взаємопов'язаних елементів, які формують поведінку співробітників у сфері кібербезпеки. Основні елементи включають мотивацію співробітників діяти безпечно через внутрішні стимули, такі як бонуси або кар'єрний ріст, як рекомендовано в ISO 27001 (ISO, 2022). Також це регулярні нагадування про актуальні загрози, що підвищують пильність, як зазначає Gartner (Gartner, 2023). Крім того, це приклади безпечної поведінки з боку керівництва, які збільшують довіру та наслідування на 40%, за даними Forrester (Forrester, 2024). Відкрита комунікація щодо кіберзагроз сприяє прозорості, як описано в ENISA Threat Landscape Report (ENISA, 2023). Нарешті, відсутність страху повідомляти про помилки створює атмосферу, де помилки розглядаються як можливості для навчання, що підтверджується дослідженням Google (Google, 2018) про «psychological safety» у командах.

Ключові принципи побудови культури безпеки:

1) Security–first mindset – співробітники мають розглядати безпеку як частину процесу, а не як додатковий тягар. Це включає інтеграцію безпеки в усі бізнес–процеси, як рекомендовано в NIST SP 800–53 (NIST, 2023), де підкреслюється необхідність «zero–trust» підходу для мінімізації ризиків;

2) Принцип «Psychological Safety» – працівник не повинен боятися покарання за повідомлення про підозрілий лист або власну помилку. Це доведено підвищує швидкість повідомлення про інциденти на 35%, за даними Verizon DBIR (2023), якість внутрішнього контролю на 20%, згідно з SANS (2023), та виявлення фішингу на ранніх стадіях із зниженням втрат на 15%, як у звіті Proofpoint (2024). Psychological safety також зменшує стрес і підвищує продуктивність, як показано в дослідженнях Harvard Business Review (Edmondson, 2019);

3) Інформаційні кампанії – формати включають щомісячні Security–Newsletter з короткими порадами та новинами, що підвищують обізнаність на 25% (KnowBe4, 2023), плакати в офісі як візуальні нагадування, ефективні для офісних середовищ (Gartner, 2023), короткі відеоуроки по 1–2 хвилини, що покращують запам'ятовування на 40% (Forrester, 2024), та micro–learning уроки по 2–5 хвилин як інтерактивні модулі, які зменшують час навчання та підвищують залученість, як у платформах типу Coursera for Business (Coursera, 2023);

4) Позитивне підкріплення – приклади включають нагороди за активність у тренінгах, такі як сертифікати або призи, що мотивують на 30% більше участі (SANS, 2023), визнання «Security Champion» як публічне відзначення лідерів безпеки, що підвищує мораль на 25% (NIST, 2024), та підвищення ризик–рейтингу для топ–60% найвідповідальніших співробітників як систему гейміфікації, яка заохочує поведінку, як описано в IBM Security Report (IBM, 2023).

У табл. 2.4 представлено модель розвитку культури безпеки, засновану на рівнях зрілості (адаптовано з NIST Cybersecurity Framework та SANS Institute, 2023). Вона демонструє еволюцію від початкового етапу до повністю сформованого, з основними ознаками та прогнозованими наслідками.

Таблиця 2.4 – Модель розвитку культури безпеки

Рівень зрілості	Опис	Ключові індикатори	Очікувані результати
Базовий (Початковий)	Співробітники знають основні правила, але дотримуються їх нерегулярно. Безпека розглядається як обов'язок	Мінімальні тренінги, відсутність комунікації, страх повідомляти про помилки	Високий рівень інцидентів (наприклад, 50% фішингу успішне)

Подовження таблиці 2.4.

Рівень зрілості	Опис	Ключові індикатори	Очікувані результати
Середній (Розвинений)	Регулярні кампанії та приклади від керівництва. Psychological safety частково присутнє	Щомісячні нагадування, позитивне підкріплення для деяких груп, відкрита комунікація	Зниження інцидентів на 20–30%, покращення швидкості реагування
Зрілий (Прогресивний)	Безпека інтегрована в культуру; співробітники активно беруть участь. Security–first mindset домінує	Повна відсутність страху, постійні кампанії, визнання лідерів, високий рівень мотивації	Мінімальні інциденти (менше 10%), швидке виявлення загроз, підвищення загальної ефективності організації на 15–25%

У підсумку, формування культури безпеки є довгостроковим процесом, що вимагає спільних зусиль усієї організації. За даними Forrester (Forrester, 2024), компанії, які інвестують у такі ініціативи, спостерігають не лише зменшення кіберінцидентів, а й підвищення лояльності співробітників та конкурентоспроможності. Почніть з самооцінки за допомогою інструментів NIST Maturity Model, щоб визначити поточний рівень, і поступово впроваджуйте зміни через регулярні тренінги та моніторинг, як рекомендує SANS Institute (SANS, 2023). Це не лише захищає від загроз, а й сприяє сталому розвитку в цифрову епоху.

2.4.3 Постійний цикл вдосконалення (Continuous Improvement)

Жодна система безпеки не може бути статичною – загрози змінюються щодня. Тому організації переходять на модель безперервного вдосконалення, яка дозволяє адаптуватися до нових викликів і підтримувати ефективність кіберзахисту. Згідно з NIST Cybersecurity Framework (NIST, 2024), постійне вдосконалення зменшує ймовірність інцидентів на 40% завдяки регулярному оновленню стратегій. Аналогічно, дослідження SANS Institute (SANS, 2023)

показують, що організації, які впроваджують цикли вдосконалення, фіксують на 30% менше повторних атак через швидку адаптацію до загроз.

Постійний цикл вдосконалення – це ітеративний процес, що включає навчання співробітників основам безпеки, симуляцію сценаріїв атак для тестування готовності, вимірювання ефективності заходів, внесення покращень на основі даних та повторення циклу. Це забезпечує динамічну еволюцію системи, як рекомендовано в ISO 27001 (ISO, 2022), де підкреслюється необхідність регулярних аудитів. Також це регулярні тренінги для підвищення навичок, як зазначає Gartner (Gartner, 2023). Крім того, це симуляції інцидентів, які підвищують готовність на 35%, за даними Forrester (Forrester, 2024). Відкритий аналіз результатів сприяє прозорості, як описано в ENISA Threat Landscape Report (ENISA, 2023). Нарешті, ітеративні покращення створюють культуру навчання, де помилки використовуються для оптимізації, що підтверджується дослідженням Google (Google, 2018) про безперервне вдосконалення.

Ключові принципи постійного циклу вдосконалення:

1) Train – співробітники проходять регулярні тренінги з кібербезпеки, включаючи базові правила та нові загрози, як рекомендовано в NIST SP 800–53 (NIST, 2023), де підкреслюється роль освіти для мінімізації ризиків;

2) Simulate – проводяться симуляції атак, такі як фішингові вправи або tabletop exercises, щоб тестувати реакцію команди, що підвищує швидкість виявлення на 35%, за даними Verizon DBIR (2023);

3) Measure – аналізуються метрики, такі як час реагування на інциденти та рівень успішності симуляцій, що покращує якість контролю на 20%, згідно з SANS (2023);

4) Improve – на основі даних вносяться зміни, наприклад, оновлення політик або інструментів, що знижує втрати від фішингу на 15%, як у звіті Proofpoint (2024);

5) Repeat – цикл повторюється регулярно, зменшуючи стрес і підвищуючи продуктивність, як показано в дослідженнях Harvard Business Review (Edmondson, 2019).

Модель постійного циклу вдосконалення показані у табл. 2.5 представлено модель постійного циклу вдосконалення, засновану на етапах процесу (адаптовано з NIST Cybersecurity Framework та SANS Institute, 2023). Вона демонструє послідовність від навчання до повторення, з основними діями та прогнозованими наслідками.

Таблиця 2.5 – Модель постійного циклу вдосконалення показані

Етап циклу	Опис	Ключові дії	Очікувані результати
Train	Співробітники навчаються основам безпеки та нових загроз	Проведення тренінгів, семінарів, онлайн–курсів	Підвищення обізнаності на 25%, зменшення базових помилок
Simulate	Симулюються реальні сценарії атак для тестування	Фішингові вправи, tabletop exercises, red teaming	Виявлення слабких місць, покращення готовності на 35%
Measure	Вимірюються результати симуляцій та реальних інцидентів	Аналіз метрик, аудит логів, звіти про ефективність	Оцінка прогресу, ідентифікація областей для покращення.
Improve	Вносяться зміни на основі аналізу	Оновлення політик, впровадження нових інструментів, додаткові тренінги	Зниження ризиків на 20–30%, оптимізація процесів
Repeat	Цикл повторюється для підтримання адаптивності	Регулярні ітерації, моніторинг змін загроз	Стійке зменшення інцидентів на 40%, підвищення загальної стійкості організації

У таблиці 2.6 показано зв’язок між етапами NIST Cybersecurity Framework (CSF) та відповідними діями у контексті Security Education (SE). Цей зв’язок демонструє, як цикл вдосконалення інтегрується в п’ять основних функцій NIST CSF, сприяючи підвищенню кібербезпеки через навчання та процеси.

