МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА УПРАВЛІННЯ КІБЕРБЕЗПЕКОЮ ТА ЗАХИСТОМ ІНФОРМАЦІЇ

КВАЛІФІКАЦІЙНА РОБОТА

на тему: “МЕТОДИ ПРОТИДІЇ СОЦІОІНЖЕНЕРНИМ АТАКАМ У КОРПОРАТИВНИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ”

на здобуття освітнього ступеня бакалавра
зі спеціальності 125 Кібербезпека
освітньої програми Управління інформаційною та кібернетичною безпекою

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ Олексій КУЦЕНКО
(підпис) *Ім’я, ПРІЗВИЩЕ здобувача*

Виконав: здобувач вищої освіти гр. УБД-41

Олексій КУЦЕНКО
Ім’я, ПРІЗВИЩЕ

Керівник: Михайло ЗАПОРОЖЧЕНКО
Доктор філософії з кібербезпеки Ім’я, ПРІЗВИЩЕ

Рецензент: _____
_____ Ім’я, ПРІЗВИЩЕ

Київ 2025

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут кібербезпеки та захисту інформації

Кафедра управління кібербезпекою та захистом інформації

Ступінь вищої освіти бакалавр

Спеціальність 125 Кібербезпека

Освітня програма Управління інформаційною та кібернетичною безпекою

ЗАТВЕРДЖУЮ
Завідувач кафедри УКБЗІ
_____ Світлана ЛЕГОМІНОВА
“____”_____2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Куценку Олексію Сергійовичу
(прізвище, ім’я, по батькові здобувача)

1. Тема кваліфікаційної роботи “Методи протидії соціоінженерним атакам у корпоративних інформаційних системах”,
керівник кваліфікаційної роботи ЗАПОРОЖЧЕНКО Михайло, доктор філософії з кібербезпеки.
(ПРІЗВИЩЕ, Ім’я, науковий ступінь, вчене звання)

затверджені наказом Державного університету інформаційно-комунікаційних технологій від “24“ лютого 2025 р. №56.

2. Строк подання кваліфікаційної роботи “12” травня 2025р.

3. Вихідні дані до кваліфікаційної роботи: *типові сценарії соціоінженерних атак, методи протидії соціоінженерним загрозам, інформаційна безпека підприємства, способи визначення рівня обізнаності та навчання персоналу.*

4. Перелік питань, які мають бути розроблені:
4.1 Провести теоретичний аналіз соціоінженерних атак як складової сучасних загроз інформаційної безпеки корпоративних систем.
4.2 Дослідити особливості вразливостей корпоративних інформаційних систем до соціоінженерних впливів.
4.3 Систематизувати методи виявлення, запобігання та реагування на соціоінженерні атаки.
4.4 Розробити методичні рекомендації щодо організації захисту від соціоінженерних атак, включаючи навчання персоналу та технічні рішення.
4.5 Здійснити практичне впровадження запропонованих заходів і оцінити їх ефективність.

5. Перелік ілюстративного матеріалу: *презентація PowerPoint*

6. Дата видачі завдання “5” березня 2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Етапи кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1.	Визначення об’єкту, предмету, мети та завдань дослідження.	18.03.2025	
2.	Збір та аналіз літератури.	29.03.2025	
3.	Аналіз протидії соціоінженерним атакам у корпоративних інформаційних системах	08.04.2025	
4.	Методика організації захисту корпоративного середовища від соціоінженерних атак	15.04.2025	
5.	Реалізація підходів організації захисту корпоративного середовища від соціоінженерних загроз	22.04.2025	
6.	Підведення підсумків за попередніми результатами проведеного дослідження.	29.04.2025	
7.	Оформлення роботи.	06.05.2025	
8.	Оформлення презентації.	09.05.2025	
9.	Отримання рецензії на роботу.	12.06.2025	
10.	Захист в ДЕК.	__.06.2025	

Здобувач вищої освіти _____ Олексій КУЦЕНКО
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Керівник
кваліфікаційної роботи _____ Михайло ЗАПОРОЖЧЕНКО
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ

ПОДАННЯ
ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ
на здобуття освітнього ступеня бакалавра

Направляється здобувач Куценко О.С. до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 125 Кібербезпека
(код, найменування спеціальності)
освітньої програми Управління інформаційною та кібернетичною безпекою
(назва)
на тему: "Методи протидії соціоінженерним атакам у корпоративних інформаційних системах"

Кваліфікаційна робота і рецензія додаються.

Директор ННІКБЗІ _____ Євгенія ІВАНЧЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Висновок керівника кваліфікаційної роботи

Здобувач КУЦЕНКО Олексій у кваліфікаційній роботі дослідив особливості соціоінженерних атак у корпоративному середовищі, провів аналіз вразливостей, розробив рекомендації щодо технічних та організаційних заходів захисту, а також реалізував навчальні заходи з кібергігієни.

Робота свідчить про високий рівень теоретичної підготовки та практичних навичок здобувача. Олексій проявив відповідальність та вміння працювати самостійно над поставленими завданнями. Результати дослідження апробовані на конференції.

Все це дозволяє оцінити кваліфікаційну роботу здобувача КУЦЕНКА Олексія на оцінку "відмінно" та присвоїти йому кваліфікацію бакалавра з кібербезпеки за освітньою програмою Управління інформаційною та кібернетичною безпекою.

Керівник кваліфікаційної роботи _____ Михайло ЗАПОРОЖЧЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

"____" _____2025 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач Куценко О.С. допускається до захисту даної роботи в Екзаменаційній комісії.

Завідувач кафедри
управління кібербезпекою та
захистом інформації _____ Світлана ЛЕГОМІНОВА
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну бакалаврську роботу

здобувача вищої освіти КУЦЕНКА Олексія
на тему “Методи протидії соціоінженерним атакам у корпоративних інформаційних системах”

Актуальність. Протягом останніх років соціоінженерні атаки набувають дедалі більшого поширення, оскільки орієнтовані не на технічні вразливості, а на маніпулювання поведінкою користувачів, використання когнітивних викривлень, нестачі обізнаності та порушень організаційної дисципліни. Особливої гостроти ця проблема набуває в корпоративному секторі, де компрометація одного працівника може призвести до системних наслідків для інформаційної безпеки всієї організації. В умовах посилення цифрових загроз та гібридних форм атак, що поєднують технічні й соціотехнічні елементи, питання підвищення стійкості персоналу до соціоінженерного впливу є критичним компонентом управління ризиками. Тому дослідження, присвячене аналізу механізмів таких атак, виявленню вразливостей персоналу та розробці практичних заходів протидії, є науково обґрунтованим і актуальним.

Позитивні сторони.

1. У роботі розкрито природу соціоінженерних атак, визначено фактори вразливості та проаналізовано способи їх подолання.
2. Представлено комплексний підхід до протидії: навчальні заходи, технічні рішення та організаційні механізми.
3. Проведено аудит безпеки на прикладі реального підприємства з оцінкою ефективності впроваджених рішень.
4. Робота структурована, має логічний виклад, супроводжується ілюстративним матеріалом та обґрунтованими висновками.

Недоліки.

1. Доцільно було б ширше охопити кількісні методи оцінювання впливу навчальних заходів та надати більше статистичних даних для верифікації ефективності запропонованих рішень.

Однак, вищезгадані зауваження не впливають на загальну позитивну оцінку кваліфікаційної роботи

Висновок: Кваліфікаційна робота виконана на належному науково-методичному рівні і заслуговує оцінки “_____”, а здобувач КУЦЕНКО Олексій заслуговує присвоєння кваліфікації бакалавра з кібербезпеки за освітньою програмою Управління інформаційною та кібернетичною безпекою.

Рецензент:
_____ _____ _____
підпис Ім’я, ПРІЗВИЩЕ

РЕФЕРАТ

Кваліфікаційна робота присвячена підвищенню рівня захищеності корпоративних інформаційних систем від соціоінженерних атак. Робота складається зі вступу, трьох розділів, що містять 36 рисунків, висновків і списку використаних джерел із 57 найменувань. Загальний обсяг роботи становить 65 аркушів, з яких 6 аркушів займає список використаних джерел.

Метою роботи є підвищення рівня захищеності корпоративних інформаційних систем від соціоінженерних атак шляхом аналізу чинників сприйнятливості користувачів, обґрунтування методів протидії та впровадження організаційних, технічних і навчальних заходів.

Об'єктом дослідження є процес забезпечення захисту корпоративної інформаційної системи від соціоінженерних атак.

Предмет дослідження – методи виявлення, запобігання та стримування соціоінженерних атак у корпоративному середовищі.

Методи дослідження. Для вирішення означеного вище наукового завдання в роботі використаний аналітичний підхід, опитування, статистичну обробку даних та класифікацію інформації.

Як результат у роботі досліджено особливості вразливостей корпоративних інформаційних систем до соціоінженерних загроз, розроблені методичні рекомендації щодо організації захисту та здійснено практичне впровадження цих заходів.

Галузь застосування. Розроблені підходи можуть бути використані для підвищення обізнаності співробітників при створенні та реалізації інформаційної та фізичної безпеки у корпоративних мережах.

Ключові слова: СОЦІОІНЖЕНЕРНА АТАКА, ФІШИНГ, ЛЮДСЬКИЙ ФАКТОР, ПСИХОЛОГІЧНА МАНІПУЛЯЦІЯ, ІНФОРМАЦІЙНА БЕЗПЕКА, КОРПОРАТИВНЕ СЕРЕДОВИЩЕ, ОБІЗНАНІСТЬ ПЕРСОНАЛУ.

ABSTRACT

The qualification work is devoted to increasing the level of security of corporate information systems against socio-engineering attacks. The work consists of an introduction, three chapters containing 36 figures, conclusions and a list of 57 references. The total volume of the work is 65 pages, of which the list of references takes up 6 pages.

The purpose of the study is to increase the level of security of corporate information systems against socio-engineering attacks by analyzing the factors of user susceptibility, substantiating methods of counteraction and implementing organizational, technical and training measures.

The object of research is the process of ensuring the protection of a corporate information system from socio-engineering attacks.

The subject of the study is methods of detecting, preventing and deterring socio-engineering attacks in the corporate environment.

Research methods. To solve the above scientific task, the paper uses an analytical approach, statistical data processing and information classification.

As a result, the paper investigates the peculiarities of vulnerabilities of corporate information systems to social engineering threats, develops methodological recommendations for organizing protection and implements these measures in practice.

Scope of application. The developed approaches can be used to raise awareness of employees when creating and implementing information and physical security in corporate networks.

Keywords: SOCIAL ENGINEERING ATTACK, PHISHING, HUMAN FACTOR, PSYCHOLOGICAL MANIPULATION, INFORMATION SECURITY, CORPORATE ENVIRONMENT, STAFF AWARENESS.

ЗМІСТ

ВСТУП

Актуальність теми. У сучасних умовах цифрової трансформації підприємств соціоінженерні атаки посідають провідне місце серед загроз інформаційній безпеці, оскільки спрямовані на експлуатацію людського фактора й психологічних вразливостей працівників. Частота й складність таких атак зростають у зв'язку з використанням автоматизованих інструментів та методик штучного інтелекту для персоналізації шкідливих повідомлень. Вітчизняні та міжнародні практики свідчать про неадекватність технічних засобів безпеки без одночасного розвитку організаційних, навчальних і психологічних заходів із протидії соціальній інженерії. Отже, вивчення методів комплексного захисту корпоративних інформаційних систем є важливим науковим і практичним завданням в інтересах підвищення стійкості бізнесу та державних інституцій.

Мета роботи полягає у підвищенні рівня захищеності корпоративних інформаційних систем від соціоінженерних атак шляхом аналізу чинників сприйнятливості користувачів, обґрунтування методів протидії та впровадження організаційних, технічних і навчальних заходів.

Об'єкт дослідження – процес забезпечення захисту корпоративної інформаційної системи від соціоінженерних атак.

Предмет дослідження – методи виявлення, запобігання та стримування соціоінженерних атак у корпоративному середовищі.

Для досягнення мети у роботі поставлено такі завдання:

1. Провести теоретичний аналіз соціоінженерних атак як складової сучасних загроз інформаційній безпеці корпоративних систем.
2. Дослідити особливості вразливостей корпоративних інформаційних систем до соціоінженерних впливів.
3. Систематизувати методи виявлення, запобігання та реагування на соціоінженерні атаки.

4. Розробити методичні рекомендації щодо організації захисту від соціоінженерних атак, включаючи навчальні програми та технічні рішення.

5. Здійснити практичне впровадження запропонованих заходів та оцінити їх ефективність.

Методи дослідження. Для вирішення означеного вище наукового завдання в роботі використаний аналітичний підхід, опитування, статистичну обробку даних та класифікацію інформації.

Практичне значення результатів. Розроблені шаблони та рекомендації можуть бути безпосередньо інтегровані в корпоративні політики безпеки для оперативного вдосконалення захисних заходів. Організаційні й навчальні програми дозволяють підвищити обізнаність персоналу та знизити рівень успішності соціоінженерних атак.

Апробація результатів кваліфікаційної роботи відбулася на Всеукраїнській науково-практичній конференції “Стратегії кіберстійкості: управління ризиками та безперервність бізнесу” 27 лютого 2025 року.

Розділ 1 ТЕОРЕТИЧНІ ЗАСАДИ ПРОТИДІЇ СОЦІОІНЖЕНЕРНИМ АТАКАМ У КОРОПОРАТИВНИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ

У першому розділі детально розглядається соціальна інженерія як вид кіберзлочинів, де зловмисники використовують психологічні маніпуляції для викрадення конфіденційних даних. Роз'яснюються механізми та принципи роботи таких атак, а також пропонуються стратегії захисту. Підкреслюється, що успіх соціальної інженерії залежить від маніпулювання жертвами, впливу на їхні рішення та дії. Аналізуються фактори, що роблять людей більш схильними до таких атак, включаючи психологічні "тригери" на кшталт тиску часу, авторитету та емоційного впливу.

Значна увага приділяється сучасним методам виявлення соціоінженерних загроз на ранніх етапах, зокрема використанню алгоритмів для моніторингу нетипової поведінки, інструментів аналізу комунікацій та можливостей штучного інтелекту. Описується процес розробки та впровадження процедур реагування на інциденти, включаючи ідентифікацію ознак злому, ізоляцію уражених систем та адаптацію політик безпеки. Наголошується на важливості навчання та підготовки персоналу для підвищення рівня кібербезпеки організації. Пропонується комплексний підхід, що включає регулярні тренінги, імітацію фішингових атак та психологічну підготовку для розвитку критичного мислення та навичок розпізнавання маніпуляцій, що сприяє формуванню культури інформаційної безпеки.

1.1 Теоретичне обґрунтування соціоінженерних атак як елементу сучасних кіберзагроз

Людський фактор є найчастішою причиною успішного злому та викрадення конфіденційних даних. Крістофер Хаднагі казав: "Мета соціального інженера – схилити вас до прийняття необдуманих рішень. Що більше у вас

буде можливостей обміркувати те, що відбувається, то з більшою ймовірністю ви розкусите маніпуляцію, а зловмисникам цього, звісно, не треба" [1].

У 1979 Кевін Мітнік зміг отримати доступ до коду операційної системи Digital Equipment Corporation. Цей акт не був вчинений заради фінансової вигоди чи руйнування – він просто хотів навчитися і зрозуміти, як працюють системи. А у 1992 році отримав доступ до систем телефонного зв'язку мережі Pacific Bell, що дозволило йому змінювати телефонні лінії і отримувати доступ до будь-якої інформації. Надалі він вже систематизував методи обману у вигляді телефонних та соціальних маніпуляції, показавши, що психологічні трюки дозволяють ефективно обходити технічні заходи захисту [2].

Надалі з появою електронної пошти з'являться більш витончені форми, зокрема фішинг та BEC (Business Email Compromise), що дозволять зловмисникам отримувати великі суми коштів, імітуючи офіційне листування керівництва і фінансових підрозділів. А у 20-х роках ключовим нововведенням стане інтеграція штучного інтелекту. Машини вийдуть на рівень автоматизації персоналізованих фішингових повідомлень та оптимізують час розсилки, щоб підвищити кількість відкритих повідомленням із шкідливим вмістом [3].

Сьогодні соціоінженерна загроза – це форма маніпуляції, що використовує психологічні слабкості людей, як-от довіра, страх або бажання отримати допомогу, щоб змусити їх розкрити конфіденційну інформацію або вжити заходів, шкідливих для організації. Адже набагато простіше підкинути фішинговий лист із шкідливим програмним забезпеченням і змусити людину його відкрити, ніж придумати новий варіант кібератаки. На відміну від вірусів і шкідливого коду, використовуються недоліки людини, а не апаратна частина. Цей принцип обману лежить в основі сучасних цифрових атак.

Реалізація найбільш популярних соціоінженерних атак відбувається через такі техніки:

1. Phishing – розсилка підроблених електронних листів або SMS/чат-повідомлень, що імітують легітимні запити (наприклад, від банку або

постачальника послуг), з метою отримати логін, пароль або фінансові дані жертви;

2. Spear phishing – адресні (цільові) версії фішингу, при яких зловмисники готують надзвичайно правдоподібні листи для конкретної особи або компанії, використовуючи відкриті дані про їх захоплення;

3. Vishing – дзвінки або голосові повідомлення, у яких зловмисник під виглядом авторитетної особи змушує жертву розкрити секрети чи змінити налаштування;

4. Quashing – розсилки SMS-повідомлень із підробленими повідомленнями (наприклад, «Ваша картка заблокована») задля того, щоб жертва перехідним посиланням завантажила шкідливий додаток або перейшла на підроблений сайт.