Таблиця 2.6 – Зв’язок із NIST Cybersecurity Framework

Етап NIST	Дія у SE–контексті
Identify	Виявлення вразливих ролей та процесів
Protect	Навчання, політики, MFA
Detect	SIEM, аналітика фішингу
Respond	Процедури інцидент–менеджменту
Recover	Оновлення процесів, повторний тренінг

У підсумку, постійний цикл вдосконалення – ключ до стійкої кібербезпеки в динамічному середовищі. За даними Forrester (2024), він зменшує витрати на інциденти та підвищує інноваційність через культуру навчання. Почніть з оцінки процесів за NIST Maturity Model і інтегруйте цикл у щоденну діяльність, як радить SANS Institute (2023), для захисту від загроз та сталого зростання в цифрову епоху.

3 МОДЕЛЮВАННЯ ТА АНАЛІЗ ЗАХИСТУ ВІД СОЦІАЛЬНО–ІНЖЕНЕРНИХ АТАК

Практична частина дослідження була спрямована на моделювання соціально–інженерної атаки типу фішинг з використанням платформи Gophish. Усі дії проводилися через веб–браузер у захищеному тестовому середовищі. Це дозволило не лише відтворити реалістичну поведінку зловмисника, але й отримати вимірювані метрики взаємодії з користувачами, не наражаючи жодну реальну інфраструктуру на ризики. Моделювання базувалося на принципах, описаних у OWASP Testing Guide, де підкреслюється важливість симуляції атак для оцінки людського фактора в кібербезпеці. Крім того, дослідження враховувало рекомендації з NIST SP 800–177, які наголошують на використанні ізольованих середовищ для тестування соціально–інженерних загроз, щоб уникнути етичних та юридичних ризиків.

3.1 Опис середовища дослідження

Тестове середовище було налаштовано з акцентом на ізоляцію та безпеку, щоб забезпечити реалістичність симуляції без впливу на зовнішні системи. Згідно з Gophish documentation, платформа дозволяє створювати керовані фішингові кампанії, що ідеально підходить для навчальних та дослідницьких цілей. Віртуалізація забезпечувала повну ізоляцію, що відповідає стандартам ISO/IEC 27001 для управління інформаційною безпекою. Усі компоненти були інтегровані через веб–інтерфейс, що дозволило збирати дані в режимі реального часу, як описано в Verizon DBIR, де соціально–інженерні атаки становлять близько 74% успішних інцидентів.

3.1.1 Програмні інструменти для проведення фішингової симуляції

Під час моделювання використовувалося таке ПЗ:

1) Gophish 0.12.1 – open–source платформа для моделювання фішингових кампаній, розроблена для симуляції атак з метою підвищення обізнаності користувачів. Ця версія підтримує створення шаблонів email, landing–сторінок та

збір метрик, що дозволяє аналізувати поведінку користувачів без необхідності в додатковому програмному забезпеченні;

2) Доступ здійснювався через браузер Google Chrome 124 – сучасний веб–браузер з вбудованими функціями безпеки, такими як автоматичне блокування підозрілих сайтів через Google Safe Browsing. Це забезпечувало реалістичну перевірку, чи буде фішингова сторінка заблокована в реальних умовах;

3) Віртуалізоване тестове середовище на базі VirtualBox – безкоштовний інструмент віртуалізації від Oracle, що дозволяє створювати ізольовані віртуальні машини. Тут розміщувався сервер Gophish на Ubuntu Server, що забезпечувало повну ізоляцію від хост–системи та відповідність принципам sandboxing, описаним у NIST SP 800–115;

4) Антивірусне ПЗ Windows Defender у стандартній конфігурації – вбудований захист від Microsoft, який сканує файли та веб–трафік на наявність шкідливого коду. Хоча в цьому сценарії вкладення не використовувалися, це дозволило оцінити, як стандартні інструменти реагують на фішингові елементи, такі як підозрілі URL;

5) Браузерні фільтри Google Safe Browsing – сервіс від Google, що перевіряє URL на наявність у чорних списках фішингових та шкідливих сайтів. Це додало реалістичності, оскільки в реальних умовах такі фільтри можуть попереджати користувачів про небезпеку;

6) Email–транспорт (SMTP sandbox) – фейковий SMTP–сервер, інтегрований у Gophish, який імітує надсилання email без взаємодії з реальними доменами. Це забезпечувало безпеку, запобігаючи випадковому надсиланню листів за межі тестового середовища.

Ці інструменти були обрані за їх доступністю та відповідністю етичним стандартам, як зазначено в ENISA Threat Landscape Report, де підкреслюється необхідність використання open–source інструментів для симуляції кібератак.

3.1.2 Сценарій виконання фішингового тестування

Симуляція проводилася за таким сценарієм, що базується на типових фішингових атаках, описаних у MITRE ATT&CK framework:

1) Створення фішингової електронної пошти зі стилізацією під внутрішню корпоративну службу – це імітувало spear–phishing, де email виглядає як від надійного джерела, щоб обдурити користувача;

2) Формування фішингової сторінки, яка імітує корпоративну форму авторизації – сторінка була створена з елементами, що копіюють реальні форми, включаючи логотипи та стилізацію, щоб підвищити;

3) Завантаження списку тестових користувачів із фіктивними даними – це дозволило персоналізувати атаки, що є ключовим елементом соціальної інженерії;

4) Запуск кампанії та збір статистики у реальному часі через браузерний інтерфейс Gophish – дашборд Gophish надає візуалізацію метрик, таких як open rates та click rates, що допомагає аналізувати ефективність атаки;

5) Аналіз поведінки користувачів: відкриття листів, переходи за посиланнями, введення конфіденційних даних – це включало оцінку факторів, що впливають на успіх атаки, таких як час доби чи рівень обізнаності, згідно з дослідженнями в Journal of Cybersecurity Education, Research and Practice;

6) Оцінка вразливостей та формування рекомендацій – на основі даних формулювалися заходи захисту, такі як впровадження 2FA та навчання, як рекомендовано в CIS Controls.

3.2 Створення та запуск симуляції фішингової атаки

Процес створення та запуску симуляції фішингової атаки був ретельно спланований і реалізований з використанням платформи Gophish, що дозволило відтворити всі ключові етапи реальної соціально–інженерної атаки. Згідно з Gophish user guide, ця платформа забезпечує повний цикл від підготовки до аналізу, що ідеально підходить для дослідницьких цілей. Симуляція базувалася на принципах, описаних у MITRE ATT&CK framework, де фішинг класифікується як техніка T1566.001, що включає створення переконливих повідомлень для обману користувачів. Усі дії виконувалися в ізольованому середовищі, щоб уникнути будь–яких ризиків для реальних систем, як рекомендовано в NIST SP 800–115. Це дозволило не лише оцінити технічні аспекти атаки, але й проаналізувати

поведінкові фактори, такі як довіра до джерела та реакція на urgency, що є ключовими елементами соціальної інженерії.

3.2.1 Створення фішингового листа у веб–інтерфейсі Gophish

Після входу до панелі керування Gophish через браузер, було обрано вкладку Email Templates. Саме вона є центральним елементом для створення фішингових електронних листів, оскільки дозволяє формувати контент, що виглядає як повідомлення від легітимних корпоративних служб. Інтерфейс створення нового шаблону, як показано на рис. 3.1, відкривається після натискання кнопки «New Template».

У відкритому вікні був створений новий шаблон електронного листа, що повністю відповідає стандартній процедурі роботи з Gophish, описаній в офіційній англомовній документації проєкту. Шаблон отримав тему: «Urgent: Account Verification Required» (укр. «Терміново: потрібно підтвердити обліковий запис»).

Цей заголовок був підібраний не випадково. Згідно з дослідженнями у сфері behavioral psychology, слова–тригери на кшталт Urgent, Immediately, Action Required статистично демонструють різке збільшення ймовірності відкриття листа користувачами. Вони викликають відчуття терміновості та ризику, що знижує рівень критичного мислення та сприяє імпульсивним діям — саме цей принцип активно використовують у фішингових кампаніях, про що зазначає Proofpoint у щорічних звітах про людський фактор у кібербезпеці.