Також не можна недооцінювати атаки фізичного роду таких як:

1. Tailgating – непомітне слідування за авторизованою особою через контрольовані двері чи турнікети. Зловмисник керується фактом, що працівники за звичкою пропускають “свого” за собою, не перевіряючи картку доступу іншої особи;

2. Shoulder surfing – візуальне спостереження за введенням паролів, PIN-кодів або інших секретних даних “через плече” жертви. Спостереження за допомогою бінокля або прихованої камери;

3. Dumpster diving – пошук інформації в смітниках і контейнерах для відходів організації. Зі сміття виймають роздруківки, носії інформації, зошити з паролями чи робочими нотатками, які дають змогу відтворити внутрішні процедури чи отримати облікові дані;

4. Baiting – розкладання заражених флеш-накопичувачів чи інших гаджетів у місцях, де співробітники можуть їх знайти (паркування, коридори). Зацікавлена особа під’єднує пристрій до робочого комп’ютера, інсталює шкідливий код і відкриває доступ зловмиснику;

5. Pretexting – зловмисник видає себе за технічного працівника провайдера, інженера чи представника служби підтримки IT, пред’являє

підроблені документи або форму, і просить увійти до приміщення або надати доступ до обладнання [4].

Типові техніки соціоінженерних атак наведені на рисунку 1.1.

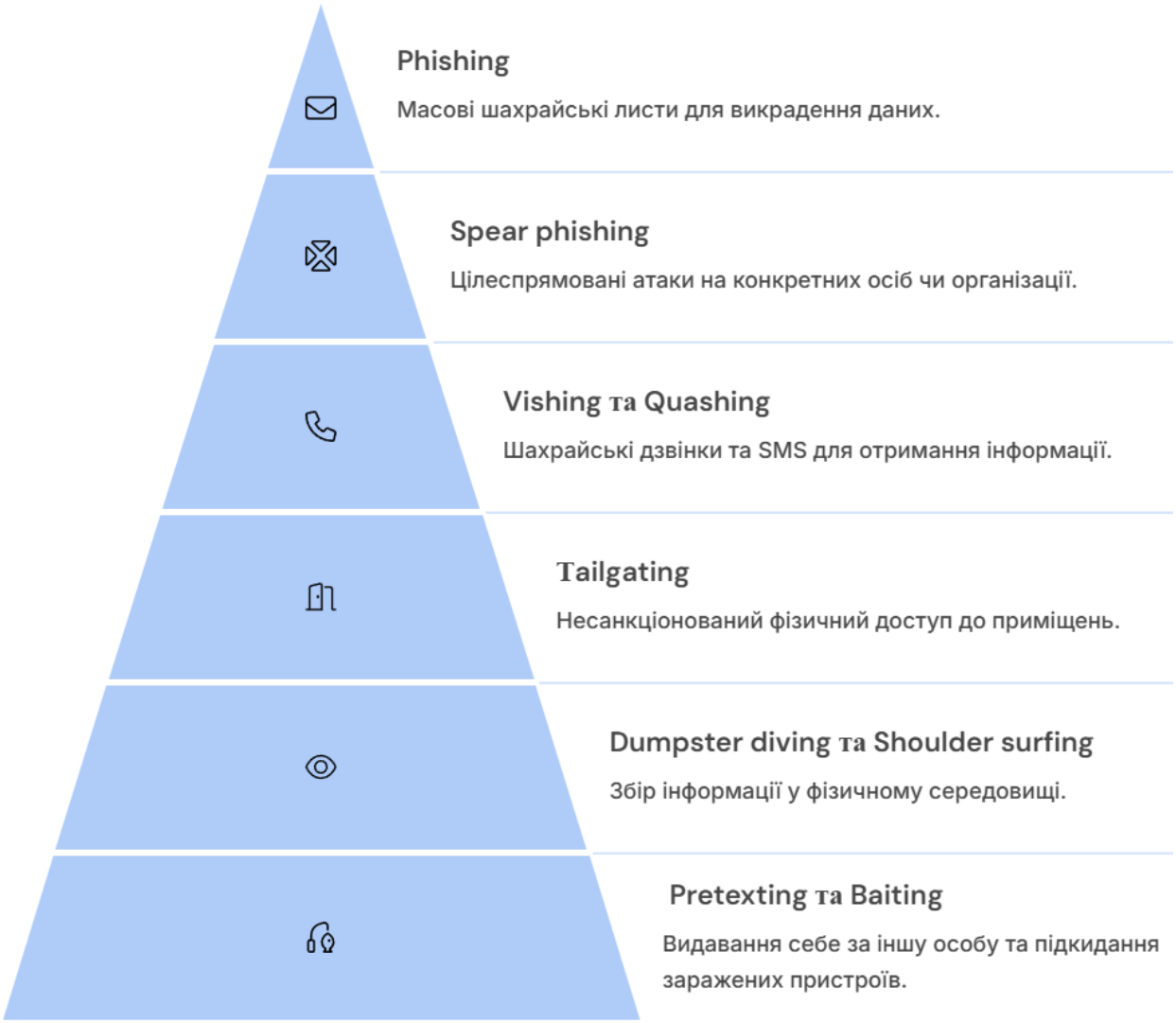

Рис. 1.1. Види соціоінженерних атак

Окрім традиційних атак, з можливостями сучасного штучного інтелекту, зловмисники здатні автоматично генерувати персоналізовані листи та повідомлення на базі відкритих даних у соціальних мережах, що дозволяє одразу ж визначити найуразливіших одержувачів, а також імітувати голоси та манеру спілкування керівників або колег через deepfake-аудіо та нейромережеві чат-боти, що значно підвищує ефективність соціальної інженерії по телефону відомого як вішинг.

Водночас фахівці з кіберзахисту також починають використовувати штучний інтелект для боротьби з подібними загрозами. Системи, навчені розпізнавати нетипову поведінку в електронному листуванні та аналізувати мовні моделі на ознаки соціальної інженерії, вже показують високу ефективність у попередженні атак. Проте остаточний рубіж оборони залишається за людиною: регулярне навчання співробітників, відпрацювання сценаріїв фішингових атак у безпечному середовищі та формування культури, в якій перевірка незрозумілих запитів стає звичкою, – це ті кроки, які можуть істотно знизити ризики успішного шкідливого втручання.

Важливо розуміти, що соціальні інженери послуговуються психологією жертви: вони викликають у людей довіру, страх, почуття терміновості або цікавість, щоб спровокувати поспішні рішення. З огляду на це, соціоінженерні атаки стають дедалі ефективнішими й складнішими. Статистика підтверджує: людський фактор більше не просто “слабка ланка”. Він став активним “входом” для зловмисників, які використовують його для отримання доступу до організаційних мереж і викрадення корпоративних даних [6].

Звіт Verizon DBIR 2024 виявив, що 74% порушень безпеки включали зловживання привілеями, викрадені облікові дані або соціоінженерні загрози. У цих даних спостерігається, що головні вектори проникнення – це викрадені облікові дані, фішинг та експлуатація відомих уразливостей (рис. 1.2).

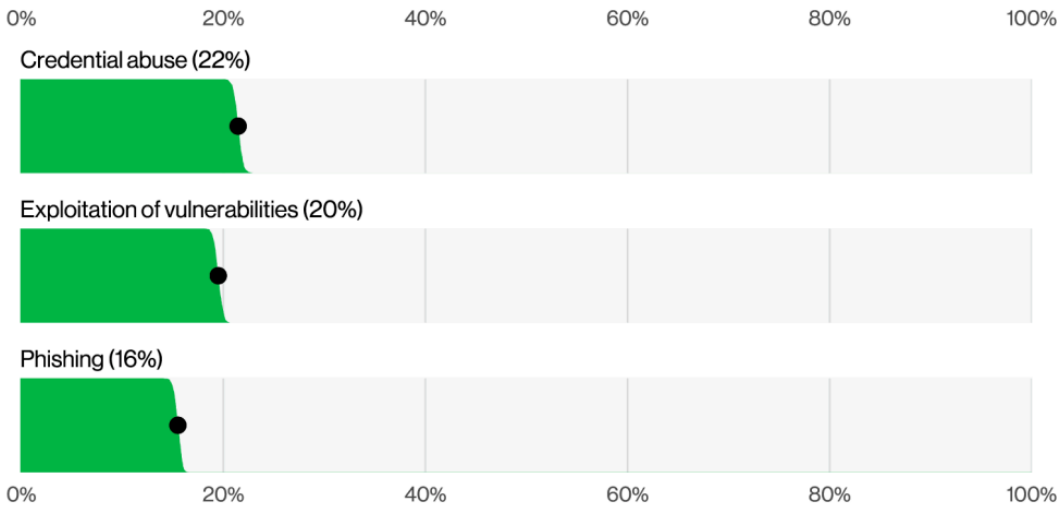

Рис. 1.2. Найпопулярніші способи викрадення даних [5]

Ці показники свідчать, що соціоінженерні атаки – чисельна і зростаюча складова сучасних кіберзагроз. Висока прибутковість і низька вартість таких атак приваблюють кіберзлочинців: кіберзлочини із застосуванням соціальних маніпуляцій регулярно входять у топ-рейтинги витрат на кібербезпеку (збитки фішингових і BEC-атак налічують сотні мільйонів доларів) [7].

Наступний опис зосереджується на ключових етапах процесу та психологічних механізмах, що їх зумовлюють (рис. 1.3).

Рис. 1.3. Етапи реалізації соціоінженерних атак

1. Розвідка – зловмисник починає з ретельного вивчення своєї жертви, збираючи всі доступні дані. Це може бути інформація з відкритих джерел, така як адреси електронної пошти, імена співробітників, їхні посади та інша

інформація про організацію. Мета – скласти детальний портрет жертви, щоб максимально персоналізувати і переконливо спланувати атаку;

2. Планування атаки – на основі зібраної інформації зловмисник розробляє стратегію. Він обирає тип атаки (наприклад, фішинг), створює переконливе повідомлення і визначає оптимальний час для його відправки. Що краще спланована атака з урахуванням особливостей жертви, то вищою є ймовірність успіху і нижчим ризик бути виявленим;

3. Доставка приманки – на цьому етапі зловмисник надсилає жертві підготовлене повідомлення, яке може містити фішинговий лист, посилання на підроблений сайт або шкідливий файл. Це момент безпосереднього контакту і початку атаки;

4. Експлуатація довіри – коли жертва реагує на повідомлення (наприклад, переходить за посиланням або відкриває файл), зловмисник використовує її довіру, страх або цікавість, щоб змусити її виконати потрібні дії. Мета – обманом отримати доступ до систем або конфіденційної інформації;

5. Закріплення в системі – після отримання доступу зловмисник намагається закріпитися в системі, щоб мати змогу повертатися в неї знову і знову. Він може встановлювати шкідливе ПЗ, створювати облікові записи або використовувати інші методи для підтримання постійного доступу та збору додаткової інформації. Зловмисники можуть залишатися непоміченими в системі протягом тривалого часу, перш ніж почати активні дії;

6. Управління та контроль – зловмисник використовує спеціальні інструменти для віддаленого управління скомпрометованою системою і для передачі даних. Він може витягувати конфіденційну інформацію або використовувати систему для подальших атак;

7. Замітання слідів – щоб уникнути виявлення, зловмисник намагається приховати сліди своєї діяльності. Він може видаляти або змінювати записи в журналах, щоб ускладнити розслідування і зберегти свій доступ до системи. Це критично важливий етап для підтримки довгострокової та непомітної присутності в системі жертви [8].

1.2 Аналіз психологічних механізмів впливу на користувачів і чинників сприйнятливості

Соціальна інженерія – великий вибір можливостей отримання доступу до комп'ютерних систем не лише технічно, а й за допомогою психологічних підходів. З роками вона переросла в окрему частину психології і наразі використовується для підготовки шпигунів. Всі техніки соціальної інженерії ґрунтуються на прийнятті рішень людиною, відомих як когнітивна основа [9].

Когнітивні упередження також грають ключову роль. До типових упереджень належать підтвердження власних очікувань, коли людина шукає у листі саме те, що вона очікувала побачити. Наприклад, шахраї часто використовують імена відомих компаній або підроблені заголовки, що автоматично збільшує довіру. Обманюють, переконують та спонукають до певних дій.

У термінології Канемана "система 1" [10] – це так звані принципи дефіциту, взаємності, авторитету і соціального схвалення (рис. 1.4).

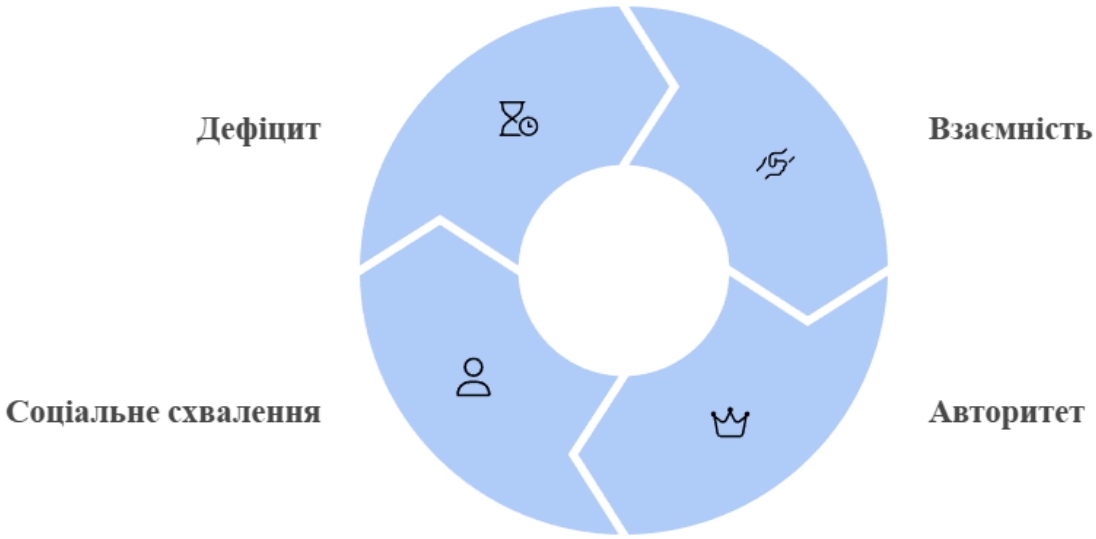

Рис 1.4. Принципи психології Канемана в соціоінженерних загрозах

Приклади експлуатації цих принципів наведені нижче:

1. Дефіцит – користувача було повідомлено: "Акція тільки сьогодні" або "Термін виконання – година, інакше аккаунт буде заблоковано";

2. Взаємність – прохання від колеги зареєструватися на одному сайті з робочою поштою бо в нього видає помилку, а в обмін буде надано купон на 50% знижку;

3. Авторитет – шахраї імітують офіційні адреси з підписами, щоб користувач не задумуючись виконав їхні вказівки;

4. Соціальне схвалення – повідомлення типу “відбулося оновлення програмного забезпечення, 80% співробітників вже використовують нову версію програми”.

Зазвичай схема фішингу має такий вигляд: жертві надходить електронний лист від банку з попередженням, що її рахунок заблоковано. Терміново потрібно натиснути посилання. Лист містить все необхідне – логотип банку, ім’я клієнта, навіть підписи від імені співробітників (рис. 1.5). Жертва в паніці слідує інструкціям, не перевіряючи доменну адресу. Як стверджує Microsoft, 91% усіх кібератак починається саме з таких фішингових повідомлень [11].

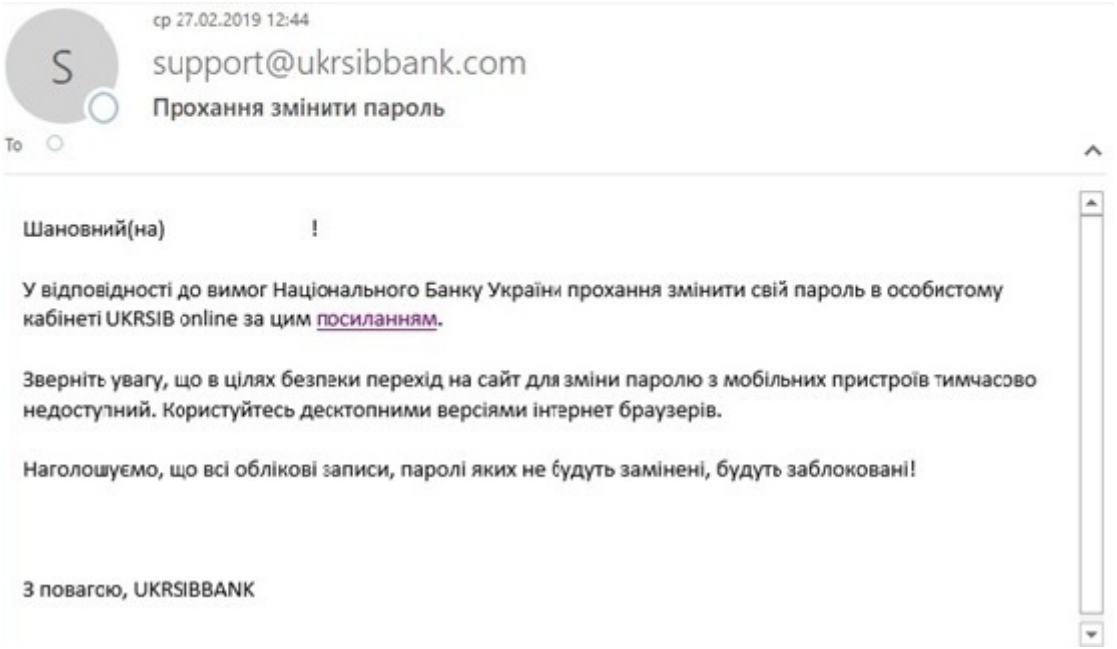

Рис 1.5. Приклад фішингового листа [14]

Нерідко для атаки створюється складний сценарій. Кілька етапів у чаті або по телефону, зміна тональності від дружнього до наказового, штучне наростання емоцій. Атаки можуть тривати годинами чи днями, коли

зловмисник спочатку налагоджує довіру, а потім домагається конкретного результату. Сучасні технології ще більше підсилюють цю динаміку: віртуальні голосові боти на основі штучного інтелекту (діпфейку), можуть імітувати голос керівника, додаючи автентичності вимозі переказати гроші.