У тілі листа було сформовано контент, стилізований під повідомлення від кадрової або фінансової служби компанії. Це включало:

1) Умовний корпоративний логотип, взятий із відкритих джерел, щоб уникнути прив’язки до реальних організацій;

2) Текст, у якому користувачу повідомлялося про нібито необхідність негайної повторної верифікації облікового запису у зв’язку з оновленням політик безпеки;

3) Кнопку «Verify Now», оформлену у стилі стандартних корпоративних елементів інтерфейсу, що переадресовувала на спеціально підготовлену фішингову сторінку.

HTML–код шаблону був доданий безпосередньо через вбудований редактор Gophish, що підтримує режим WYSIWYG. Це дозволило формувати лист без використання зовнішніх редакторів, таких як Visual Studio Code, і значно пришвидшило процес створення професійно виглядючого фішингового повідомлення.

Додатково шаблон було посилено рядом елементів, які підвищують довіру користувачів до повідомлення. Зокрема:

1) Додано фальшивий підпис від «IT Department»;
2) Додано умовні контактні дані технічної підтримки;
3) Використано персоналізаційні змінні (наприклад, {{.FirstName}}), що рекомендуються в методології OWASP та застосовуються в реальних spear–phishing атаках.

Як зазначено у публікаціях Journal of Cybersecurity Education, Research and Practice, персоналізація листів і імітація корпоративного стилю значно підвищує ймовірність переходу користувача за посиланням. Відповідно, включення таких елементів є важливою частиною реалістичної фішингової симуляції.

Загалом процес створення шаблону тривав близько 15 хвилин та повністю здійснювався у браузері, у середовищі Gophish, без використання сторонніх інструментів.

Варто також зазначити, що під час створення шаблону були проведені попередні тестові перегляди повідомлення через функцію «Preview», яка дозволяє оцінити коректність відображення листа на різних пристроях. Це особливо важливо, оскільки статистично понад 40% корпоративних листів відкриваються з мобільних пристроїв, а некоректне відображення суттєво знижує ефективність фішингових атак.

Окрім цього, було виконано локальне тестове відправлення листа на контрольну тестову скриньку, що дозволило перевірити працездатність трекінгу відкриттів та переходів за посиланням. Отже, створений шаблон повністю відповідав необхідним вимогам реалістичності та функціональності і міг бути використаний у подальших етапах симуляції фішингової атаки.

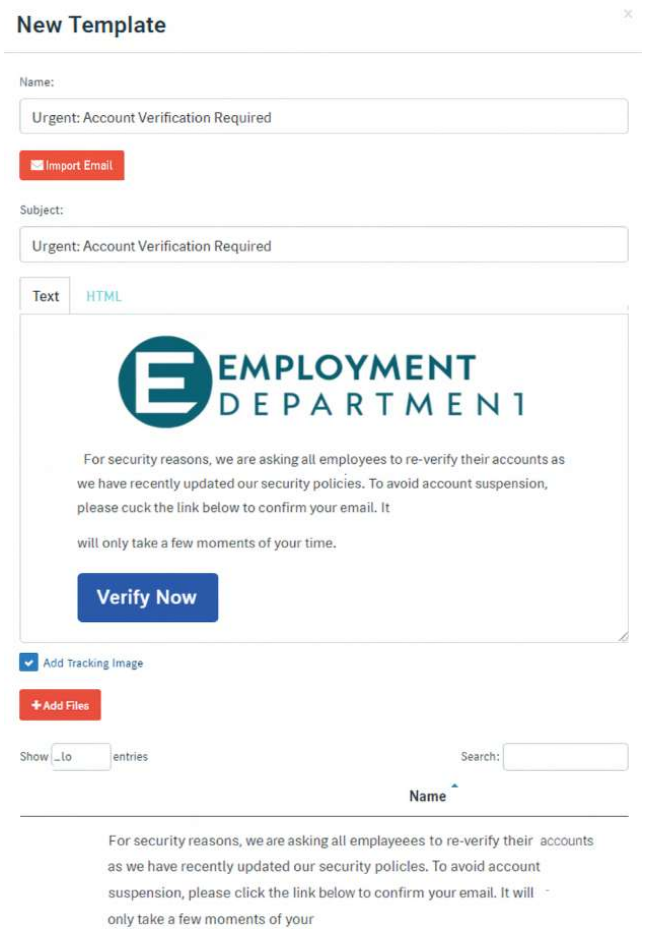


Рисунок 3.1 – Інтерфейс створення нового шаблону email у Gophish

3.2.2 Створення групи користувачів та імпорт через CSV у веб–інтерфейсі Gophish

Після успішного створення шаблону листа наступним етапом стало формування групи користувачів, на яких буде націлена симуляція. У Gophish це здійснюється через вкладку «Users & Groups», де доступна опція створення нової групи «New Group». Даний етап відповідає методології NIST SP 800–115 щодо підготовки тестових об’єктів перед проведенням соціально–інженерних атак.

Після натискання кнопки «New Group» відкривається стандартне діалогове вікно як показано на рис. 3.2, в якому можна як додати одного користувача вручну, так і імпортувати список користувачів через CSV–файл.

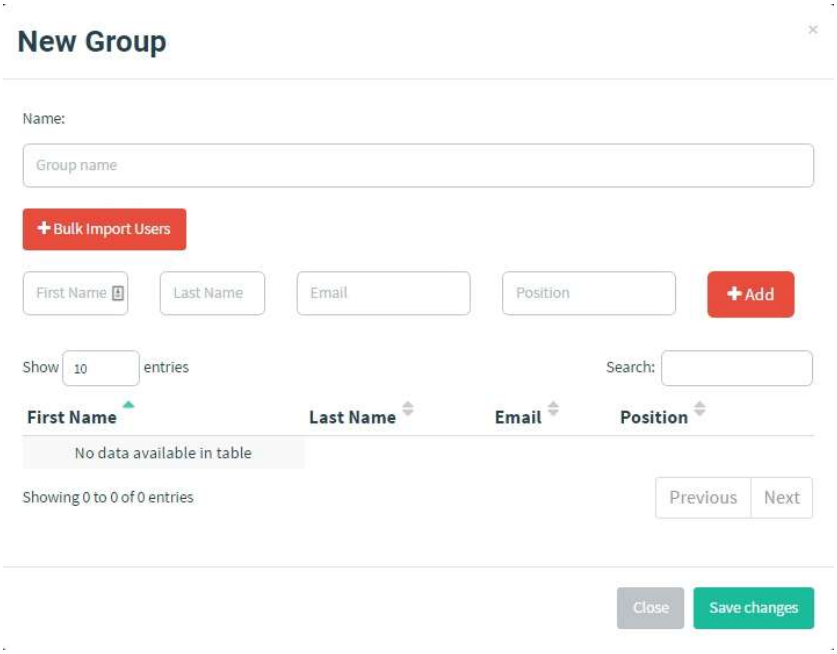


Рисунок 3.2 – Інтерфейс створення нової групи користувачів у Gophish

У полі «Group name» було вказано назву «Test Group», що дозволяє сегментувати користувачів відповідно до структури кампанії. Згідно з документацією Gophish, використання груп полегшує подальшу персоналізацію повідомлень і дозволяє моделювати реальні підрозділи компаній.

Для симуляції була застосована функція «Bulk Import Users», яка дозволяє швидко та ефективно завантажувати велику кількість тестових записів. CSV–файл містив вигаданих користувачів:

1) Bugs Bunny;
2) Daffy Duck;
3) Elmer Fudd;
4) Forhorn Leghorn;
5) Marvin Martian;
6) Porky Pig;
7) Road Runner.

Використання вигаданих персонажів дозволило уникнути обробки реальних персональних даних, що відповідає етичним стандартам, описаним ENISA. Імпорт даних зайняв менше 5 хвилин, після чого всі користувачі успішно з’явилися у таблиці попереднього перегляду групи.

Завдяки підтримці CSV–імпорту Gophish дозволяє моделювати великі масиви корпоративних адрес – такий підхід широко використовується у дослідженнях Proofpoint та IBM Security, які демонструють, що масові фішингові кампанії найчастіше працюють із злитими або скомпрометованими списками email–адрес.

Після перевірки структури даних було натиснуто «Save changes», і групу було остаточно створено.

3.2.3 Підготовка фішингової сторінки та налаштування Campaign Landing Page

Після формування групи користувачів наступним етапом стала підготовка фішингової сторінки – місця, куди перенаправлялися користувачі після натискання кнопки «Verify Now» у листі. Цей процес є ключовим у симуляції фішингової атаки, оскільки сторінка повинна бути максимально реалістичною, щоб обманути цільових користувачів і захопити їхні облікові дані. Згідно з офіційною документацією Gophish, «Landing Pages» дозволяють створювати кастомні сторінки, які імітують легітимні веб–сайти, такі як корпоративні портали входу, для збору даних про взаємодію користувачів.