Приклади в корпоративному середовищі ілюструють ці механізми. Наприклад, відділ маркетингу отримав надзвичайно важливий імейл від гендиректора з проханням терміново надати доступ до звітів. Співробітник, боячись виглядати непрофесійно, виконав прохання без перевірки. Або шахраї склали фіктивну компанію, нібито партнера, і пропонують бухгалтерії вигідну угоду. Ще один випадок – це атака CEO Fraud (шахрайство від імені топ-менеджера). Зазвичай у таких атаках використовується саме бажання підлеглих догодити шефу, а також завчені обороти і терміни, які викликають сприйняття реальності повідомлення [12].

Класифікація чинників сприйнятливості діляться на індивідуальні риси, демографічні, ситуаційні та середовищні фактори:

1. Низький рівень потреби в когнітивному контролі – менша мотивація до глибокого аналізу інформації;
2. Вік – молодь і люди похилого віку по-різному реагують на ризики і страхові сигнали;
3. Стать – чоловіки й жінки можуть відрізнятися за чутливістю до різних стратегій переконання;
4. Освітній рівень та цифрова грамотність – низька обізнаність про технології підвищує вразливість до маніпуляцій;
5. Когнітивне навантаження та стрес – знижують критичне мислення й посилюють упередження;
6. Емоційний стан – страх чи жадоба прискорюють імпульсивні рішення;
7. Дизайн інтерфейсу – колір кнопок, розміщення елементів можуть сприяти “темним патернам”;
8. Обмеження часу – обмежений термін дії пропозицій змушує приймати швидкі рішення під тиском часу [13].

1.3 Дослідження вразливостей корпоративних інформаційних систем до соціоінженерних загроз

На сьогоднішній день кількість кіберзагроз зростає в геометричній прогресії, а з цим і потреба в обізнаності в інтернет-просторі. У зв'язку з тим, що соціоінженерна загроза не є програмним кодом, а напряму залежить від людського чинника, потрібно розуміти, які є можливі вразливості втрати персональних даних і конфіденційної інформації через людину. Поділити вразливості можна на 4 основні категорії, а саме: технічні вразливості – дефекти в інфраструктурі [16], організаційні вразливості – слабкі місця в політиках безпеки та управління ризиками [17], процедурні вразливості – можливість обходу наявних контрольних пунктів [18], вразливості людського фактору – психологія та поведінка співробітників [15] (рис. 1.6).

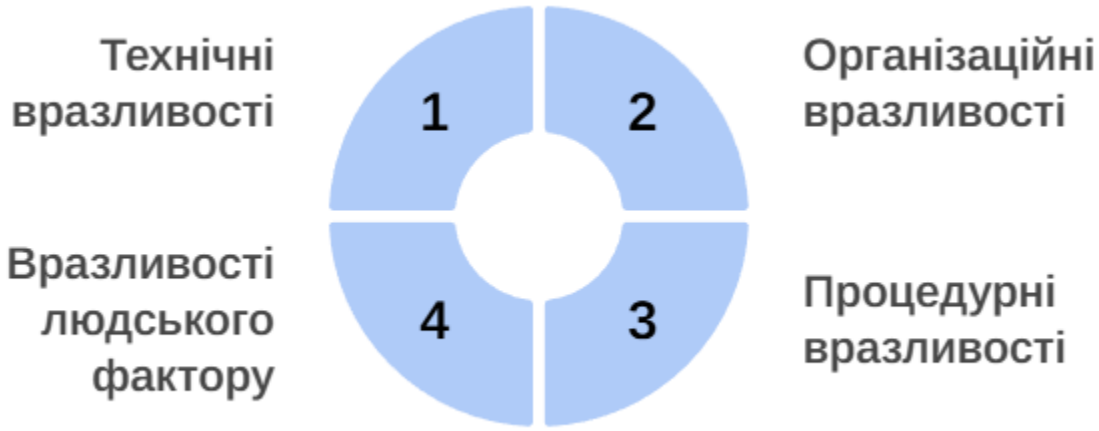

Рис 1.6. Основні вразливості ІКС до соціоінженерних загроз

Типові приклади наведених категорій вразливостей наведені нижче:

1. Технічні вразливості – баги в ПЗ можуть давати змогу виконувати довільний код чи обхід механізмів автентифікації; не налаштовані облікові записи, відкриті порти й неправильні політики міжмережевих екранів створюють "відчинені двері" для зовнішніх атак; відсутність оновлень до актуально важливих патчів залишає систему вразливою до атак; відсутність багатофакторної аутентифікації, використання простих або повторно використовуваних паролів значно підвищують ризик взлому облікових записів;

незашифрований або ненадійно захищений трафік і ненадійні VPN-конфігурації спрощують переспрямування чи перехоплення даних.

CERT-UA відзначає [19], що підприємства часто ігнорують патчі й оновлення публічних сервісів (веб-сайтів, поштових серверів тощо), що полегшує використання відомих уразливостей. У мережах компаній часто бракує сегментації: наприклад, відсутня демілітаризована зона (DMZ), через що компрометація одного сервера може “розповсюджувати” атаку далі. Також небезпечно, коли віддалений доступ (VPN, RDP) відчинений для всіх співробітників без належного контролю – нападник із викраденим паролем без проблем увійде в систему. Не рідкість і неналежний контроль розгортання додатків: використання піратського програмного забезпечення призводить до випадкового встановлення бекдорів та троянів. Таким чином, навіть технічні недоліки перетворюються на сприятливе середовище для соціальних інженерів.

2. Організаційні вразливості – відсутність або застарілі політики безпеки; працівники без регулярного навчання та мотивації повідомляти про підозрілі випадки уповільнюють виявлення та реагування; неналежний розподіл ролей та відсутність керівника процесу безпеки.

Щодо процедур і політик, часто виявляється: відсутня або неефективна внутрішня політика роботи з кібербезпекою. Наприклад, немає чітких інструкцій, як перевіряти незвичні запити або підтверджувати їх іншими каналами зв’язку. Такі “сіра зона” дозволяє шахраям видавати фальшиві накази керівництва, а працівники виконують їх через страх або небажання виглядати неввічливими.

3. Процедурні вразливості – відсутність перевірки запитів дозволяють зловмиснику видавати себе за уповноважену особу; відсутність належного тестування й аналізу ризиків; неправильно класифіковані загрози; затримка з анулюванням прав колишніх співробітників.

4. Вразливості людського фактору – видавання себе за “свого”; відкриття шкідливих посилань або введення пароля на підроблених сайтах;

використання простих паролів, відсутність MFA; неналежне управління доступом до критично важливих ресурсів [15, 16, 17, 18].

Багато компаній мають процеси на папері, але не дотримуються їх. Наприклад, заявлені двофакторна автентифікація та навчання співробітників існують у документах, але на практиці відсутні. CERT-UA констатує [19], що викрадений логін і пароль – це результат типової помилки компаній – відсутність MFA. Аналогічно, більшість організацій не проводять регулярних тренінгів з кібергігієни або ігнорують результати соціоінженерних тестувань. Як наслідок, працівники погано помічають підроблені листи чи телефонні шахрайства. У різних галузях ці слабкості проявляються по-різному.

1.4 Огляд підходів до виявлення, запобігання та реагування на соціоінженерні атаки

Захист від соціоінженерних атак – надзвичайно складне завдання, оскільки в основі цих атак лежить маніпулювання людською психологією. Зловмисники керуються довірою та іншими слабкостями, щоб отримати доступ до бажаного. Це ретельний процес підбору жертви, використовуючи відкриті джерела та соціальні мережі, щоб втертися максимально у довіру, знайти місця, на які можна надавати або ж підсунити те, що жертва проковтне. Окрім цього, соціальні інженери також використовують технічні вразливості, такі як недоліки в програмному забезпечення, що робить стандартні засоби захисту недостатніми. Швидкість та непередбачуваність атак, особливо в умовах стресу, ускладнюють їх виявлення. Недостатня обізнаність про такі методи атак робить людей особливо вразливими, оскільки зловмисники вміло маскуються під знайомих осіб або організації, використовуючи фішинг та інші технічні засоби.

Для початку потрібно розуміти рівень знань користувачів. Таких можна поділити на 4 типи: прагматик, скептик, знавець та простак:

- прагматик [20] – особа яка не сумнівається в своїх знаннях і не буде опиратися на досвід інших. Такий користувач буде вважати, що цьому посиланню можна довіряти, адже нічого такого не помітили з перших секунд, тим паче воно з поміткою “терміново”, тому сумнівів точно не буде;
- скептик [21] – такий користувач знаходиться в постійних сумнівах і буде довга реакція на підозрілі листи і скоріш за все чекатиме ще когось. Може здатися, що цей тип небезпечний в рамках безпеки даних. Але, якщо така людина знає свого співрозмовника короткий час, вона буде прискіпливо до нього ставитися та перевіряти інформацію, що до неї приходить. А це вже можна рахувати за переваги;
- знаток – цей тип людей найважче піддається маніпуляціям, оскільки він завжди знає, з ким він спілкується, але і не забуває піддаватися сумніву та перевіряти все;
- простак – для соціального інженера це найпростіший тип, що підлягає будь яким маніпуляціям та натиску. Такі користувачі абсолютно впевнені в безпеці і вважають, що вони не можуть помилитися. Для такого типу найкраще підходить двофакторна аутентифікація і спеціалізоване програмне забезпечення.

Проте, своєчасне виявлення соціоінженерних атак, що є необхідною умовою для їх успішного запобігання, ускладнюється через брак чітких технічних ознак та велику різноманітність маніпулятивних методів.

Методи виявлення соціоінженерних атак спираються на поєднання технічних засобів: IDS/IPS (Intrusion Detection/Prevention Systems), SIEM (Security Information and Event Management), UEBA (User and Entity Behavior Analytics), а також машинне навчання.

1. IDS/IPS (системи виявлення вторгнень) – це спеціалізоване програмно-апаратне рішення для захисту мережі, яке в режимі реального часу аналізує весь трафік чи дії користувачів, виявляє підозрілі шаблони поведінки та реагує на них: IDS сповіщає адміністратора про потенційну загрозу, а IPS може одразу блокувати підозрілі з’єднання або транзакції. Основна ідея в тому,

щоб бачити весь або ключовий трафік мережі, але не перериває його потік – вона працює пасивно, просто аналізуючи пакети даних. IPS, натомість, розміщується прямо в лінії руху трафіку і може переривати чи перенаправляти підозрілі з'єднання до подальшого аналізу або блокування (рис. 1.7) [23].

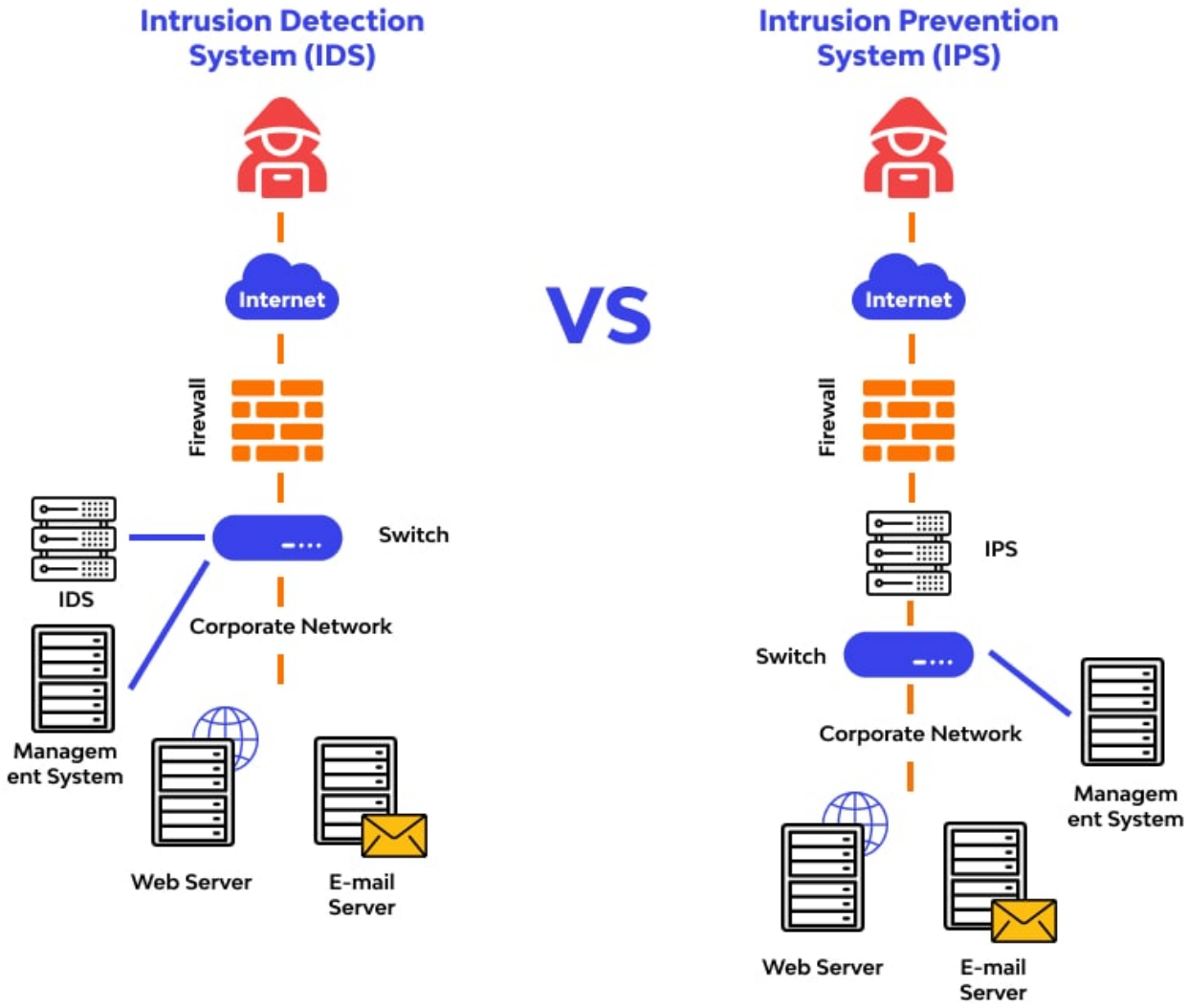

Рис 1.7. Порівняння схеми роботи IDS/IPS [23]

2. SIEM (інформація про безпеку та управління подіями) – системи збирають логи з поштових шлюзів, мережевих пристроїв і кінцевих точок, корелюють події та піднімають оповіщення при виявленні індикатори компрометації (IOC, Indicators of Compromise) – наприклад, масові розсилки електронних листів із незвичних адрес або численні невдалі спроби входу (рис. 1.8). Такі системи дозволяють централізовано аналізувати події й швидко реагувати на інциденти [24].

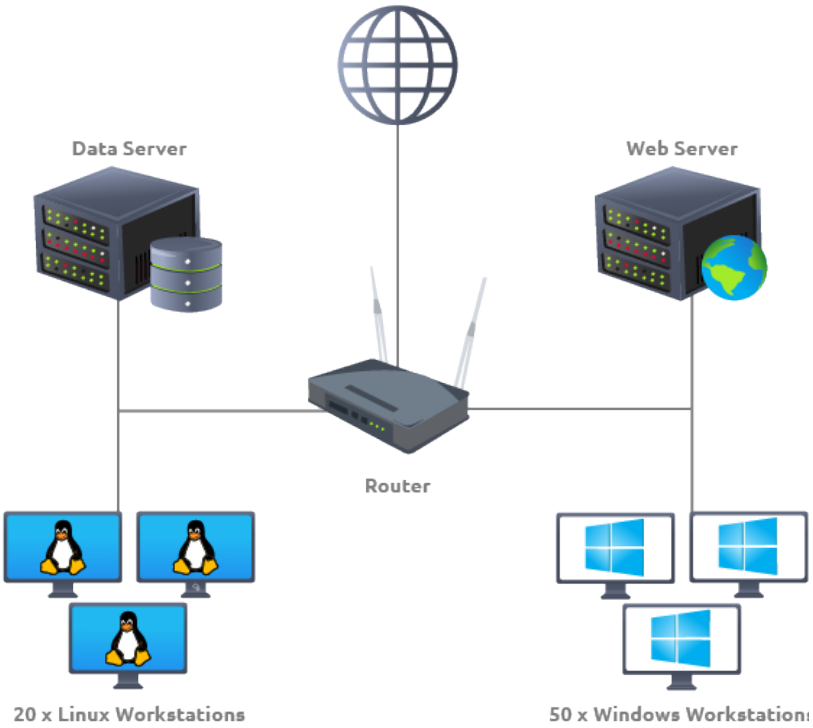

Рис 1.8. Схема роботи SIEM-системи [24]

3. UEBA (аналітика поведінки користувачів та організацій) – це методологія інформаційної безпеки, що займається аналізом поведінки користувачів і пристроїв для виявлення аномалій і потенційно небезпечних дій, які традиційні рішення виявити не можуть (рис. 1.9). UEBA використовує машинне навчання, статистичний аналіз та моделювання нормальної поведінки, щоб встановити базовий профіль кожного об’єкта (користувача, сервера, програми тощо) і згодом ідентифікувати відхилення, що можуть свідчити про компрометацію або внутрішню загрозу [25].

Рис 1.9. Схема роботи UEBA-системи [25]

4. Машинне навчання та штучний інтелект для автоматичної класифікації листів як фішингових або легітимних на основі лінгвістичних та метаданих. Алгоритми аналізують тональність, граматику та структуру повідомлення, виявляючи стилістичні відмінності від звичних для організації шаблонів. Крім того, новітні рішення використовують Deep Learning для розпізнавання діпфейків у голосових й відео дзвінках, що стає дедалі актуальнішим вектором загроз [26].

Однак соціальна інженерія – це атаки, які прикидаються звичайним спілкуванням, щоб завоювати довіру та отримати доступ до інформації. Для протидії цим загрозам необхідний багатошаровий захист, що включає навчання персоналу виявленню шахрайських схем, фільтрацію спаму та фішингу, використання двофакторної автентифікації, захист від перехоплення даних, моніторинг активності та використання надійних паролів. Ефективний захист – це поєднання технічних рішень, навчання та пильності користувачів, що дозволяє створити надійну систему безпеки.

Висновки до розділу 1

У розділі розглянуто соціоінженерні атаки як ключовий тип загроз, що експлуатують психологічні вразливості користувачів. Проаналізовано основні методи маніпуляції, зокрема вплив через авторитет, терміновість, соціальну довіру та інші когнітивні викривлення, що широко застосовуються у таких атаках.

Було ідентифіковано основні чинники сприйнятливості персоналу до соціоінженерних впливів, серед яких особистісні характеристики, рівень інформаційної обізнаності, відсутність підготовки до виявлення шахрайських сценаріїв, а також дефіцит організаційної культури безпеки.

Окрему увагу приділено аналізу поточних недоліків корпоративних інформаційних систем, зокрема відсутності системного навчання співробітників, недостатньому контролю доступу до ресурсів, а також

неформалізованості процедур реагування на інциденти соціоінженерного характеру.

У підсумку досліджено роль технічних засобів запобігання атакам: моделювання атак, систем виявлення та запобігання вторгненням (IDS/IPS), а також засобів централізованого моніторингу подій (SIEM). Доведено, що саме їх комплексне впровадження створює ефективну багаторівневу систему захисту від соціоінженерних загроз.

Загалом, перший розділ сформував теоретичне підґрунтя дослідження, обґрунтувавши актуальність загроз, виявивши механізми їх реалізації та ключові фактори вразливості, що створює підстави для розроблення методичних підходів до їх попередження у наступних розділах.

Розділ 2 МЕТОДИЧНІ ПІДХОДИ ДО ОРГАНІЗАЦІЇ ЗАХИСТУ ВІД СОЦІОІНЖЕНЕРНИХ АТАК У КОПОРАТИВНОМУ СЕРЕДОВИЩІ

Успіх вдалої соціоінженерної атаки переважно базується на втраті пильності та уважності співробітника. Ефективна система протидії загрозам має включати в себе багаторівневу стратегію, яка комбінує технічні підходи безпеки з людським фактором. А безпека організації залежить від того, як вона дотримується принципів побудови системи захисту.

2.1 Визначення принципів побудови системи протидії соціоінженерним загрозам

Результат атаки значно залежить від наявності підготовлених і кваліфікованих співробітників та їх особистої психологічної поведінки.

За даними IBM [30] витоки даних призвели до втрати мільйонів доларів, при цьому середня вартість витоку даних у Сполучених Штатах сягнула 9,44 мільйона доларів. На інфографіці нижче (рис. 2.1), наведені методи кібератак які вартували мільйони доларів, а саме: фішинг; компрометація бізнес-електронної пошти; вразливість у сторонньому ПЗ; вкрадені або скомпрометовані облікові дані; зловмисний інсайдер; неправильні налаштування хмарної інфраструктури; соціальна інженерія; порушення фізичної безпеки; випадкова втрата даних або пристрою; системна помилка.

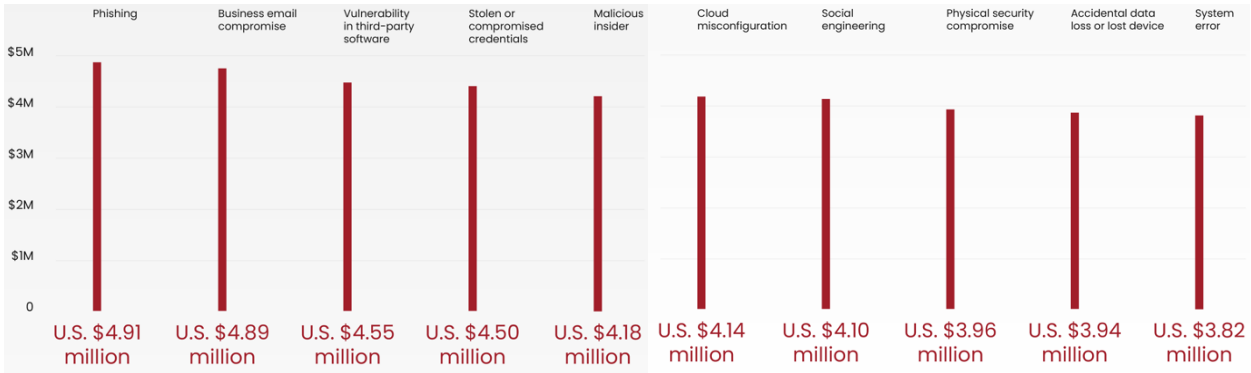

Рис. 2.1. Витік даних в доларовому еквіваленті за 2022 рік [30]

Для побудови системи захисту визначається рівень вразливостей та комплексна оцінка рівня загроз (рис. 2.2).

Рис 2.2. Модель захисту персоналу в корпоративній мережі [26]

Вплив факторів на можливість реалізації соціоінженерної атаки зображено на рисунку 2.3.

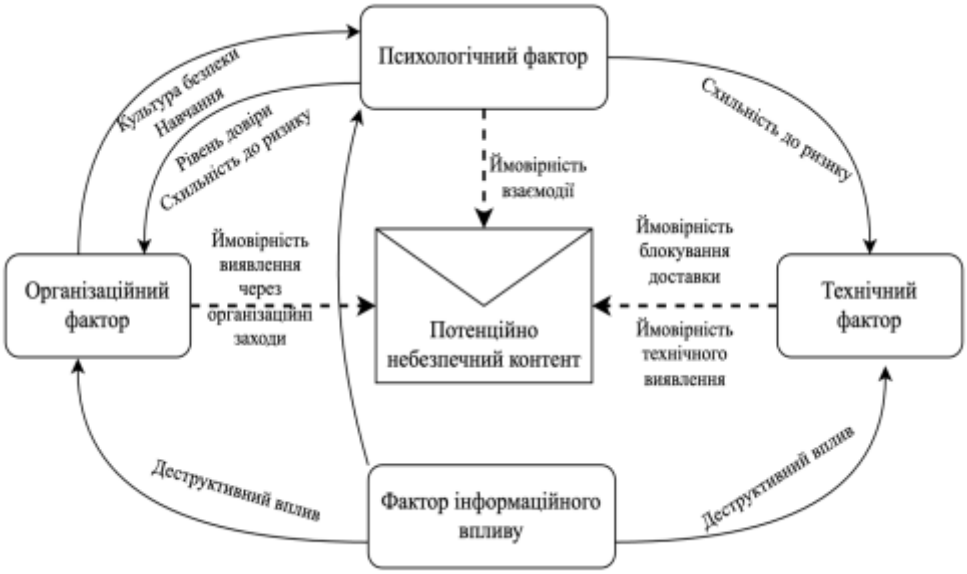

Рис. 2.3. Вплив факторів на можливість реалізації соціоінженерної атаки [26]

Модель спрямована на виявлення уразливих місць, створення рекомендацій щодо подальших дій і застосування заходів для їх уникнення.

Психологічний фактор демонструє індивідуальність особи схильної до соціоінженерного впливу. Це дозволяє розуміти майбутню поведінку користувача у критичних ситуаціях для формування превентивних заходів.

Організаційний фактор відповідає за виконання політик безпеки та ефективність навчання захисту даних. Компанії що проводять на регулярній основі тренінги, не порушують чітке виконання процедур, проводять аудити, створюють план дій на випадок інциденту, кількісно знижують ризик вразливостей своїх співробітників до соціоінженерних атак. Наприклад, аналітичні платформи можуть виявляти нові шаблони фішингових листів або нетипові сценарії зв'язку, після чого автоматично генерувати правила блокування або додаткові перевірки.

Технічний фактор приділяє увагу саме програмним засобам захисту в системі. Розглядаються багатофакторна автентифікація, антивірусне програмне забезпечення, поштові та веб-фільтри, IDS/IPS, засоби управління доступом.

Фактор інформаційного впливу визначає стійкість до маніпуляцій в умовах стресу. Такі явища, як економічна криза, воєнні конфлікти або політична дестабілізація, значно підвищують рівень вразливості користувачів. Оскільки в усіх умовах навколишнього середовища, користувачі приймають рішення без детального аналізу, що призводить до зниження ефективності перевірки отриманої інформації. А це в свою чергу, створює комфортні умови для реалізації соціоінженерних атак [26].

Обов'язково, система має бути ризик-орієнтованою. Це означає, що вибір і інтенсивність заходів мають відповідати оціненому ризику втрати ресурсів. Моделі від NIST CSF [29] і ISO/IEC 27001 [27] передбачають проведення оцінки ризиків (Risk Assessment) і побудову заходів безпеки відповідно до отриманих результатів. Наприклад, стандарт ISO/IEC 27001 рекомендує створювати інформаційну систему управління безпекою (ISMS) з безперервним удосконаленням, що базується на управлінні ризиками. У NIST CSF функція "Ідентифікація" передбачає оцінку середовища та ризиків, тоді як функція "Захист" включає такі категорії, як управління доступом і навчання персоналу.

Застосування цих підходів забезпечує відповідність заходів протидії реальному профілю загроз і бізнес-цілям організації.

2.2 Розробка програм навчання та підвищення обізнаності користувачів

У зв’язку із прогресивним зростанням кількості соціоінженерних атак на користувачів, ключовим принципом боротьби є навчання та підвищення кваліфікації співробітників на постійній основі.

На конференції USENIX SOUPS 2024 продемонстрували результати дослідження стосовно обізнаності користувачів виявляти фішингові листи в залежності від частоти навчання. У ньому розглядалися тренінги з виявлення фішингу та IT-безпеки. Респонденти проходили тести у кілька різних інтервалів часу після проходження відповідного тренінга з кібербезпеки.

Дослідження показало, що через чотири місяці після тренування результати були відмінними. Учасники експерименту точно ідентифікували фішингові електронні листи та уникали їх. Але вже через шість місяців показники почали погіршуватися. Ця тенденція набирала обертів протягом наступних місяців [31].

Згідно рекомендацій Національного інституту стандартів і технологій, підвищення кваліфікації в інформаційній безпеці повинні проходити не лише основний персонал, а й сторонні особи, що мають доступ до інформаційних систем організації [32].

Методологія навчання повинна передбачати поєднання теоретичних та практичних елементів: від ознайомчих лекцій і відеоуроків до інтерактивних тестів і симуляцій. Прикладом успішної практики є Microsoft, де усі співробітники проходять базове навчання з безпеки вже на етапі адаптації і протягом всієї кар’єри. Їхня програма навчання виглядає приблизно таким чином: спершу відбувається ознайомлення з політиками безпеки, загальні поняття про конфіденційність, парольну гігієну. Далі тренінги для різних груп працівників (наприклад, фінансистів – про безпеку фінансових операцій, розробників – про безпеку коду, менеджерів – про управління ризиками).

Короткі навчальні відео, e-mail міні-тренінги про нові загрози, що виходять періодично, тести після модулів, опитування, обговорення інцидентів.

Проте теорія не забезпечить належного рівня підготовки для протидії фішинговим атакам. Для цього потрібно проводити практичні симуляції, які максимально наближають користувачів до реальних сценаріїв атак, що дозволяє краще розуміти потенційні ризики для себе та організації через неуважність або необачність [33].

Рішенням для компаній є використання Gophish [34] або Keepnet Labs' Phishing Simulator [35], які надають змогу створювати персоналізовані фішингові атаки. Аналіз реакції та визначення їх вразливих місць. Це дозволяє не тільки зекономити витрати на залученні зовнішніх спеціалістів, а й можливість постійного вдосконалення користувачів під час симуляцій наближених до реальних.

На прикладі показано використання утиліти Gophish. Після встановлення машини та завершення всіх налаштувань її конфігурації переходимо до створення фішингового листа. Початкова панель налаштування HTML-сторінки зображена на рисунку 2.4.

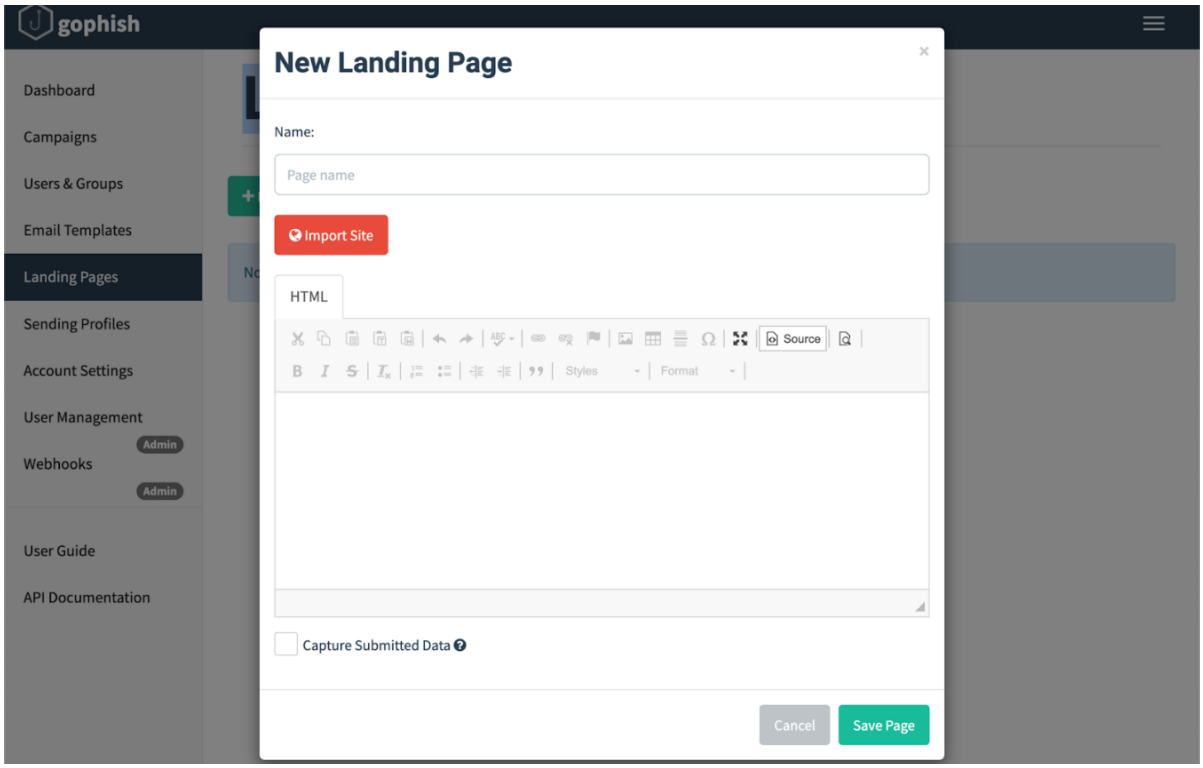

Рис. 2.4. Панель налаштування HTML-сторінки в Gophish [36]

В цьому розділі є можливість створення HTML-сторінки, на які при переході із фішингового посилання потрапляє “ціль” (рис. 2.5).

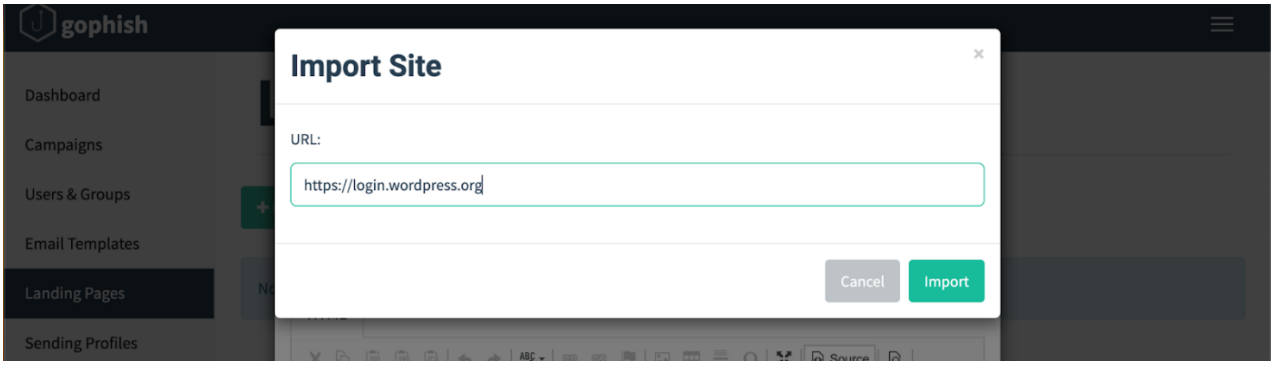

Рис. 2.5. Імпорт сторінки логіну [36]

Після імпорту у візуальному редакторі з’являється копія сторінки логіну. За потреби можна відредагувати цю сторінку, переключившись у режим редагування HTML (рис. 2.6).