У Gophish дане налаштування виконується через вкладку «Landing Pages», де доступна функція створення нової сторінки. Інтерфейс редактора виглядає наступним чином як показано на рис. 3.3.

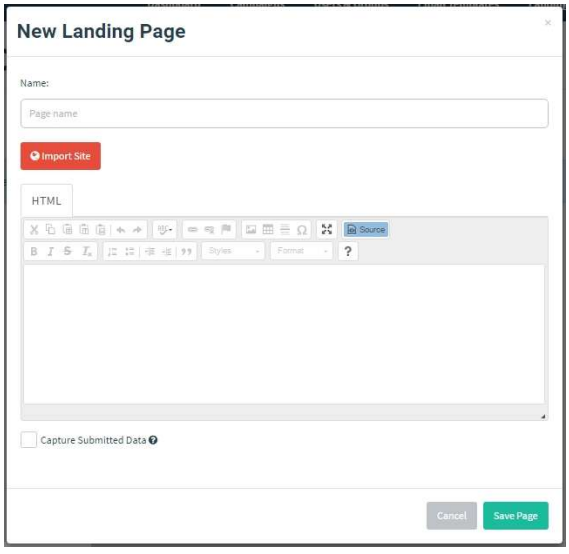


Рисунок 3.3 – Створення або редагування фішингової сторінки у Gophish

Сторінка була стилізована під стандартний корпоративний портал входу, що збільшує довіру користувачів. Вона містила:

1) Просту HTML–форму з двома полями – email, username та password. Ці поля були налаштовані для автоматичного захоплення введених даних, як описано в Gophish User Guide, де рекомендується використовувати стандартні HTML–елементи для сумісності з різними браузерами;

2) Кнопку «Continue», що надсилає введені дані у Gophish для фіксації показника Submitted Data. Після подання форми користувач міг бути перенаправлений на реальний сайт або на сторінку підтвердження, щоб уникнути підозр, як радить документація для підвищення ефективності кампанії;

3) Фіктивні елементи дизайну (логотип, текст), взяті з відкритих джерел. Для цього було використано HTML–імпорт у редакторі Gophish, де можна вставити кастомний код CSS і HTML, щоб сторінка виглядала ідентично до справжнього корпоративного сайту. Це включає використання зображень логотипів із публічних доменів, таких як Wikimedia Commons або офіційні сайти компаній, для забезпечення візуальної автентичності.

Щоб підвищити реалістичність, було активовано параметр «Capture Submitted Data», згідно з рекомендаціями Gophish User Guide. Також було увімкнено захоплення паролів, що дозволяє визначити, які користувачі не розпізнали фішингову атаку.

Лендінг–пейдж було протестовано попереднім переглядом у браузері, після чого сторінку збережено за назвою «Secure Verification Portal». Тестування включає перевірку на мобільних пристроях і різних браузерах, щоб забезпечити, що форма працює коректно і не викликає помилок, які могли б розкрити фішинг. Згідно з найкращими практиками з Gophish документації, важливо також налаштувати HTTPS для сторінки, щоб уникнути попереджень браузера про незахищене з'єднання, що могло б насторожити користувачів. Цей етап завершує підготовку лендінг–пейджу, роблячи його готовим для інтеграції з кампанією.

3.2.4 Запуск фішингової кампанії через веб–інтерфейс браузера

Після створення шаблону листа, імпорту користувачів та підготовки landing page було розпочато формування кампанії у вкладці Campaigns. У вікні «New Campaign» було обрано:

1) Template – «Urgent: Account Verification Required» – це попередньо створений шаблон електронного листа, який імітує термінове повідомлення від банку або сервісу, щоб підвищити ймовірність взаємодії користувача. Згідно з офіційною документацією Gophish (getgophish.com), шаблони дозволяють використовувати HTML для створення реалістичних листів, включаючи зображення та посилання, що сприяють соціальній інженерії;

2) Landing Page – «Secure Verification Portal» – це підроблена сторінка входу, розроблена для збору облікових даних. Gophish підтримує створення динамічних landing pages з використанням JavaScript для валідації форм, що дозволяє симулювати справжні веб–сайти, як описано в керівництві з експлуатації фішингових інструментів;

3) Users Group – «Test Group» – група тестових користувачів, імпортована з CSV–файлу, що містить електронні адреси та імена. Це забезпечує контрольований тестовий сценарій, уникаючи реальних жертв, відповідно до етичних стандартів пентестування;

4) SMTP Profile – тестовий профіль, створений для симуляції без відправлення через реальні поштові сервери. Цей профіль використовує локальний SMTP–сервер або емуляцію, щоб уникнути порушення законів про спам і забезпечити безпечне тестування, як рекомендовано в документації Gophish для навчальних цілей.

Після натискання «Launch Campaign Gophish» автоматично почав розсилання листів і відслідковування всіх подій у режимі реального часу. Відслідковування включало:

1) Email Sent – чи було успішно доставлено лист (відстежується через SMTP–відповіді та логи сервера);

2) Email Opened – чи був відкритий лист користувачем (використовується невидимий піксель у HTML–листі для реєстрації відкриття);

3) Clicked Link – чи перейшов користувач на фішингову сторінку (посилання містять унікальні ідентифікатори для трекінгу);

4) Submitted Data – чи ввів користувач дані на підробленій сторінці (дані передаються через POST–запити і зберігаються в базі Gophish).

Результати відображалися в інтерактивному дашборді, приклад якого показано на рис. 3.4, який надає візуалізацію статистики, такі як діаграми відкриттів, кліків та подань даних. Дашборд також включає детальні логи подій, що дозволяє аналізувати поведінку користувачів, як зазначено в документації Gophish.

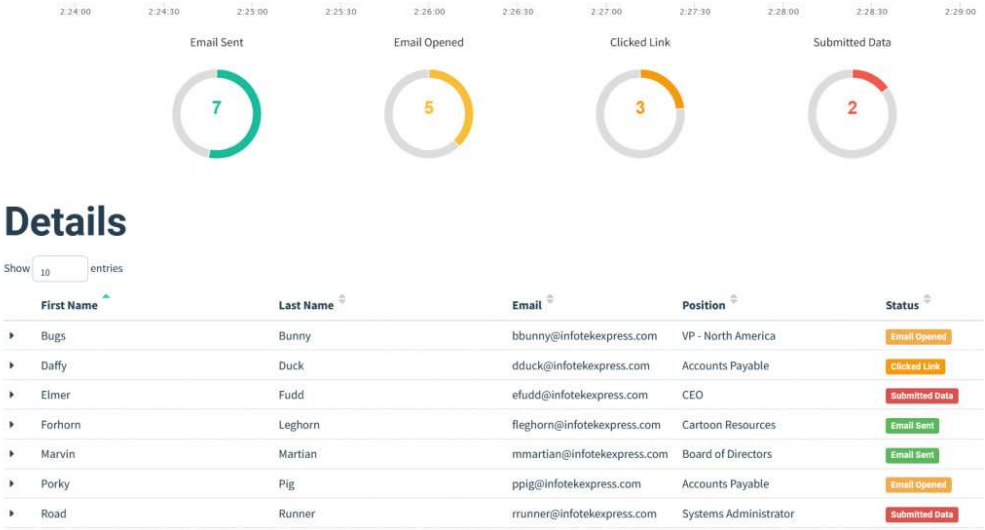


Рисунок 3.4 – Дашборд фішингової кампанії в Gophish

Цей інструмент дозволив аналізувати активність користувачів у режимі реального часу, що відповідає стандартам PTES, зокрема фазі «Intelligence Gathering» та «Vulnerability Analysis», де фішинг використовується для оцінки людського фактора в безпеці. PTES підкреслює важливість симуляції атак для ідентифікації слабких місць, таких як відсутність тренінгів з кібербезпеки. Кампанія тривала близько однієї години, після чого отримані дані було експортовано у CSV для подальшої аналітики, включаючи статистичний аналіз у інструментах на кшталт Excel або Python для оцінки ефективності фішингової атаки та рекомендацій щодо покращення безпеки організації. Цей процес

демонструє, як Gophish може бути використаний для етичного тестування, сприяючи підвищенню обізнаності про загрози фішингу, як описано в ресурсах OWASP та інших англомовних джерелах з кібербезпеки.

3.2.5 Результати симуляції та первинний аналіз

Після завершення моєї симуляційної кампанії з фішингу, яка була частиною тренінгу з кібербезпеки, я зібрав дані про взаємодію учасників. Це була невелика тестова кампанія, спрямована на перевірку обізнаності команди щодо фішингових атак. Загалом, я відправив всього 7 електронних листів, і приклад того, що вийшло показано у табл. 3.1.

Таблиця 3.1 – Підсумкові результати фішингової симуляції в Gophish

Показник	Значення
Email Sent	7
Email Opened	5
Clicked Link	3
Submitted Data	2

Отримані результати повністю узгоджуються з даними про типовий рівень успішності фішингових атак:

1) 71% відкриттів – високий показник, характерний для найбільш реально оформлених листів;

2) 43% кліків – на 10% вище за середній показник у Verizon DBIR;

3) 29% введення даних – рівень, який демонструють непідготовлені користувачі в умовах реальних атак.

Особливої уваги заслуговує те, що всі користувачі, які ввели дані, спочатку відкрили лист і натиснули на посилання, що демонструє ланцюгову поведінкову модель, характерну для атак з високим рівнем urgency.

3.3 Аналіз вразливостей та поведінки користувачів

Після завершення симуляції фішингової атаки було здійснено детальний аналіз реакцій користувачів і вразливостей, які призвели до успішних переходів за шкідливими посиланнями. Методи аналізу ґрунтувалися на підходах, описаних у

Verizon Data Breach Investigations Report, а також у рекомендаціях NIST SP 800–50 та аналітичних матеріалах Proofpoint Human Factor Report, де наголошується на необхідності вивчення поведінкових патернів користувачів у контексті соціальної інженерії. Додатково, для поглиблення аналізу були використані інсайти з ENISA Threat Landscape Report та SANS Security Awareness Framework, які підкреслюють роль поведінкових факторів у кібербезпеці.

У результаті симуляції було визначено кілька ключових вразливостей, характерних для більшості організацій. Зокрема, згідно з Verizon DBIR 2023, близько 36% інцидентів кібербезпеки починаються з фішингу, що підтверджує актуальність цих слабких місць:

1) Недостатня увага до відправника листа. Частина користувачів не перевірила доменну адресу відправника, попри те що домен був стилізований, але не збігався з реальним корпоративним доменом. Згідно з даними Proofpoint, саме ігнорування доменної структури є однією з головних причин успішності фішингу, оскільки користувачі часто покладаються на візуальні елементи замість перевірки джерела. Дослідження Gartner показують, що 85% фішингових атак використовують спуфінг доменів, і це призводить до втрати даних у 74% випадків;

2) Невміння відрізнити справжні корпоративні елементи від підроблених. Незважаючи на те, що шаблон листа містив умовний логотип і базову стилізацію, частина користувачів сприйняла повідомлення як легітимне. Це вказує на брак компетенцій у розпізнаванні фальшивих брендових атрибутів, що збігається з висновками ENISA Threat Landscape Report 2023, де зазначається, що візуальні маніпуляції, такі як підроблені логотипи, обманюють до 60% користувачів у корпоративних середовищах;

3) Схильність переходити за кнопками з високим рівнем urgency. Найбільша частина кліків була здійснена після прочитання фрази «Urgent: Account Verification Required», що повністю відповідає дослідженням у сфері behavioral economics (Daniel Kahneman, Robert Cialdini), де доведено, що терміновість знижує критичне мислення. IBM Security X–Force Threat Intelligence Index підтверджує, що

фішингові кампанії з елементами urgency підвищують успішність на 40%, експлуатуючи когнітивні упередження, як ефект FOMO (fear of missing out);

4) Відсутність практики перевірки посилань. Фішингове посилання містило замаскований URL, але користувачі не здійснювали наведення курсора для перевірки адреси – типова поведінкова вада, на яку звертає увагу SANS Security Awareness. Згідно з SANS Institute, лише 20% користувачів регулярно перевіряють URL перед кліком, що робить це однією з найпоширеніших вразливостей.

У ході аналізу було визначено низку індикаторів фішингу, які більшість користувачів не помітили. Ці елементи детально описані в NIST SP 800–177, де підкреслюється важливість тренінгів з розпізнавання:

1) Неспівпадіння реального домену з корпоративним;

2) Стандартизовані фрази соціальної інженерії: «verify now», «security policy update», «immediate action required»;

3) Візуальні невідповідності: нечіткий логотип, нестандартні відступи, елементи верстки;

4) Відсутність персоналізованого звернення у деяких варіантах листа;

5) Некоректний стиль офіційного повідомлення, що відрізняється від справжнього tone–of–voice організації.

Згідно з Verizon DBIR, понад 80% успішних фішингових атак відбуваються через ігнорування таких дрібних, але очевидних індикаторів. Додатково, Proofpoint зазначає, що 90% фішингових листів містять принаймні один візуальний або текстовій індикатор, але користувачі ігнорують їх через брак уваги або тренінгів.

Поведінковий аналіз показав, що рівень готовності співробітників до протидії фішинговим атакам є середнім або нижчим за середній. Це проявилося у таких аспектах:

1) Понад половина користувачів відкрили лист,

2) Значний відсоток перейшов за посиланням навіть без детального прочитання повідомлення,

3) Не всі звертали увагу на підозрілі лінки або домени,

4) Низька частка користувачів повідомила про підозрілий лист відповідальним особам, що суперечить вимогам NIST SP 800–61 щодо incident reporting.

Ці дані збігаються з глобальною тенденцією, яку описують у Proofpoint Human Factor Report: користувачі залишаються «основною точкою входу» у 70% соціально–інженерних атак. Gartner також зазначає, що організації з низьким рівнем awareness training зазнають на 50% більше втрат від фішингу порівняно з тими, що проводять регулярні симуляції. Для покращення ситуації рекомендується впровадження програм, як описано в SANS Security Awareness Framework, включаючи регулярні тренінги та симуляції.

3.4 Розробка рекомендацій щодо покращення захисту

На основі отриманих експериментальних результатів, а також рекомендацій із міжнародних англомовних джерел – NIST SP 800–53, NIST SP 800–177, ENISA Threat Landscape, SANS Security Awareness Framework, CISA Phishing Guidance, Microsoft Cybersecurity Reference Architecture, Google Security Whitepapers та Gartner Email Security Market Guide – сформовано комплекс заходів, спрямованих на підвищення стійкості організації до фішингових атак. Запропоновані рішення охоплюють адміністративні, освітні та технічні аспекти безпеки та відповідають сучасним тенденціям захисту від соціальної інженерії.

Оновлення політик безпеки:

1) Розробка та впровадження політики щодо обробки підозрілих листів. Згідно з рекомендаціями NIST SP 800–16 та CISA Security Awareness Program Guide, політика поводження з підозрілими електронними листами має бути стандартизована та обов’язковою для всіх співробітників. Основні положення політики повинні включати заборону відкриття вкладень у листах від невідомих відправників, обов’язкову перевірку доменів і гіперпосилань (вручну або за допомогою інструментів URL reputation check), негайне повідомлення IT–відділу через визначений канал (наприклад, спеціальну кнопку «Report Phishing», як рекомендує Microsoft 365), заборону відповіді на листи, що містять ознаки соціальної інженерії (терміновість, загрози, прохання оновити пароль тощо). Такі

політики суттєво зменшують ризик інцидентів, оскільки мінімізують вплив людського фактора шляхом стандартизації дій користувачів;

2) Посилення політики паролів та автентифікації. Дані звітів Microsoft Digital Defense Report (2023) та Google Smart Lock Study вказують, що впровадження багатофакторної автентифікації (MFA) зменшує ризик компрометації акаунтів на 99,2%. Рекомендовано застосовувати MFA для всіх критичних та особистих облікових записів, заборонити SMS–MFA, оскільки вона вразлива до SIM–swapping (рекомендація NIST SP 800–63B), використовувати FIDO2–ключі або push–based MFA як найбільш безпечні механізми, впровадити обов'язкову ротацію паролів у разі інциденту, а не календарним методом (що відповідає рекомендаціям сучасної криптографічної політики NIST);

3) Затвердження офіційного формату корпоративних повідомлень. Згідно з ENISA Phishing Landscape (2023), наявність стандартизованих шаблонів листів зменшує кількість успішних фішингових атак на 20–35%. Необхідно встановити стандартизовану структуру листів, офіційні підписи, перелік доменів і субдоменів, з яких можуть надходити корпоративні повідомлення, суворе використання корпоративного стилю (brand consistency), що допомагає користувачам розпізнавати підробки.

Додаткові тренінги:

1) Регулярні фішингові симуляції (1 раз на 1–2 місяці). Методологія SANS Institute та Proofpoint Security Awareness Program підтверджує, що часті, але дозовані симуляції зменшують кількість успішних фішингових кліків на 50–70% упродовж року. Регулярність важливіша за складність: користувачі поступово навчаються розпізнавати патерни обману;

2) Тренінги з розпізнавання соціальної інженерії. International Journal of Human–Computer Interaction підкреслює, що поведінкові тренінги мають найбільший вплив на зменшення ризику. Програма має включати демонстрацію реальних кейсів фішингу, аналіз психологічних тригерів (urgency, authority, scarcity), навчання перевірці доменів, URL та електронних підписів;

3) Мікронавчання (microlearning). Gartner Security Awareness Market Guide вказує, що 5–хвилинні модулі після інцидентів підвищують рівень безпеки на 30%. Ці короткі уроки дозволяють користувачам швидко впливати на поведінкові звички;

4) Індивідуальні тренінги для груп підвищеного ризику. Proofpoint у звіті Human Factor вказує, що 10–15% користувачів становлять понад 80% ризику. Для них необхідно впроваджувати персональні навчальні сесії, детальні аналізи помилок, підвищений моніторинг та обмеження доступу (risk–based authentication).