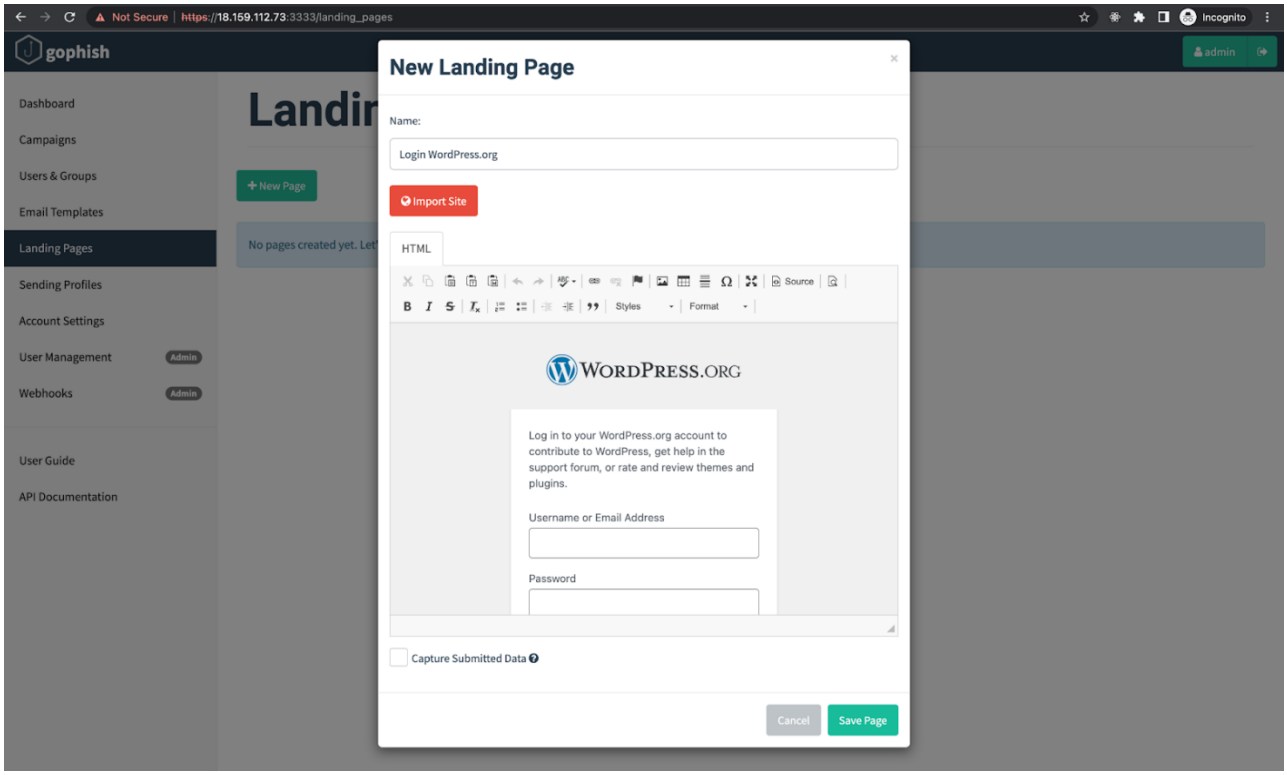

Рис. 2.6. Вигляд сторінки логіну [36]

Оскільки ми зацікавлені у логіні й паролі користувачів, ставимо галочку “Capture Submitted Data” і також ставимо позначку навпроти нового пункту,

який з’явиться, – “Capture Passwords”. Оскільки ми не хочемо викликати підозр навіть коли користувач уже ввів свої дані, вкажемо, щоб “ціль” перенаправлялась на сторінку профілю.

Також є можливість використовувати змінні, які будуть підставляти відповідні значення у конкретний лист ім’я чи email. Ставимо галочку “Add tracking image”, щоб мати статистику про відкриття email потенційними жертвами.

Далі потрібно налаштувати SMTP-сервер, який надсилатиме електронні листи. І останнім кроком додаємо перелік адрес, на які прийде фішингове повідомлення (рис. 2.7).

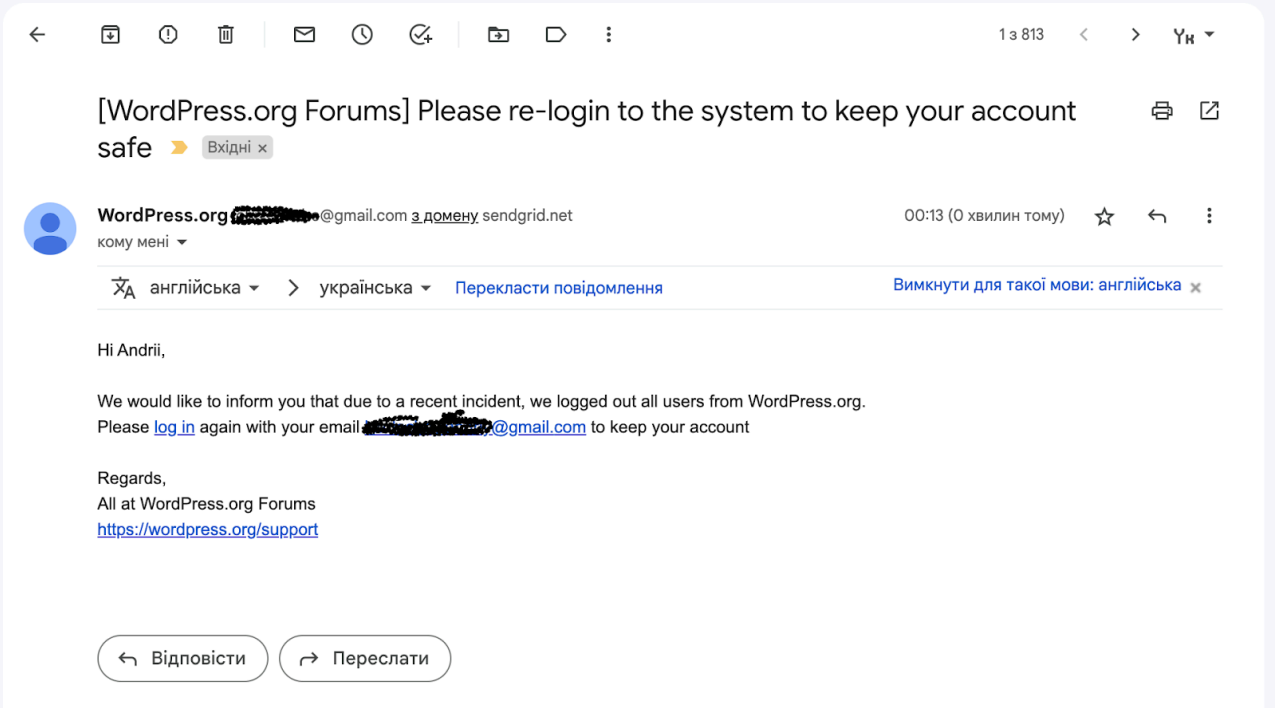

Рис. 2.7. Вигляд створеного фішингового повідомлення [36]

Після переходу по створеному посиланню користувач бачить сторінку входу в систему (рис. 2.8). Додатково є можливість провести повноцінний аналіз: коли був відправлений лист, з якого пристрою відкритий, та дані, які ввів користувач (рис. 2.9).

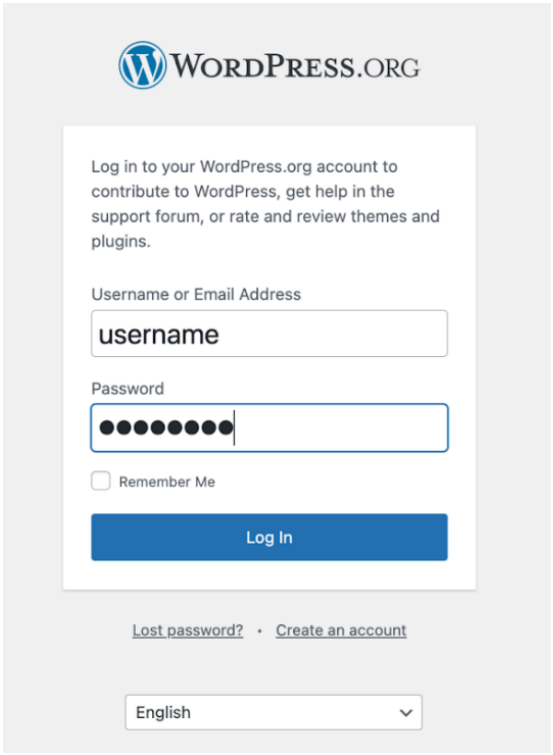

Рис. 2.8. Сторінка після переходу по створеному посиланню [36]

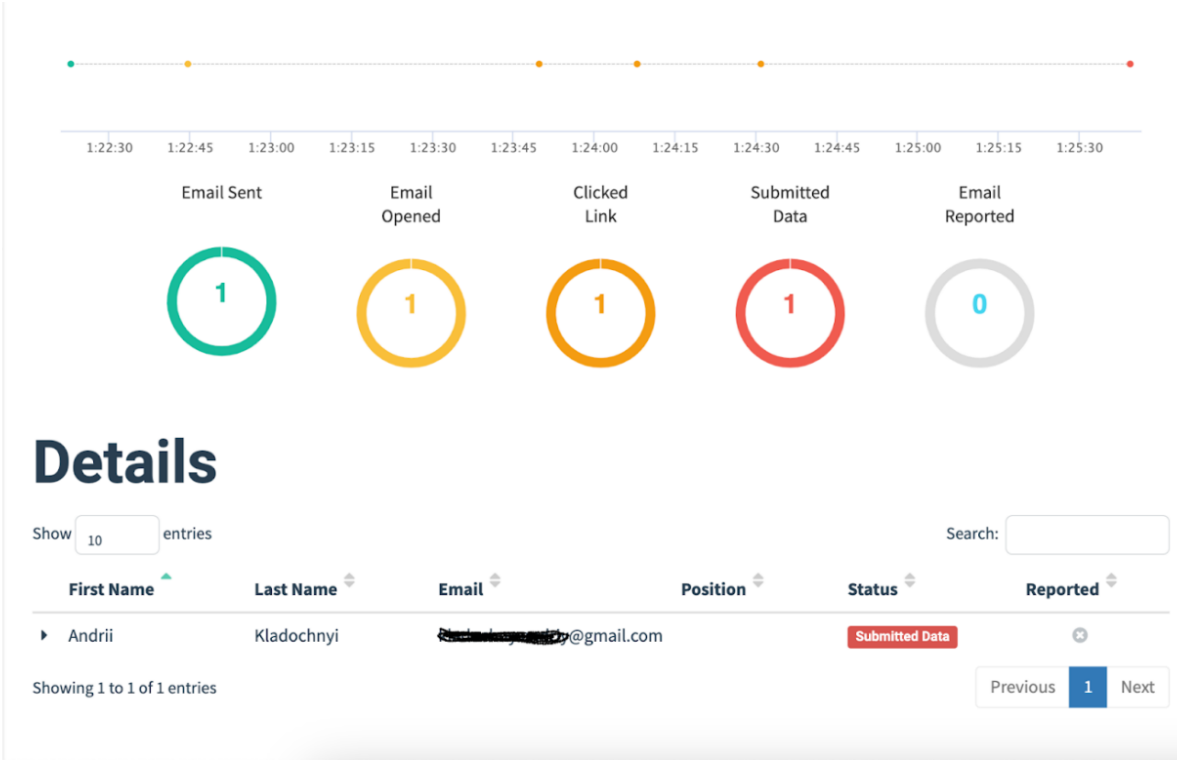

Рис. 2.9. Дашборд Gophish з результатами тестування [36]

2.3 Застосування технічних і організаційних заходів для забезпечення корпоративної безпеки

Окрім навчання, захист від соціоінженерних атак передбачає широкий спектр технічних та організаційних контрзаходів. До них належать засоби контролю доступу, мережеві та поштові фільтри, системи моніторингу, захист кінцевих точок, а також стандарти та політики безпеки.

Організація повинна впроваджувати багатофакторну аутентифікацію (MFA), модель Zero Trust та системи ролей (RBAC) [37] для зменшення ризику несанкціонованого доступу. MFA змушує користувача проходити додаткові перевірки (наприклад, код з мобільного телефону або біометрію), що значно ускладнює використання вкрадених облікових даних, а RBAC гарантує, що користувачі мають лише ті права, що відповідають їхній ролі.

Комплексне застосування політики нульової довіри дає змогу перехоплювати запити, відкрито підтверджувати сигнали для всіх шести основних елементів відповідно до конфігурації й надавати доступ із мінімальними правами (рис. 2.10).

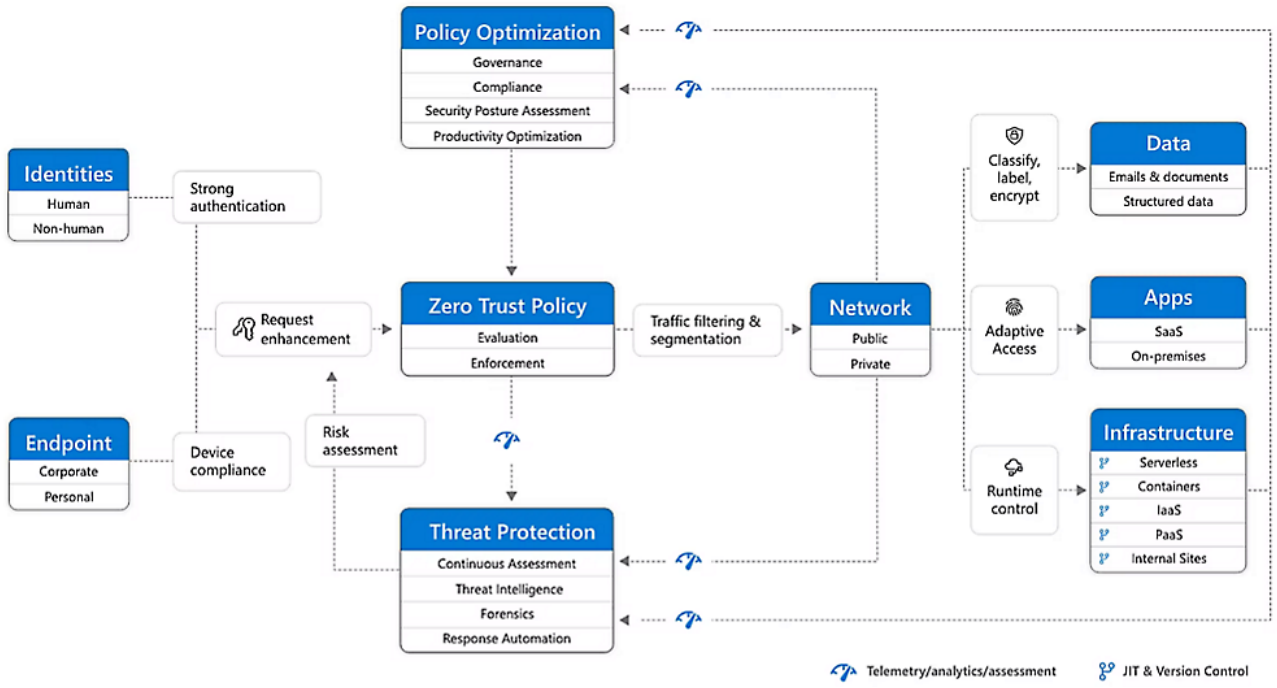

Рис. 2.10. Модель нульової довіри [41]

До сигналів належать ролі користувачів, розташування, відповідність пристроїв вимогам, а також конфіденційність даних і програм. Перш ніж надати доступ до приватної або загальнодоступної мережі, система виконує фільтрування й сегментацію трафіку та застосовує до нього політику нульової довіри.

Популярні рішення Zero Trust наведені на рисунку 2.11.

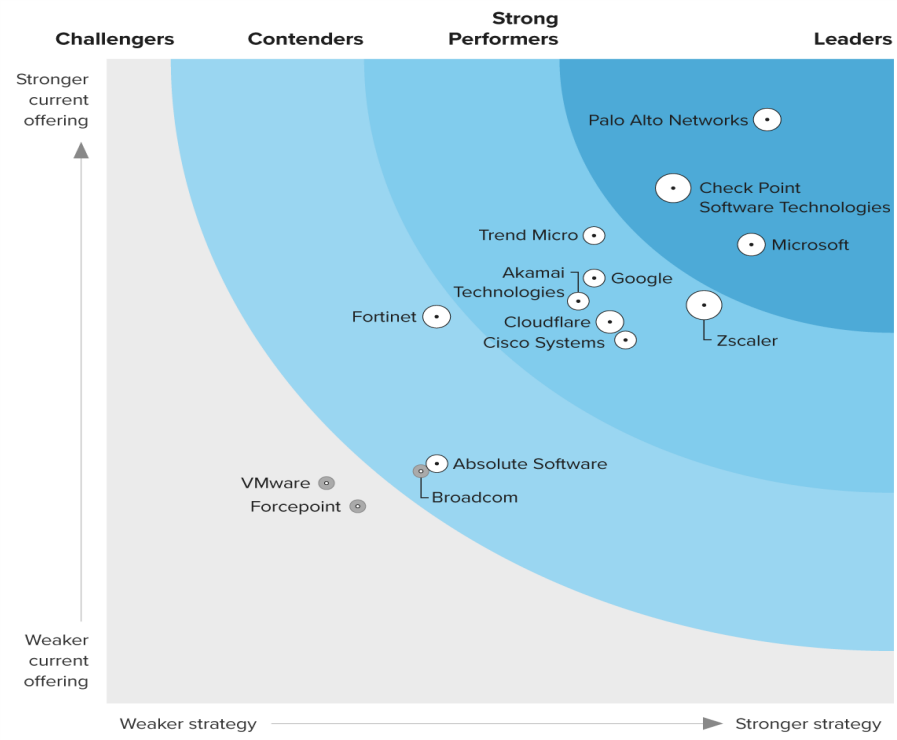

Рис. 2.11. Оцінка Forrester Wave популярних рішень Zero Trust [42]

Усі ці заходи реалізують принцип найменших привілеїв та унеможливлюють переміщення зловмисника всередині мережі.

Також повинні вводитися політики прийому пошти (наприклад, блокування деяких типів файлів, попереджувальні банери в листах ззовні тощо), мережеві й поштові фільтри, що будуть блокувати або відстежувати підозрілий трафік з позаорганізаційних ресурсів. Поштові фільтри на рівні сервера сортують вхідні листи, відсіюючи відомі фішингові шаблони, вкладення з шкідливим ПЗ і підозрілі посилання.

Бажаною умовою є впровадження систем моніторингу та реагування, а саме: SIEM [38], UEBA [39] і SOAR [40] (Security Orchestration, Automation and Response) (рис. 2.12):

- SIEM збирає журнали подій з пристроїв і аналізує кореляції подій;
- UEBA використовує машинне навчання для виявлення аномалій в поведінці користувачів – наприклад, надзвичайно велика кількість введень пароля або нетипова активність після робочого часу;
- SOAR автоматизує процес реагування: коли виявлено підозру, система може одразу ініціювати блокування обліку, сповіщення аналітиків тощо. Такий набір рішень забезпечує швидке виявлення й локалізацію наслідків успішної соціоінженерної атаки.