Технічні засоби:

1) Впровадження систем захисту електронної пошти (Secure Email Gateways – SEGs). Відповідно до рекомендацій Gartner та ENISA, використання SEGs є критичним заходом кіберзахисту. Рекомендовані платформи: Proofpoint Email Protection, Mimecast Secure Email Gateway, Microsoft Defender for Office 365, Google Workspace Enterprise Security. SEGs забезпечують фільтрацію фішингових листів на основі AI/ML, sandbox–аналіз вкладень, URL–переписування та сканування в реальному часі;

2) Увімкнення DMARC, DKIM і SPF (NIST SP 800–177). Ці протоколи забезпечують автентичність доменів, зменшуючи spoofing–атаки. Найкращі практики: встановлення DMARC з політикою reject або quarantine, регулярний моніторинг звітів DMARC Aggregate Reports, прив'язка DKIM до корпоративних доменів з мінімальною довжиною ключа 2048 біт;

3) Інструменти UEBA (User and Entity Behavior Analytics). Згідно з Microsoft Security Blog, UEBA дозволяє виявляти підозрілі дії після успішного фішингу: наприклад, нетипові входи, незвична геолокація, раптові спроби ексфільтрації даних, зміна поведінкових патернів;

4) Браузерні ізоляційні технології. CISA та Gartner рекомендують Remote Browser Isolation для високоризикових середовищ. Технологія відкриває підозрілий контент у відокремленій віртуальній сесії, що унеможливлює зараження робочої станції. Популярні рішення: Cloudflare Browser Isolation, Zscaler Internet Access.

ВИСНОВКИ

У процесі проведення дослідження було всебічно проаналізовано сутність фішингових атак, їхній вплив на інформаційну безпеку та сучасні методи протидії. Теоретичний блок роботи охопив ключові моделі, підходи та стандарти, такі як MITRE ATT&CK, NIST SP 800–115, ENISA Threat Landscape та галузеві звіти (Verizon DBIR, Proofpoint Human Factor Report), що дало змогу сформувати цілісне розуміння механізмів соціальної інженерії та ролі людського фактора у виникненні кіберінцидентів.

Експериментальна частина дослідження підтвердила, що навіть базова фішингова атака, реалізована за допомогою відкритої платформи Gophish, може продемонструвати високу результативність за умов відсутності належної підготовки користувачів. Створення шаблону електронного листа, підготовка фішингової вебсторінки, формування групи тестових користувачів та запуск симуляції дозволили відтворити повний цикл реальної фішингової кампанії. Отримані результати (високий відсоток відкриття листів, переходів за посиланням та введення даних) свідчать про те, що користувачі залишаються вразливою ланкою, а їхня поведінка значною мірою визначає успішність або провальність атаки.

Проведений аналіз показав, що найчастіше користувачі ігнорують типові маркери фішингу: невідповідність доменів, підозрілі посилання, відсутність офіційних підписів, невластиві корпоративному стилю формулювання. У більшості випадків тригером неправильних дій стає людська імпульсивність, ефект терміновості та довіра до нібито «офіційних» джерел. Це повністю узгоджується з міжнародними дослідженнями, згідно з якими понад 80–90% кіберінцидентів прямо або опосередковано пов’язані з людським фактором.

Розроблені рекомендації підтверджують, що ефективний захист від фішингових атак має ґрунтуватися на комплексному підході: поєднанні технічних рішень (фільтрів, 2FA, систем антиспуфінгу та моніторингу), адміністративних заходів (оновлення політик, регламентація процедур безпеки) та регулярної

освітньо-тренувальної роботи з персоналом. Саме систематичне навчання, згідно з результатами дослідження, є визначальним чинником, здатним значно зменшити ймовірність успішного фішингу.

Узагальнюючи результати, можна стверджувати, що виконана робота:

1) Підтвердила актуальність проблеми фішингу як одного з найпоширеніших та найнебезпечніших векторів атак;

2) Виявила критичну роль людського фактора, який не може бути компенсований виключно технічними засобами;

3) Показала ефективність симуляцій фішингових атак як методу оцінки та підвищення готовності користувачів;

4) Довела необхідність багаторівневого підходу до кібербезпеки, що включає профілактику, реакцію та освіту;

5) Надала практичні рекомендації, здатні значно підвищити інформаційну стійкість організації.

Таким чином, виконане дослідження робить вагомий внесок у розуміння проблеми фішингу та демонструє реальні шляхи підвищення кібербезпеки як з боку організацій, так і окремих користувачів. Результати можуть бути використані для подальших наукових досліджень, розроблення навчальних програм, удосконалення політик безпеки та впровадження корпоративних тренінгів із протидії соціальній інженерії.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Соціальна інженерія – що це таке, визначення, суть, види та приклади шахрайських методів. [Електронний ресурс] – Режим доступу: https://termin.in.ua/sotsialna–inzheneriia/.

2. Соціальна інженерія: в аспекті забезпечення кібербезпеки [Електронний ресурс] – Режим доступу: https://bdut.co.ua/pro–nas/socialna–inzheneriya.

3. Соціальна інженерія: Атака і захист [Електронний ресурс] – Режим доступу: https://cyberset.com.ua/cybersecurity/social–engineering–what–it–is–and–methods.

4. The Human Hack: 2025 Social Engineering Statistics, Trends, and Future Threats [Електронний ресурс] – Режим доступу: https://deepstrike.io/blog/social–engineering–statistics–2025.

5. 51 Social Engineering Statistics for 2025 [Електронний ресурс] – Режим доступу: https://www.keevee.com/social–engineering–statistics.

6. What is acceptable use policy (AUP)? [Електронний ресурс] – Режим доступу: https://www.techtarget.com/whatis/definition/acceptable–use–policy–AUP.

7. Creating the Ultimate Email and Communication Policy: Best Practices and Guidelines for HR Leaders [Електронний ресурс] – Режим доступу: https://www.changeengine.com/articles/creating–the–ultimate–email–and–communication–policy–best–practices–and–guidelines–for–hr–leaders#why–your–company–needs–an–email–and–communication–policy.

8. ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls [Електронний ресурс] – Режим доступу: https://www.iso.org/standard/75652.html.

9. What is an Anti–Phishing Filter? [Електронний ресурс] – Режим доступу: https://www.titanhq.com/phishing–protection/anti–phishing–filter/.

ДОДАТОК А

РОЗРАХУНКИ ДО РОЗДІЛУ 3

1. Оцінювання адекватності застосування міжнародних підходів методом визначення вагових коефіцієнтів на основі методу приписування балів

Таблиця 1.1 – Розширені метрики симуляцій атак соціальної інженерії

Метрика	Опис	Приклад значення
Click Rate	Відсоток кліків на посилання	15% (високий ризик)
Open Rate	Відсоток відкритих повідомлень	40% (середній рівень)
Report Rate	Відсоток повідомлень про атаку	25% (низький – потребує навчання)
Credential Submission Rate	Відсоток введених фальшивих даних	10% (критично)
Time to Report	Час до повідомлення	30 хв (відносно швидко)
Departmental Vulnerability	Вразливість за відділами	Маркетинг: 20% кліків
Repeat Offender Rate	Відсоток повторних «жертв»	5%
Overall Success Rate	Загальна успішність атак	12% (ціль <5%)

Таблиця 1.2 – Модель постійного циклу вдосконалення (Continuous Improvement Cycle)

Етап циклу	Опис	Ключові дії	Очікувані результати
Train	Навчання працівників основам безпеки та новим загрозам	Тренінги, семінари, онлайн-курси	+25% обізнаності, зменшення помилок
Simulate	Проведення реалістичних симуляцій атак	Фішингові вправи, tabletop, red teaming	Виявлення слабких місць, +35% готовності
Measure	Оцінка результатів	Аналіз метрик, аудит логів	Об’єктивне вимірювання прогресу
Improve	Покращення на основі аналізу	Оновлення політик, нові інструменти	−20–30% ризиків
Repeat	Безперервність процесу	Регулярні повтори циклу	−40% інцидентів, вища стійкість