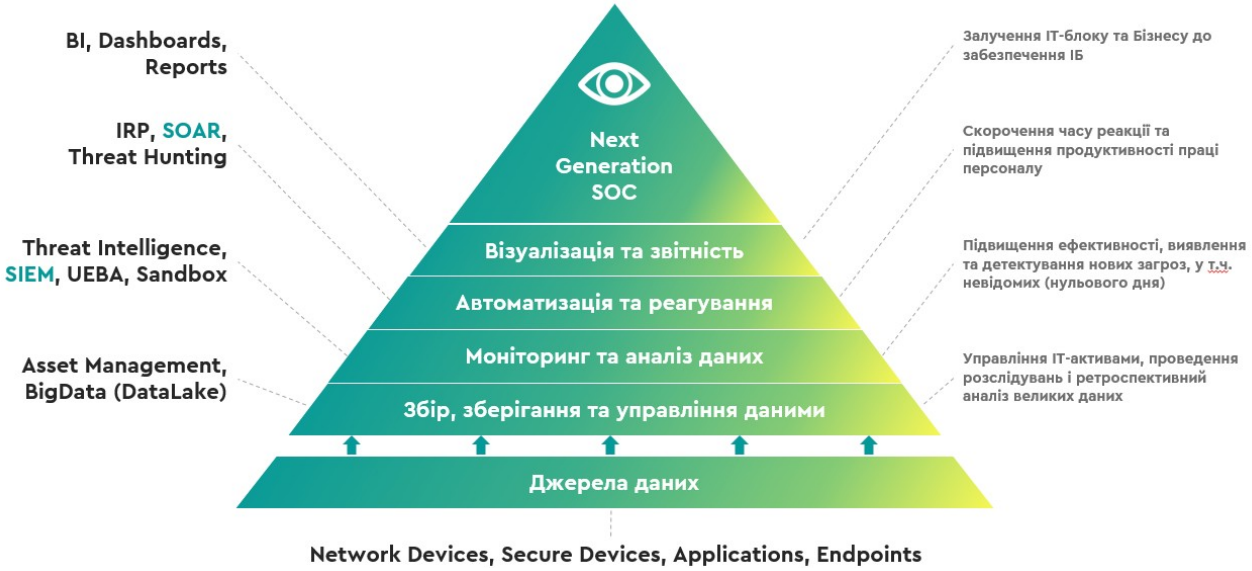

Рис. 2.12. Побудова SOC [31]

Управління доступом та механізми захисту мають бути єдиною комплексною системою. Наприклад, навіть якщо зловмисник переконає працівника розкрити пароль, MFA та політика найменших привілеїв не дозволять завдати серйозної шкоди. Наявність міжнародних стандартів ISO/IEC 27001/27002 [27] та рекомендацій NIST CSF [29], COBIT [28] допомагають формалізувати ці заходи в організації і перевіряти їх відповідність найкращим практикам. В цілому, комбінація технічних рішень (MFA, фільтри, SIEM, шифрування) і організаційних заходів (політики, аудит доступів, управління змінами) створює надійну протидію соціальній інженерії в корпоративному середовищі (табл. 2.1).

Таблиця 2.1

Засоби контролю доступу

Спосіб захисту	Визначення	Засіб
MFA	Підвищення впевненості в ідентичності користувача за рахунок додаткових факторів (пароль + код, біометрія)	SMS-код, апаратний токен, біометричний зчитувач
RBAC	Призначення прав за ролями, зменшення надлишкових привілеїв	Active Directory групи безпеки, IAM ролі в хмарі
Файрвол	Блокування небажаного вхідного/вихідного трафіку	Network firewall, корпоративні проксі
Антивірус	Виявлення та нейтралізація шкідливого ПЗ на пристроях	CrowdStrike, Microsoft Defender for Endpoint
SIEM/UEBA	Збір подій, кореляція, пошук аномалій	Splunk, IBM QRadar, Exabeam
Поштові та веб-фільтри	Фільтрація небезпечної пошти за визначеними правилами	Proofpoint, Microsoft Defender for Office365
Шифрування даних	Захист конфіденційної інформації при зберіганні/передачі	BitLocker, TLS, VPN

2.4 Встановлення критеріїв оцінювання ефективності впроваджених заходів захисту

Для забезпечення безпеки системи протидії соціоінженерним атакам важливо впроваджувати не лише заходи, а й сформувати чітку схему оцінювання, за якими можна об’єктивно проводити оцінку користувачів.

Ефективність заходів з підвищення обізнаності користувачів щодо соціоінженерних атак оцінюється через поняття результативності, ефективності та впливу. Результативність означає ступінь досягнення цілей програми – наскільки зменшилась частка успішних фішингових спроб завдяки навчальним ініціативам. Ефективність пов’язана з раціональністю витрат ресурсів: співвідношенням результатів навчання до витрат часу та бюджету. Вплив демонструє ширший ефект, зокрема зниження організаційного ризику або покращення захисної поведінки персоналу [43].

ISO/IEC 27004:2016 визначає загальні вимоги до моніторингу та вимірювання продуктивності ІБ та ефективності системи управління інформаційною безпекою. Згідно з цим стандартом, організація повинна сформулювати показники які потрібні для оцінки ефективності. Результати

вимірювань повинні допомагати бізнесу приймати рішення щодо покращення ІБ. Наприклад, стандарт наводить приклад метрики розподілу ресурсів (Annex B.2) – співвідношення фактично використаних ресурсів до запланованих. Подібним чином для оцінки навчальних ініціатив ISO 27004 рекомендує визначати зрозумілі показники залученості та результатів.

В Додатку В ISO/IEC 27004:2016 наведено низку прикладів конструкцій вимірювань для різних процесів ІБ. Зокрема, щодо обізнаності та навчання персоналу прикладними є метрики із пунктів B.11–B.15. B.11 (ISMS training/awareness) – показник обізнаності, що визначається як відсоток співробітників, які пройшли необхідне навчання з інформаційної безпеки.

У цьому прикладі стандарту пропонується розраховувати два показники: I1 – частка працівників, що отримали базове навчання (I = (отримали / повинні отримати)×100), і I2 – частка оновлення знань (II = (поновили / всіх в межах обсягу)×100). Цільові пороги визначаються так: Green – коли I1>90% і I2>50%, Yellow – проміжні значення, Red – значно нижче. B.12 (Information security training) орієнтована на оцінку виконання обов’язкового щорічного навчання: відсоток співробітників, які пройшли навчання протягом року, (% = (пройшли / повинні)×100) і щорічними порогами 90–100% (Green), 60–90% (Yellow), <60% (Red). B.13 (Awareness compliance) фокусується на виконанні політик обізнаності: % тих, хто підписав угоду про ознайомлення. B.14 (Awareness campaigns effectiveness) – на тестуванні знань після кампаній: це відсоток співробітників, що успішно склали короткий тест після навчальної кампанії з ІБ.

У прикладі ISO 27004 пропонують, наприклад, надати вибірці працівників тест до і після кампанії і розрахувати відсоток тих, що набрали прохідний бал. Вважається, що при результаті ≥90% більшість працівників добре засвоїли матеріал (зелений рівень), 60–90% – достатньо (жовтий), <60% – необхідне повторне навчання (червоний). Найбільш близькою до соціоінженерних атак є B.15 (Social engineering preparedness) – метрика підготовленості до реальних атак. Цей показник визначено як відсоток співробітників, що коректно відреагували на симульований соціоінженерний

тест, не натиснули на шкідливе посилання або повідомили про підозрілий лист. У прикладі стандарта для B.15 пропонується декілька проміжних параметрів:

a = (співробітники, які натиснули на посилання / учасники),

b = 1 – (співробітники, які повідомили про небезпечний email / учасники),

c = (співробітники, які, натиснувши на посилання, почали вводити пароль / учасники).

Далі формується зважений сумарний показник d цих параметрів за характером тесту. Наприклад, чим менше вийде d, тобто більша частка співробітників правильно ідентифікувала атаку, тим кращий результат. Цільові значення для d в ISO наведені так: 90–100% (Green), 60–80% (Yellow), 0–60% (Red). Частина організації створює учасників для щомісячних чи щоквартальних симуляцій, звітуючи про кількість клікнули та повідомили [44].

Оцінка ефективності заходів безпеки здійснюється за допомогою метрик, ключових показників (KPI) та аналітичних індексів. Прикладом таких критеріїв є SOC-метрики, показники обізнаності персоналу, середні часи виявлення та реагування, а також комплексні індекси кіберстійкості.

Заходи безпеки зазвичай оцінюють через роботи Security Operations Center (SOC [52]). Набір типових метрик включає кількість виявлених інцидентів, частку помилкових спрацювань, середню кількість інцидентів на аналітика, а також середній час реагування. Наприклад, Splunk зазначає, що такі показники, як Mean Time to Resolve (MTTR) та Mean Time to Detect (MTTD), дозволяють оцінити, наскільки швидко SOC-операції виявляють і вирішують інциденти. METRIC MTTR (час до повного вирішення) показує швидкість відновлення після атаки, а MTTD вимірює середній час від початку події до її виявлення. Коротші значення цих метрик свідчать про більш ефективні процеси виявлення та реагування. У рамках SOC відстежуються також MTTA (mean time to acknowledge) та MTTI (mean time to investigate) для детального аналізу інцидентів [53].

Окрім технічних метрик, важливо вимірювати ефективність навчальних програм. Типові KPI включають відсоток працівників, які успішно пройшли

навчальні курси, співвідношення виявлених співробітниками потенційно небезпечних листів до загального числа отриманих, кількість інцидентів соціальної інженерії, що були припинені завдяки звітуванню користувачами, тощо.

Наприклад, можна відслідковувати Click-Rate – частку користувачів, що натиснули на підозрілі посилання під час симуляцій, та Report-Rate – частку тих, що повідомили про атаку. Зниження Click-Rate із часом свідчить про підвищену обізнаність персоналу. Також використовують тестування з контрольними питаннями після навчань, сертифікацію з інформаційної безпеки або опитування для зворотного зв'язку.

Для процесів розслідування кіберінцидентів визначаються математичні формули. Формула MTTD (Mean Time to Detect) – середній час, який проходить від початку інциденту (тобто фактичного моменту його виникнення) до моменту, коли інцидент було виявлено засобами моніторингу або вручну проаналізовано персоналом. Може бути записана як:

$$MTTD = \frac{\sum_{i=1}^{N}(t_{\text{виявлення}} - t_{\text{початок}})}{N}, \quad (2.1)$$

де $t_{\text{початок}}$ – час початку інциденту, $t_{\text{виявлення}}$ – час виявлення інциденту, N – загальна кількість зареєстрованих інцидентів за визначений період [54, 55].

Формула MTTR (Mean Time to Respond або Resolve) – це середній час, який проходить від моменту виникнення інциденту до його повного усунення, включаючи аналіз, ізоляцію, нейтралізацію та відновлення нормального функціонування системи. Можна записати так:

$$MTTR = \frac{\sum_{i=1}^{N}\left(t_{\text{впровадження}} - t_{\text{виявлення}}\right)}{N}, \quad (2.2)$$

де $t_{\text{виправленння}}$ – час повного усунення інциденту, $t_{\text{виявлення}}$ – час виявлення інциденту, N – загальна кількість зареєстрованих інцидентів за визначений період [55].

Висновки до розділу 2

У розділі визначено ключові принципи формування системи протидії соціоінженерним атакам. Зокрема, наголошено на доцільності застосування багаторівневого захисту, ризик-орієнтованого підходу до управління вразливостями, а також інтеграції технічних і організаційних заходів в єдину систему інформаційної безпеки.

Сформовано вимоги до навчальних програм для підвищення обізнаності працівників, які базуються на комбінації теоретичних тренінгів та практичних симуляцій фішингових атак. Такий підхід дозволяє не лише забезпечити засвоєння знань, але й сформувати сталі поведінкові реакції на типові соціоінженерні сценарії.

Розглянуто сукупність технічних (багатофакторна автентифікація, фільтрація пошти, контроль доступу) та організаційних (впровадження політик, аудитів, планів реагування) заходів, які, у взаємодії, спрямовані на мінімізацію як людського фактору, так і вразливостей інформаційної інфраструктури.

Окрему увагу приділено розробці критеріїв оцінювання ефективності впроваджених заходів, серед яких: рівень охоплення навчанням, показники успішного виявлення атак у симуляціях, а також динаміка змін поведінкових характеристик персоналу. Ці метрики створюють підґрунтя для регулярного моніторингу результативності та адаптації стратегії захисту до нових загроз.

Загалом, другий розділ визначає методичну основу розроблення та впровадження практичних інструментів захисту від соціоінженерних атак, що забезпечує логічний перехід до емпіричної перевірки запропонованих рішень у наступному розділі дослідження.

Розділ 3 ПРАКТИЧНА РЕАЛІЗАЦІЯ МЕТОДІВ ПРОТИДІЇ СОЦІОІНЖЕНЕРНИМ АТАКАМ У КОРПОРАТИВНІЙ ІНФОРМАЦІЙНІЙ СИСТЕМІ

У третьому розділі зосереджено увагу на практичній реалізації раніше розроблених методів протидії соціоінженерним атакам у корпоративній інформаційній системі. Основна мета цього розділу – перевірити ефективність запропонованих підходів в умовах реального підприємства, ідентифікувати критичні вразливості, а також оцінити рівень підготовки персоналу до виявлення та відбиття соціоінженерних загроз.

Буде проведено комплексний аналіз поточного стану безпеки системи, враховуючи що людина і є ключовим важелем всієї організації. А далі будуть продемонстровані результати досліджень та рекомендації стосовно уникнень усіх ризиків та навчанню персоналу.

3.1 Аналіз поточного рівня стійкості корпоративної системи до соціоінженерних атак

Безперебійна робота будь якої корпоративної системи напряму залежить від обізнаності співробітників і налагодженої безпеки захисту. На цьому етапі особливо важливо зрозуміти де критично не вистачає знань, а де не має контролю доступу.

Для визначення рівня безпеки, було проведено тестування усіх співробітників компанії ТОВ “MegaTech Distribution” і тест на фізичне проникнення, відомий як tailgating або piggybacking. Фізичне тестування проводилося за допомогою сторонньої особи, не пов’язаною із співпрацею цієї організації. А для визначення обізнаності, був проведено опитування на розуміння фішингу і які його методи та прийоми.

Під час перевірки безпеки корпоративних приміщень, стороння особа, яка не мала жодного дозволу, успішна пройшла повз пункт охорони,

скориставшись моментом, коли охоронця відволікли та відсутністю камер, спокійно зайшла на склад. І так само але вже назад, разом із обладнанням покинула територію. Стосовно головного офісу ситуація повторилася. Двері завжди відчинені і будь який охочий може зайти і нести потенційну небезпеку.

Тест показав, що відсутність турнікетів, камер спостереження, електронного замку повністю суперечить принципам багаторівневого захисту, що може призвести до викрадення конфіденційних документів, крадіжки обладнання.

Для визначення обізнаності співробітників (у кількості 18 осіб) було створено онлайн анкету на 8 загальних питань, використовуючи Google Forms [45]. Оцінювалося у відповідності: 1 – правильна відповідь; 0 – неправильна відповідь (рис. 3.1).

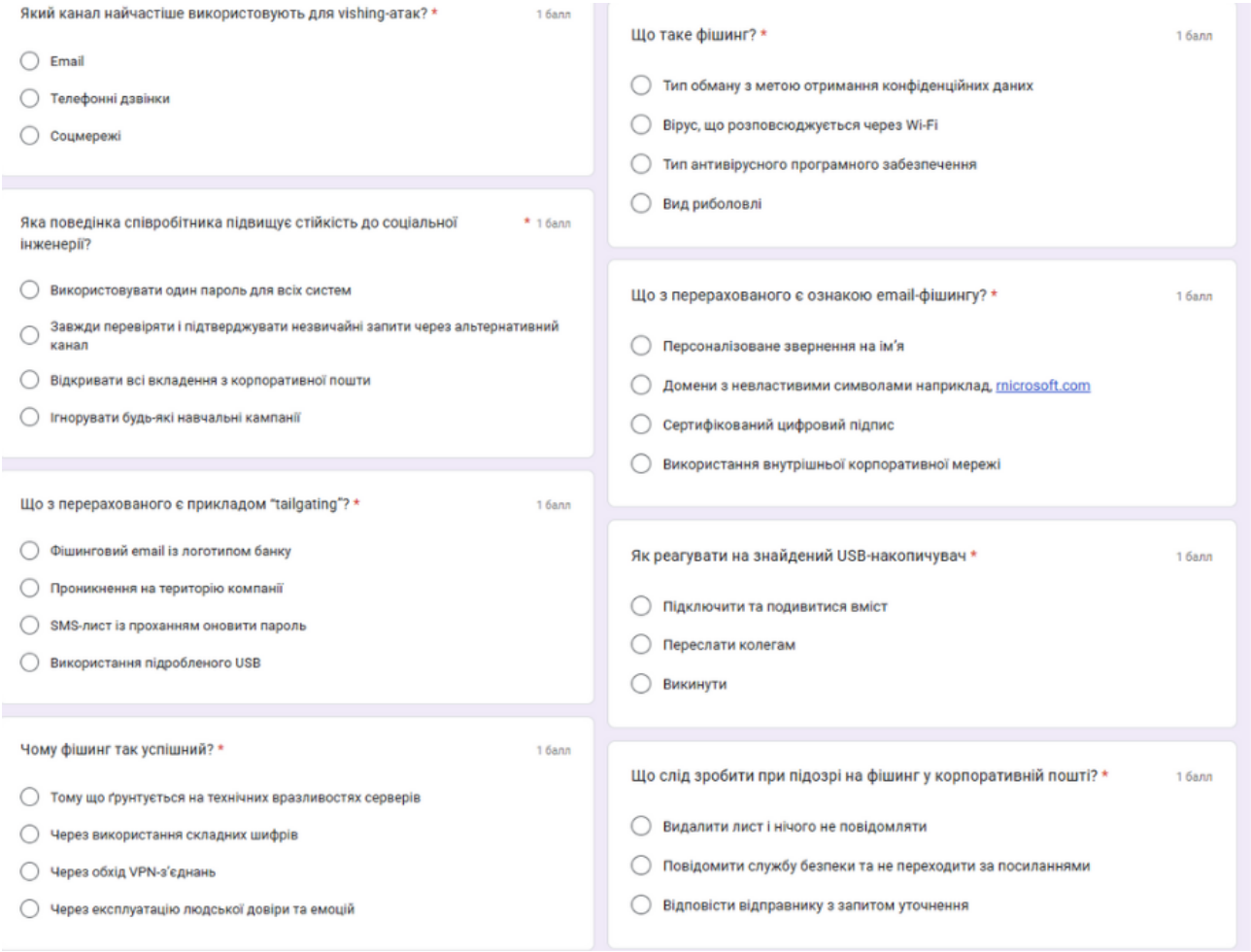

Рис. 3.1. Перелік питань для визначення обізнаності співробітників

Згідно отриманих даних, можна зробити висновок, що компанії потрібно проводити тренінги та симуляції, оскільки з 18 осіб, коректно на всі питання відповіло лише 3. 12 співробітників відповіли правильно на 5,6 питань, а ще троє отримали результат менше 4 правильних відповідей. Середня правильна кількість відповідей дорівнює 66%.