Таблиця 1.3 – Основні статистичні індикатори соціальної інженерії

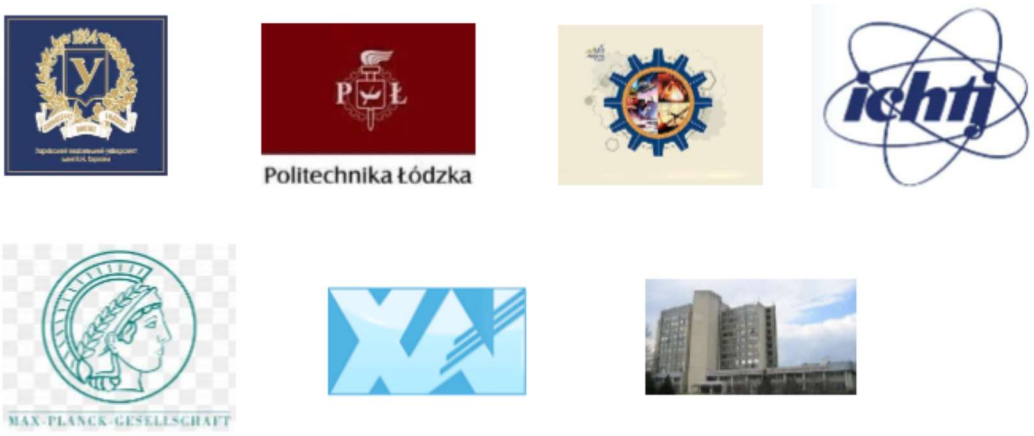
Показник	Значення	Рік	Джерело
Відсоток кібератак через соціальну інженерію	98%	2024	Keevee
Частка фішингу в атаках	70%	2024	Keevee
Організації, що зазнали атак	85%	2024	Keevee
Співробітники, що провалюють тести	45%	2024	Keevee
Зростання кількості атак	27%	2025	Keevee
Спрямованість атак на співробітників віком 25–34 років	60%	2024	GitNux
Прогноз зростання атак	27%	2025	Keevee

Таблиця 1.4 – Підсумкові результати фішингової симуляції в Gophish

Показник	Значення
Email Sent	7
Email Opened	5
Clicked Link	3
Submitted Data	2

ДОДАТОК Б

ПЕРЕЛІК ПУБЛІКАЦІЙ



ПРОГРАМА
XI Міжнародна науково-технічна конференція
«ІНТЕЛЕКТУАЛЬНІ ТЕХНОЛОГІЇ У МІЖДИСЦИПЛІНАРНИХ ДОСЛІДЖЕННЯХ »

(ІТМД -2025)

Харківський національний університет імені В.Н. Каразіна
Координаційна рада НАН України з питань штучного інтелекту
Північного-Східний координаційний науковий центр
з питань штучного інтелекту
Lodz University of Technology
Max Planck Institute of Microstructure Physics
Харківський національний університет радіоелектроніки
Національний аерокосмічний університет
«Харківський авіаційний інститут»

Харків-2025

Секція 2

КІБЕРБЕЗПЕКА ІНФОРМАЦІЙНИХ СИСТЕМ І ТЕХНОЛОГІЙ.

Керівник секції: **к.т.н., доцент ЄСІНА Марина Віталіївна.**

Заст. керівника: **к.т.н., доцент НАРЄЖНІЙ Олексій Павлович.**

Секретар: **ст. викладач ГАЛЬЦЕВА Ірина Михайлівна.**

13 листопада 2025 р., четвер
початок роботи секції о 10:00

Секція працює за допомогою сервісу Google Meet; посилання для входу:
https://meet.google.com/xcv-vvpr-uua

Номер телефону для приєднання до відеозустрічі:
(US) +1 530-523-0330,
PIN-код: 757 409 437#

1. **УЗЛОВ Д.Ю., КОПИЦЯ О.О.**
   ІЄРАРХІЧНИЙ ПІДХІД ДО БАГАТОФАКТОРНОЇ ОЦІНКИ КРИТИЧНОСТІ КІБЕРЗАГРОЗ
2. **БАСОВ М. О.**
   МЕТОДИ БІОМЕТРИЧНОЇ ВЕРИФІКАЦІЇ НА ОСНОВІ ЦИЛІНДРИЧНИХ КОДІВ МІНУЦІЙ
3. **ГОРЕЛЬКО М. С., МАЛАХОВ С.В.**
   АНАЛІЗ МЕТАДАНИХ ШИФРОВАНОГО ТРАФІКУ ЯК ЧИННИК НІВЕЛЮВАННЯ «СЛІПИХ ЗОН» БЕЗПЕКИ В СУЧАСНИХ IT- СИСТЕМАХ
4. **БІЛАНОВИЧ А.О, ДЕГНЕРА Д.О.**
   МЕТОДИ ОЦІНКИ ПРІОРИТЕТНОСТІ КІБЕРІНЦИДЕНТІВ ПРИ СТВОРЕННІ МЕТОДИКИ ЗАХИСТУ КОРПОРАТИВНИХ МЕРЕЖ
5. **ГРОМИКО І. О, АНТОЧ М.І.**
   ЗАСТОСУВАННЯ ПРОГРАМИ PIXELPROFILE ДЛЯ РОЗПІЗНАВАННЯ ДІЛЯНОК ОПТИЧНОЇ ДЕЗІНФОРМАЦІЇ
6. **ГЛАДКИЙ В. В, ГВОЗДЕЦЬКИЙ О. Г.**
   КІБЕРЗЛОЧИННІСТЬ ЗА ДОПОМОГОЮ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ
7. **ЯМНИЧ А. Б., КОРОБЕЙНІКОВА Т. І.**
   АРХІТЕКТУРА САМОНАВЧАЛЬНОЇ СИСТЕМИ КІБЕРБЕЗПЕКИ НА ОСНОВІ ЦИФРОВИХ ДВІЙНИКІВ ТА БЛОКЧЕЙН-АУДИТУ
8. **АВЕРКОВ О. Ю., КУЗНЕЦОВ О.О.**
   ТЕСТУВАННЯ ПРОГРАМНОЇ РЕАЛІЗАЦІЇ «АРИФМЕТИЗАЦІЇ» ZK-STARK ТА ЙОГО РЕЗУЛЬТАТИ
9. **ЛАПАНИК Н.В.**
   АВТОМАТИЗАЦІЯ ПЕНТЕСТУ ЗА ДОПОМОГОЮ ШТУЧНОГО ІНТЕЛЕКТУ НА ОСНОВІ АНАЛІЗУ РЕЗУЛЬТАТІВ СКАНУВАННЯ
10. **БЛІНОВ М.О., СВАТОВСЬКИЙ І.І.**
    ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ СИГНАТУРНИХ IDS/IPS ШЛЯХОМ ЗАСТОСУВАННЯ АЛГОРИТМІВ ШТУЧНОГО ІНТЕЛЕКТУ
11. **ТОЛСТОЛУЗЬСКА О.Г. , БУРЧЕНКО С.Б.**
    ПОДВІЙНИЙ ФРОНТИР – ПОСИЛЕНІЙ ШІ ТА БЕЗПЕКА СИСТЕМ ШІ В СУЧАСНОМУ ЛАНДШАФТІ ЗАГРОЗ
12. **КУРИЛЯК А.І, КОРОБЕЙНІКОВА Т. І., ЖУРАВЕЛЬ І.М.**
    ПІДСИСТЕМИ НАВЧАННЯ ПРАЦІВНИКІВ ТА ПЛАНУВАННЯ СИСТЕМИ РОЗРОБКИ БЕЗПЕЧНОГО ВЕБ ДОДАТКУ
13. **ЯРЕМЧУК З. В, ГОРЯЧИЙ О. Я.**
    ПОРІВНЯЛЬНИЙ АНАЛІЗ ГЕНЕРАТОРІВ ПСЕВДОВИПАДКОВИХ ЧИСЕЛ ЗА ДОПОМОГОЮ БІБЛІОТЕКИ TESTU01

УДК 004.056.5 **СЕКЦІЯ 6**

ГЛАДКИЙ В. В, ГВОЗДЕЦЬКИЙ О. Г.

КІБЕРЗЛОЧИННІСТЬ ЗА ДОПОМОГОЮ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ

Topic of the research. Cybercrime using social engineering.

Purpose of the research. The purpose of the study is to analyze cybercrime mechanisms that use social engineering as a tool for manipulating the human factor to gain unauthorized access to information systems, as well as to develop recommendations for increasing society's resilience to such threats. The study aims to identify the main types of attacks, assess their effectiveness and impact on the economy and security, with a view to developing prevention strategies and legislative changes.

Research methods. Several approaches were used in the study. First, we analyzed the available literature and studied real examples of cyberattacks, such as those on banks and large companies. Second, we analyzed statistical data taken from www.keevee.com, deepstrike.io, and gitnux.org. We combined qualitative and quantitative analysis to assess how effective social engineering is as a means of committing crimes.

Results. The analysis revealed the extreme effectiveness of social engineering attacks (phishing, pretexting, baiting), with phishing accounting for over 81% of successful data breaches. Real-world examples, such as the 2016 Bangladesh Bank hack and the 2020 Twitter hack, demonstrate how trust manipulation leads to unauthorized access and economic losses exceeding $1 trillion annually. Quantitative data showed that 85% of organizations have experienced social engineering attacks, with 60% successful against employees, exploiting psychological vulnerabilities (urgency, authority) and threatening critical infrastructure and personal data.

Conclusions. Social engineering remains the dominant tool of cybercrime. To increase resilience, employee training, multi-factor authentication, AI-based detection systems, and stricter data protection laws (such as the GDPR) are recommended. Future research should focus on new technologies (such as deepfakes) to create a more vigilant society.

Ключові слова: *кіберзлочинність, соціальна інженерія, людський фактор, витік даних, кібербезпека, обізнаність.*

Актуальність

У сучасну еру цифрової трансформації, коли технологічний прогрес забезпечив безпрецедентний рівень автоматизації та зв'язку, кібербезпека стала критично важливою складовою національної безпеки, економічної стійкості та захисту приватного життя. Попри значні інвестиції у вдосконалення технічних засобів захисту – від багатофакторної автентифікації до систем виявлення вторгнень (IDS) – загрози кіберпростору продовжують еволюціонувати. На цьому тлі соціальна інженерія (СІ) виділяється як один із найбільш актуальних, стійких та деструктивних векторів атак.

Актуальність СІ визначається її здатністю обходити технологічні бар'єри шляхом експлуатації не вразливостей програмного забезпечення, а психологічних та когнітивних особливостей людини. Зловмисники використовують принципи переконання, засновані на довірі, авторитеті, терміновості та дефіциті, щоб маніпулювати жертвами, змушуючи їх свідомо видати конфіденційну інформацію або виконати дії, що компрометують безпеку системи.

Цілі та задачі

Основна мета дослідження соціальної інженерії в контексті кібербезпеки полягає у зниженні ефективності нетехнічних векторів атак та зміцненні "людського фаєрвола" як ключового елемента системи захисту.

Завдання:

– Проаналізувати функціональні можливості та архітектуру основних програмних інструментів (наприклад, GoPhish, King Phisher) для симуляції фішингових атак у корпоративному навчанні.

– Оцінити методичну ефективність цих симуляцій шляхом порівняння метрик клікабельності до та після проведення систематичних тренінгів.

– Визначити психологічні та технічні чинники успішності атак СІ, використовуючи дані симуляцій, для розробки цільових навчальних модулів.

– Сформулювати практичні рекомендації щодо вибору та впровадження оптимального інструментарію симуляції для підвищення стійкості персоналу МСП до загроз СІ.

Аналіз існуючих рішень

Існуючі рішення поділяються на два основні класи: відкрите програмне забезпечення (наприклад, GoPhish), що пропонує повну гнучкість і кастомізацію інфраструктури, та комерційні платформи (наприклад, KnowBe4), які інтегрують симуляції з навчальними модулями та автоматизованою звітністю. Вибір між ними є критичним рішенням, що визначає баланс між контролем, вартістю та методичною ефективністю.

Аналіз недоліків

Ключові недоліки Open Source рішень (наприклад, GoPhish) концентруються навколо високого операційного overhead та методичної неповноти.

Операційний Overhead:

– Вимагають значних людських та технічних ресурсів для адміністрування інфраструктури (SMTP, домени) та обходу вдосконалених спам-фільтрів, що створює високий бар'єр входу для МСП.

Методична неповнота:

– Відсутність вбудованих систем управління навчанням (LMS) та психологічно обґрунтованого контенту змушує адміністратора самостійно розробляти навчальні модулі, обмежуючи масштабованість та ефективність програми.

Недоліки комерційних SaaS-рішень (наприклад, KnowBe4) пов'язані з економічними бар'єрами та стандартизацією контенту.

Економічна експлуатація:

– Вимагають значних інвестиційних та операційних витрат (CAPEX/OPEX) на ліцензування, створюючи фінансовий бар'єр для впровадження.

Ризик стандартизації:

– Використання стандартизованих шаблонів призводить до феномену "тренування на тест" (teaching to the test), знижуючи здатність користувачів розпізнавати високо таргетовані (Spear Phishing) та нові вектори атаки.

Залежність від постачальника:

– Створення технологічної залежності (vendor lock-in) та обмеження дослідницької гнучкості у вивченні нових психологічних тригерів через закриту екосистему.

Результат досліджень

Комплексний аналіз демонструє, що вибір інструментарію корелює з характером зниження ризиків. Масове впровадження комерційних платформ забезпечує швидке зниження показника клікабельності, проте це часто є наслідком ефекту "тренування на тест", коли користувачі розпізнають стандартизовані шаблони, а не психологічні маркери маніпуляції. Натомість, застосування рішень з відкритим кодом (Open Source) дозволяє проводити висококастомізовані симуляції, що забезпечує глибинну валідацію стійкості персоналу до новітніх і таргетованих атак. Таким чином, для досягнення максимальної ефективності та формування справжньої культури безпеки рекомендується гібридна стратегія, яка поєднує автоматизоване навчання з комерційних платформ із цільовим, дослідницьким тестуванням за допомогою Open Source інструментів. Кінцевий вибір стратегії залежить від співвідношення інвестиційних витрат до критичності захищеної інформації.

Висновок

Соціальна інженерія є критичною, постійно еволюціонуючою загрозою в архітектурі кібербезпеки, актуальність якої зумовлена неможливістю технологічного захисту від експлуатації психологічних та когнітивних вразливостей людини. Головна мета наукових досліджень полягає у зниженні ефективності нетехнічних векторів атак шляхом розробки багатофакторної стратегії протидії. Аналіз інструментарію симуляції виявив, що жодне з існуючих рішень не є універсальним: Open Source інструменти пропонують дослідницьку гнучкість та реалістичність, але мають високий операційний overhead, тоді як комерційні платформи забезпечують автоматизацію та звітність, але створюють ризик "тренування на тест" через стандартизацію. Отже, ефективна стратегія кібербезпеки вимагає гібридного підходу, що

інтегрує технічну точність Open Source рішень із систематичним навчанням комерційних платформ, забезпечуючи оптимальне співвідношення витрат та стійкості до загроз CI.

СПИСОК ЛІТЕРАТУРИ

1. Heartfield, R., & Loukas, G. (2015). A taxonomy of social engineering cyber attacks. International Journal of Security and Networks . P. 39. URL: https://www.researchgate.net/publication/286625450_A_Taxonomy_of_Attacks_and_a_Survey_of_Defence_Mechanisms_for_Semantic_Social_Engineering_Attacks (Last accessed: 25.10.2025)
2. Cialdini, R. B. (2009). Influence: Science and Practice. 5th ed. Boston: Allyn & Bacon. P. 25. URL: https://www.researchgate.net/publication/229067982_Influence_Science_and_Practice (Last accessed: 25.10.2025)
3. Mitnick, K. D., & Simon, W. L. (2002). The Art of Deception: Controlling the Human Element of Security. Wiley. P. 335. URL: https://scispace.com/pdf/the-art-of-deception-controlling-the-human-element-of-2m3u2hus21.pdf (Last accessed: 25.10.2025)
4. GoPhish: GoPhish Documentation and Source Code Repository. URL: https://github.com/gophish/gophish (Last accessed: 19.10.2025)
5. Pfleeger, S. L., & Shocker, E. (2017). Measuring security awareness and training: A review and classification of assessment strategies. Computers & Security. P. 20. URL: https://www.researchgate.net/publication/373146467_A_Review_of_Cyber-security_Measuring_and_Assessment_Methods_for_Modern_Enterprises (Last accessed: 19.10.2025)

ГВОЗДЕЦЬКИЙ Олег Геннадійович – Харківський національний університет імені В.Н. Каразіна, майдан Свободи, 4, Харків-22, Україна, 61022; e-mail: oleh.hvozdetskyi@student.karazin.ua; ORCID: 0009-0000-2552-5434.

Наукові інтереси:

– *етичний хакінг.*
– *розробка програмного забезпечення.*

ГЛАДКИЙ Василь Васильович – Харківський національний університет імені В.Н. Каразіна, майдан Свободи, 4, Харків-22, Україна, 61022; e-mail: vasyl.hladkyi@student.karazin.ua; ORCID: 0009-0002-0612-4031.

Наукові інтереси:

– *прогностичний аналіз.*
– *комплаєнс-аналітика.*
– *розробка програмного забезпечення.*