Також в якості експерименту був відправлений лист на пошту кожному співробітнику (рис. 3.2), від CRM системи Odoo, в якій працює організація з наказом про оновлення паролю, оскільки обліковий запис було “зламано”.

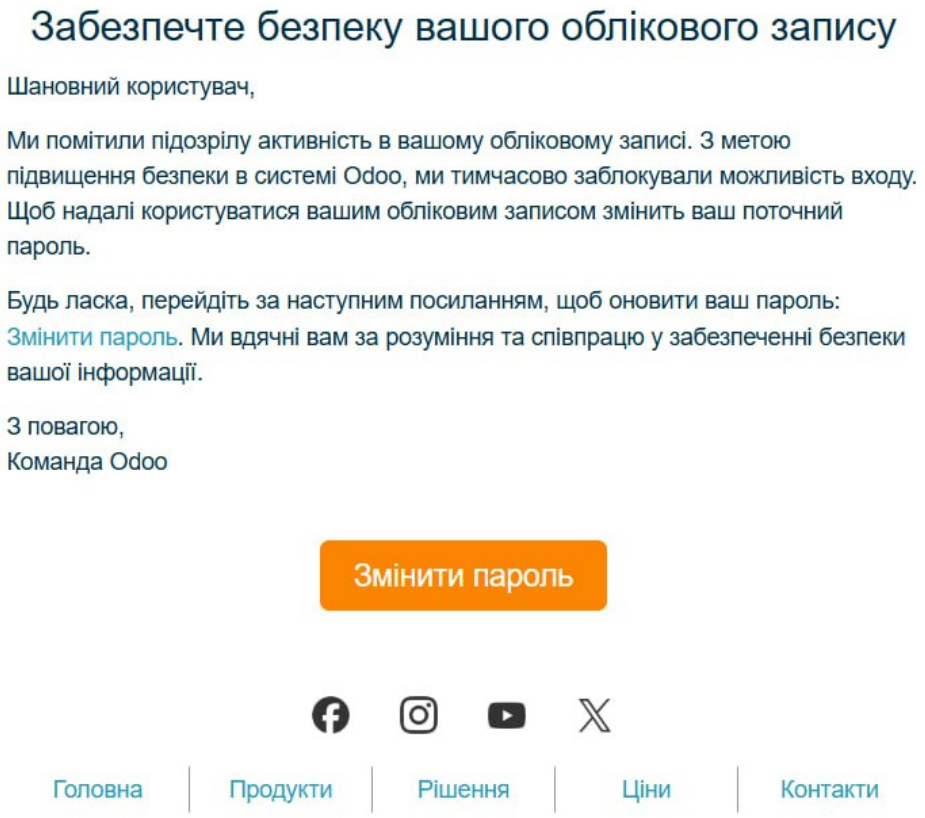

Рис. 3.2. Текст фішингового листа

Після отримання всіма цього листа, було отримано такі результати (табл. 3.1):

Таблиця 3.1

Результати аналізу реакцій співробітників на фішинговий лист

Слова співробітників	**Шкала оцінки**	**Кількість осіб**
Чомусь не грузиться сайт за посиланням	0 - погано	5
Ігнорування листа	0.3 - не погано	3
Перевірив(ла) відправника, не зрозумів і перепитав у відділі IT.	0.7 - добре	7
Одразу помітив(ла) фейк і повідомив про це.	1 - чудово	3

3.2 Виявлення критичних уразливостей і планування комплексу контрзаходів

Враховуючи результати внутрішньої перевірки і симуляцій у ТОВ “MegaTech Distribution”, можна охарактеризувати ключові категорії вразливостей:

1. Фізичний доступ: відсутність системи контролю доступу до складу та офісу призвела до успішного проникнення сторонньої особи. Двері не обладнані електронними замками, а зона ссладу позбавлена камер спостереження.

Відповідно до стандарту ISO/IEC 27001, критичні активи мають охоронятися в межах визначених периметрів безпеки – склади та серверні приміщення необхідно віднести до зони підвищеного захисту з чіткими правилами доступу [47].

2. Фішингові загрози: під час тестових розсилок понад 60 % співробітників натискали на фішингові посилання в імітаційних листах, що свідчить про низький рівень розпізнавання соціоінженерних атак.

Для кожної категорії розроблено план подальших дій, що враховує ймовірність експлуатації вразливості та потенційний вплив на бізнес-процеси.
Далі, згідно з NIST SP 800-53 Rev. 5 [48], для фізичного захисту пропонується встановити електронні контролери доступу із журналізацією вхідних/вихідних подій. Кожному співробітнику видається токен який прив’язаний за фото та іменем, що унеможливлює передачу засобу доступу стороннім особам. Також обов’язкове встановлення камер відеоспостереження для цілодобового моніторингу руху офісі та на складі.

Для протидії фішинговим загрозам передбачається обов’язкове застосування двофакторної аутентифікації та проведення симуляцій атак.

3.3 Впровадження навчальних, організаційних та технічних рішень

На основі запропонованих контрзаходів вводяться навчальні заходи для підвищення обізнаності. Поквартально будуть проводитися онлайн-модулі, внутрішні опитування, короткі лекції з обговоренням актуальних проблем і загроз, практичні вправи із протидії реалістичним фішинговим розсилкам (без попереджень), вступні курси для нових співробітників. Результати тренінгів регулярно фіксуються та перевіряються. Таким чином це відповідає вимогам ISO 27001 A.7.2.2 про освіту і підвищення обізнаності [49].

Для організаційних рішень розробляються та оновлюються політики та процедури, що пов’язані із забезпеченням безпеки. Введення відповідальної особи – менеджера з інформаційної безпеки, який відповідає за оновлення патчів, видачу пропусків, ведення журналу відвідувань. Спостереження за відвідувачами відповідно до NIST як PE-2 і PE-3. Співробітникам надаються права лише на їх зону відповідальності. Обов’язкова багатофакторна аутентифікація для всіх облікових записів, поштових скриньок, віддаленого доступу. Виключення прав локального адміністратора, що значно зменшує ризик встановлення шкідливого програмного забезпечення. Налаштування антифішингових фільтрів і протоколів. Впровадження регулярного резервного копіювання.

Технічними рішеннями є встановлення електронного замку на всі двері. Видача ключ-карти, яка підв’язана під конкретну особу зі своїми правами доступу. Нижче наведена рекомендація, якого типу має вигляд СКД (рис. 3.3).

Рис. 3.3. Електронний замок U-PROX [50]

Також обов’язковою умовою є монтаж IP-камер, які забезпечать постійний нагляд із можливістю перегляду у реальному часі з будь якого пристрою (рис. 3.4).

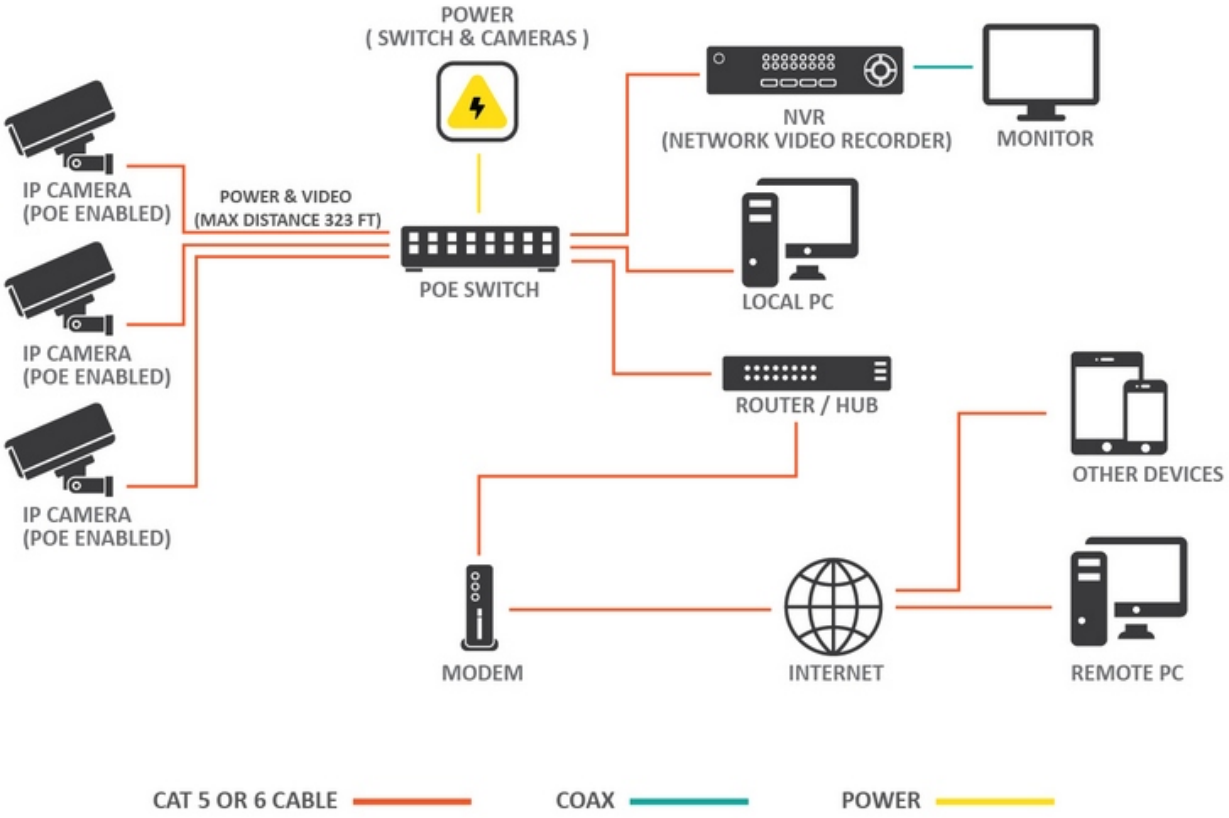

Рис. 3.4. Схема підключення IP камер [51]

Таким чином керуючись усіма рішеннями контрзаходів, мінімізується ризик крадіжка обладнання, проникнення на територію, викрадення та злом корпоративної пошти і конфіденційних матеріалів.

3.4 Оцінювання результатів реалізації та визначення напрямів удосконалення системи протидії

Враховуючи всі тести, симуляції, лекції, доцільно буде провести ще одне опитування на засвоєння матеріалу, що в майбутньому допоможе формувати подальші рекомендації стосовно навчання та подання інформації (рис. 3.5).

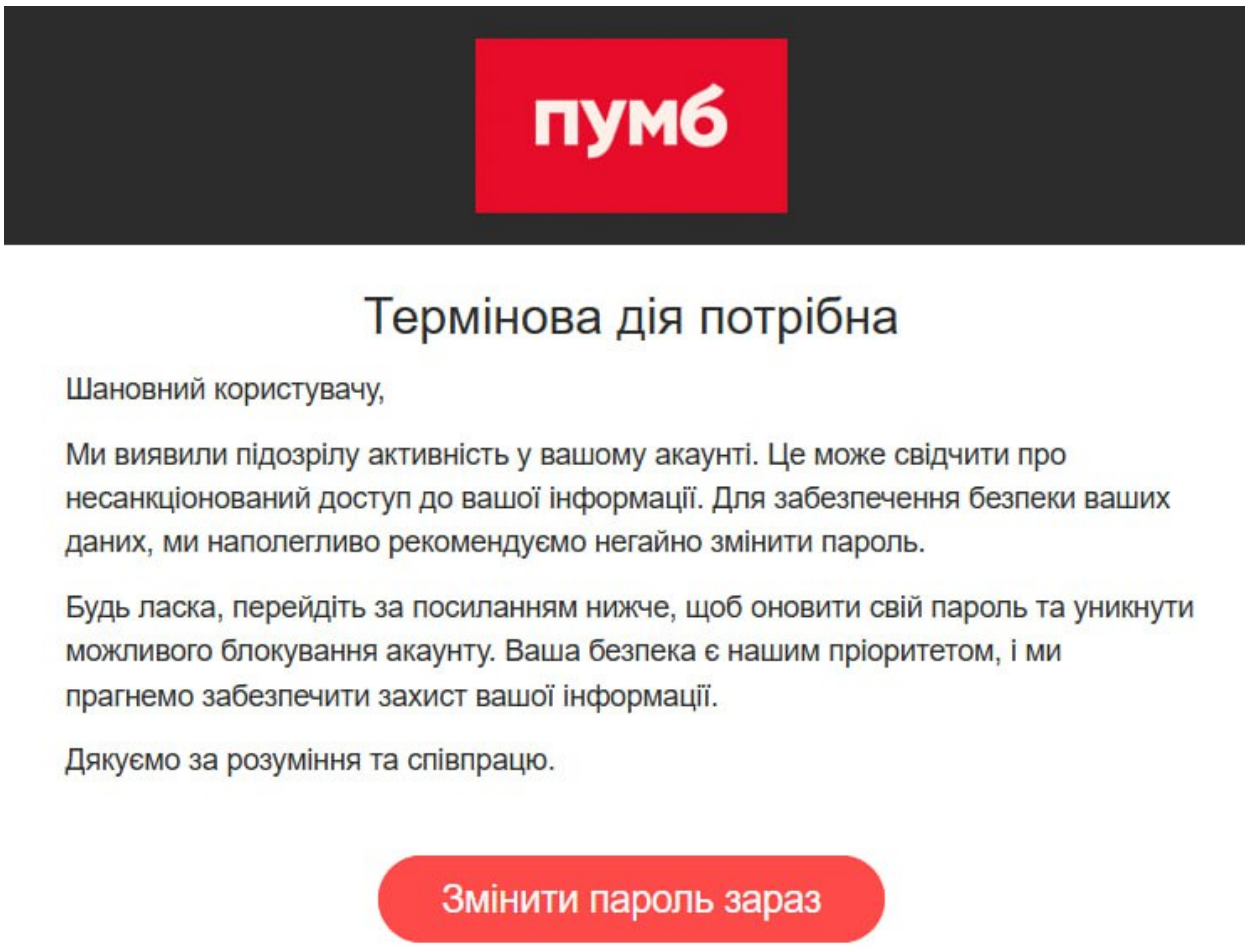

Рис. 3.5. Текст фішингового листа

Щоб переконатися в засвоєнні матеріалу було надіслано повторно усім співробітникам підроблений лист про зміну паролю від імені банку “ПУМБ”. Дослідження показало що всі співробітники засвоїли минулий досвід і одразу звернулися до відділу ІТ і також самостійно перевірили лист на оригінальність (табл. 3.2).

Таблиця 3.2

Результати аналізу реакцій співробітників на фішинговий лист

Реакція співробітників	**Шкала оцінки**	**Кількість осіб**
Одразу помітив(ла) фейк, перевірив(ла) ім’я відправника, звірили і повідомив про це відповідальних осіб.	1 - чудово	18

Також повторно проведено тестування на розуміння фішингових повідомлень у вигляді онлайн опитування [46]. Потрібно визначити кожен з п’яти електронних листів чи є він фішинговим або ж справжній (рис. 3.6 – 3.15).

Рисунок 3.6 демонструє перший сценарій тестування.

[Legal Compliance] Негайно оновіть політику конфіденційності

Шановний користувачу,

Згідно з оновленням GDPR та внутрішніх регламентів ISO/IEC 27001, вам необхідно пройти оновлену політику конфіденційності.

Перейдіть за наступним посиланням та натисніть “Підписати”:

🔗 **https://secure.docs-legalcorp.com/gdpr2025**

У разі невиконання вимоги до 17:00 сьогодні, ваш обліковий запис буде тимчасово деактивований.

Дякуємо за відповідальність.

— Юридичний відділ

Рис 3.6. Перший сценарій тестування

Результати оцінки за першим сценарієм зведені на рисунку 3.7 (16 вірних відповідей).

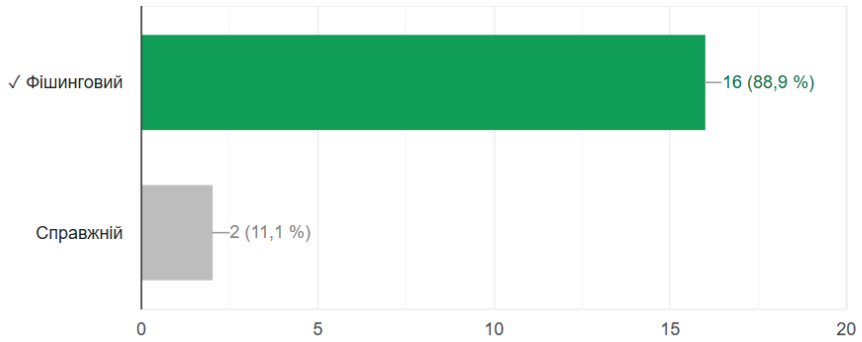

Рис 3.7. Правильних відповідей в межах першого сценарію тестування

Рисунок 3.8 демонструє другий сценарій тестування.

FWD: Інвойс постачальника “Trinetra Systems GmbH” — Уточнення

Привіт, Іване,

Надсилаю повторно рахунок від Trinetra за травень. Схоже, що виникла розбіжність у сумі. Можеш глянути і підтвердити?

📎 **Invoice_Trinetra-2305.pdf**

Дякую!

— Катерина
бух.відділ

(переслано з: finance@trinetra.systems)

Рис 3.8. Другий сценарій тестування

Результати оцінки за другим сценарієм зведені на рисунку 3.9 (13 вірних відповідей).

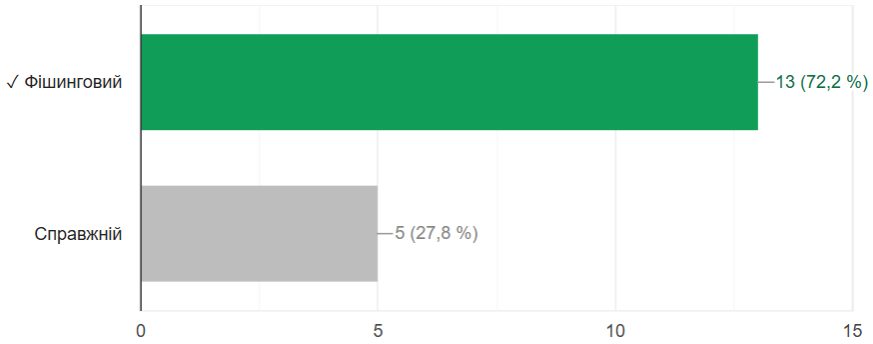

Рис 3.9. Правильних відповідей в межах другого сценарію тестування

Рисунок 3.10 демонструє третій сценарій тестування.

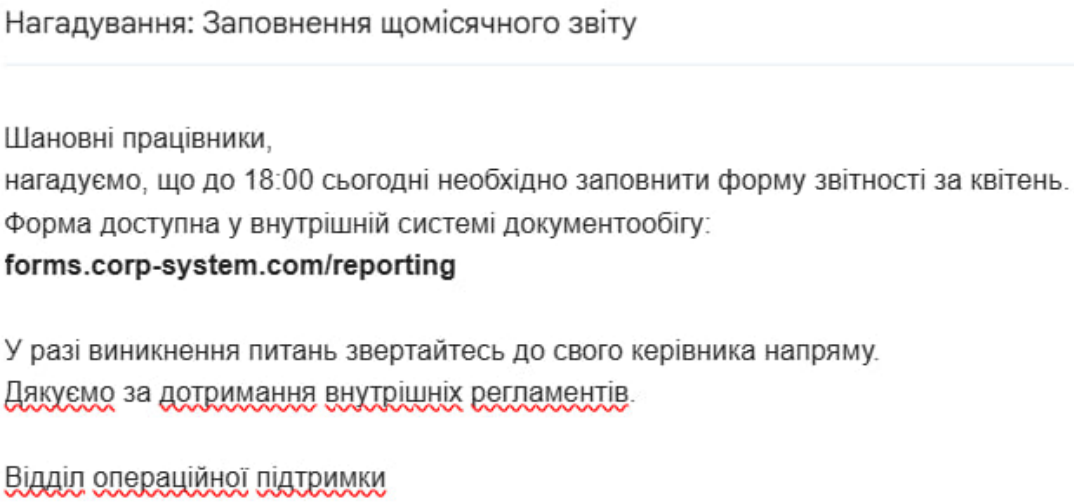

Рис 3.10. Третій сценарій тестування

Результати оцінки за третім сценарієм зведені на рисунку 3.11 (17 вірних відповідей).

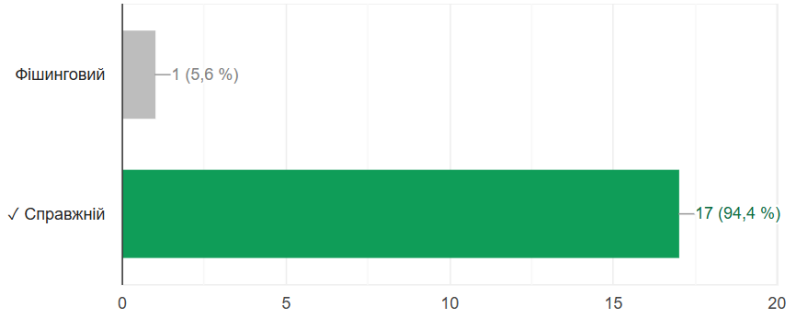

Рис 3.11. Правильних відповідей в межах третього сценарію тестування

Рисунок 3.12 демонструє четвертий сценарій тестування.

Графік чергувань охорони на червень (Оновлено)

Колеги,

Нагадуємо, що з 10 травня діє новий графік змін для об'єктів категорії “А”.

📎 **Оновлений графік у вкладенні: 2024_6_security_shifts.xlsx**

Просимо ознайомитись і підтвердити ознайомлення через внутрішній канал.

З повагою,
Відділ фізичної безпеки

Рис 3.12. Четвертий сценарій тестування

Результати оцінки за четвертим сценарієм зведені на рисунку 3.13 (14 вірних відповідей).

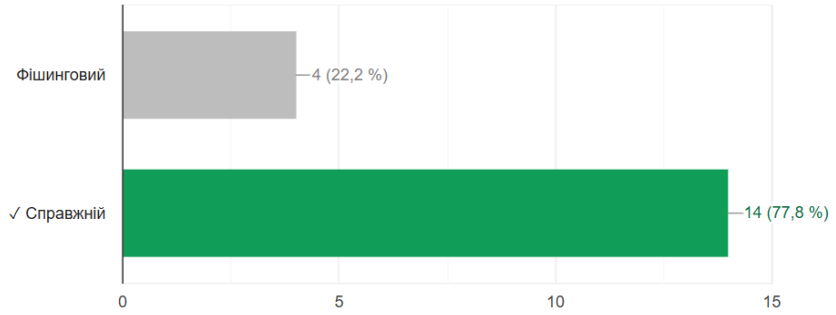

Рис 3.13. Правильних відповідей в межах четвертого сценарію тестування

Рисунок 3.14 демонструє п’ятий сценарій тестування.

Сповіщення про сторонню активність у вашому профілі Teams

Ваш акаунт було використано з незвичної локації:

📍 IP: 31.134.92.218 | Київ, UA
🕒 Час: 06:22, 7 травня

Якщо ви не впізнаєте цю активність, негайно увійдіть і змініть пароль:

🔗 **teams-access.microsoftsec-alerts.com**

— Microsoft Teams Secure Access System

Рис 3.14. П’ятий сценарій тестування

Результати оцінки за п’ятим сценарієм зведені на рисунку 3.15 (18 вірних відповідей).

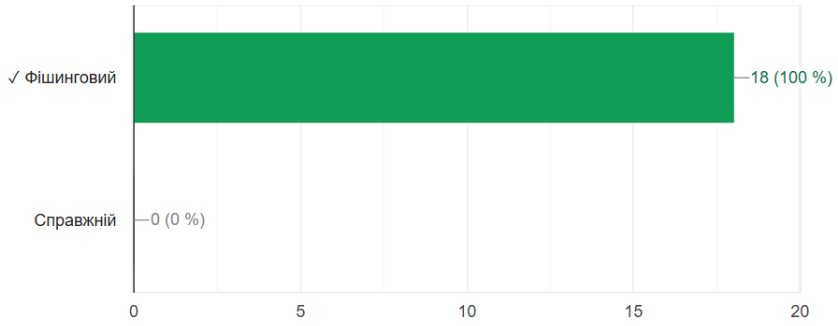

Рис 3.15. Правильних відповідей в межах п’ятого сценарію тестування

Отримані результати демонструють, що в середньому показники зросли на 22% і тепер це дорівнює 88% правильних відповідей. Такий результат може свідчити як про ефективність структури навчальної програми, так і про поступове формування сталих навичок кібергігієни серед персоналу.

Висновки до розділу 3

У розділі здійснено прикладне впровадження розроблених методичних підходів у корпоративному середовищі на прикладі підприємства ТОВ «MegaTech Distribution». Проведено аудит поточного стану інформаційної безпеки, який виявив низький рівень обізнаності персоналу щодо соціоінженерних загроз, відсутність централізованого контролю доступу та фрагментованість підходів до захисту.

На основі аналізу було ідентифіковано критичні вразливості, зокрема: вільний фізичний доступ до чутливих зон, використання незахищених каналів електронного листування та відсутність належної сегментації мережевої інфраструктури. Відповідно до виявлених ризиків сформовано план контрзаходів, спрямований на усунення найуразливіших елементів системи.

Реалізовано комплекс заходів, які включають навчальні ініціативи (проведення семінарів, запуск симуляцій фішингових атак), організаційні зміни

(оновлення нормативних документів, призначення відповідальних осіб), а також технічні вдосконалення (впровадження багатофакторної автентифікації, встановлення електронних замків та систем відеоспостереження).

На основі результатів аналізу здійснено оцінювання ефективності впроваджених заходів. За результатами спостережень зафіксовано зростання рівня обізнаності працівників, зменшення кількості помилок під час ідентифікації соціоінженерних загроз та скорочення часу реагування на інциденти.

Таким чином, третій розділ підтвердив прикладну ефективність запропонованої системи протидії соціоінженерним атакам, демонструючи її здатність істотно підвищити рівень інформаційної безпеки в корпоративному середовищі.

ВИСНОВКИ

З огляду на глобальні тенденції цифрової трансформації, корпоративні інформаційні системи дедалі частіше стають об’єктами соціоінженерних атак, що базуються не стільки на технічних вразливостях, скільки на експлуатації когнітивних та поведінкових особливостей співробітників. Актуальність проблеми обумовлена тим, що традиційні засоби кіберзахисту виявляються недостатніми перед маніпулятивними техніками, спрямованими на обхід людської уваги та довіри.

У межах проведеного дослідження здійснено комплексне вивчення методів протидії соціоінженерним атакам у корпоративному середовищі. Основною метою було визначення ефективних організаційно-технічних рішень для підвищення загального рівня інформаційної безпеки підприємства шляхом зниження вразливості персоналу та інформаційної інфраструктури до соціоінженерних загроз. Проведено аналіз типових сценаріїв атак, оцінено ключові вразливості ІТ-систем та поведінкові ризики, що притаманні співробітникам.

Під час роботи виконано аудит безпеки корпоративної мережі, який включав тестування вразливостей, аналіз політик безпеки, а також проведення контрольованих симуляцій фішингових та інших соціоінженерних впливів. На підставі отриманих результатів розроблено низку рекомендацій щодо удосконалення системи захисту, зокрема щодо впровадження технічних засобів контролю доступу, багатофакторної автентифікації та організаційних заходів, спрямованих на підвищення рівня обізнаності персоналу.

Особливу увагу приділено формуванню навчальних програм з кібергігієни, які поєднують теоретичні знання з практичними тренуваннями у формі рольових симуляцій атак. Проведення навчальних курсів дозволило сформувати у співробітників стійкі навички розпізнавання ознак соціоінженерних маніпуляцій. За результатами повторного тестування

зафіксовано суттєве підвищення рівня розпізнавання фішингових повідомлень, а також зростання кількості випадків повідомлення про інциденти.

Аналіз підтвердив, що людський фактор залишається найуразливішою ланкою у системі кіберзахисту, що потребує безперервної роботи у напрямі підвищення цифрової обізнаності персоналу. Запропоновані підходи, які включають регулярні тренінги, симуляції та оцінювання ефективності, формують стійкий захисний бар’єр проти соціоінженерних впливів.

Таким чином, результати дослідження доводять доцільність впровадження комплексної системи протидії соціоінженерним атакам, що поєднує технічні, організаційні та освітні заходи. Такий підхід дозволяє суттєво підвищити рівень стійкості корпоративної інформаційної системи до загроз соціоінженерного характеру та знизити ризик компрометації критично важливих даних.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Christopher J. Hadnagy. Social Engineering: The Art of Human Hacking. 2010. P. 29. URL: https://kniga.biz.ua/pdf/27094

2. The History of Social Engineering. URL: https://www.mitnicksecurity.com/the-history-of-social-engineering

3. Бурячок В. Л., Корченко О. Г., Бурячок Л. В. Social engineering as a method of information and telecommunication systems intelligence. *Ukrainian Information Security Research Journal.* 2012. Т. 14, № 4 (57). URL: https://doi.org/10.18372/2410-7840.14.3471

4. Гуралюк А.Г. Social engineering and protection against it. *Сучасна парадигма освіти з охорони праці*: матеріали Всеукр. наук.-практ. конф. до Дня охорони праці. 2021. С. 1-4. URL: https://lib.iitta.gov.ua/id/eprint/729293/

5. What Is Social Engineering in Cybersecurity? Real-World Examples and Prevention Methods. *Hideez.* 2024. URL: https://hideez.com/uk-ua/blogs/news/social-engineering

6. Jing Gu. Verizon DBIR 2025: Access is Still the Point of Failure. 2025. URL: https://www.beyondidentity.com/resource/verizon-dbir-2025-access-is-still-the-point-of-failure

7. IBM. What is social engineering? 2022. URL: https://www.ibm.com/think/topics/social-engineering

8. Emily Bonnie. 60+ Social Engineering Statistics. 2025. URL: https://secureframe.com/blog/social-engineering-statistics

9. Understanding the steps in a social engineering attack: from reconnaissance to covering tracks. 2023. URL: https://sendmarc.com/blog/understanding-the-steps-in-a-social-engineering-attack/

10. Простір Психологів. *Когнітивна психологія.* 2023. URL: https://psyhology.space/psypedia-post/kognityvna-psyhologiya/

11. Daniel Kahneman. Thinking, Fast and Slow. 2011 С. 5-10 URL: http://loveread.ec/read_book.php?id=45769&p=5

12. Савчук Т.А. Соціальна інженерія: як шахраї використовують людську психологію в інтернеті. *Радіо Свобода.* 2018. URL: https://www.radiosvoboda.org/a/socialna-inzhenerijashaxrajstvo/29460139.html

13. JC Pass. Social Engineering: Why We Fall for Scams. 2025. URL: https://simplyputpsych.co.uk/global-psych/the-psychology-of-social-engineering-why-we-fall-for-scams

14. Heather Wolters, Kasey Stricklin, Neil Carey, Megan K. McBride. The Psychology of (Dis)information: A Primer on Key Psychological Mechanisms. 2021. С. 8-52 URL: https://www.cna.org/reports/2021/10/psychology-of-disinformation-key-psychological-mechanisms

15. Мінфін. Укрсиббанк попереджає про шахраїв. 2019. URL: https://minfin.com.ua/ua/2019/02/28/36899115/

16. Dan Scherr, Tanya M. Scherr. The Human Factor in Cybersecurity Events: Critical Education Components. 2025. URL: https://domesticpreparedness.com/articles/the-human-factor-in-cybersecurity-events-critical-education-components

17. Юстіменко Ю.В. Як хакери проникають у системи: топ-5 вразливостей українських організацій. *УНН. Ukrainian National News.* 2025. URL: https://unn.ua/en/news/how-hackers-penetrate-systems-top-5-vulnerabilities-of-ukrainian-organizations

18. Karin Kelley.Vulnerability in Security: A Complete Overview. 2025. URL: https://www.simplilearn.com/vulnerability-in-security-article

19. Courtney Goodman. What Is a Vulnerability? Understanding Weak Spots in Your Cybersecurity. 2025. URL: https://www.balbix.com/insights/what-is-a-vulnerability/

20. Найтиповіші помилки підприємств та організацій при кібератаках. *CERT-UA.* 2025. URL: https://cip.gov.ua/ua/news/naitipovishi-pomilki-pidpriyemstv-ta-organizacii-pri-kiberatakakh-rekomendaciyi-cert-ua

21. Прагматизм – що це таке та хто такі прагматики. *Termin.in.ua.* 2019. URL: https://termin.in.ua/prahmatyzm/

22. Скептицизм – що це таке, та хто такі скептики. *Termin.in.ua.* 2019. URL: https://termin.in.ua/skeptytsyzm/

23. Ivan Lee. What is IPS. 2024. URL: https://www.wallarm.com/what/intrusion-prevention-system

24. Securio. Introduction to SIEM: A Tryhackme writeups. 2023. URL: https://securio.hashnode.dev/introduction-to-siem-a-tryhackme-writeups

25. LTS Secure. UEBA Solution for Data Security. 2024. URL: https://ltssecure.com/strengthen-network-security-with-ueba/

26. Єсаф'єв Є.О., Барановський О.М. Виявлення фішингових листів за допомогою машинного навчання та аналізу IOC. *Теоретичні і прикладні проблеми фізики, математики та інформатики*: матеріали XXII Всеукр. наук.-практ. конф. студентів, аспірантів та молодих вчених. Київ. 13-17 травня 2024 р. С. 137-139. URL: https://ela.kpi.ua/items/a80af360-8232-4652-ab8f-769a873cee3e

27. Запорожченко М.М. Моделювання профілю захищеності користувача для визначення його потенційної вразливості до соціоінженерних атак. *Телекомунікаційні та інформаційні технології.* 2024. №4. С. 66–88 URL: https://doi.org/10.31673/2412-4338.2024.049842

28. ISO. What is ISO/IEC 27001? 2022. URL: https://www.iso.org/standard/27001

29. ISACA. Effective IT Governance at Your Fingertips. 2019. URL: https://www.isaca.org/resources/cobit

30. NIST. Cybersecurity Framework. 2025. URL: https://www.nist.gov/cyberframework

31. IBM. Cost of a Data Breach Report. 2024. URL: https://www.ibm.com/reports/data-breach

32. Apu Kapadia. Twentieth Symposium on Usable Privacy and Security. 2024. URL: https://www.usenix.org/conference/soups2024

33. The NIST Cybersecurity Framework (CSF) 2.0. National Institute of Standards and Technology. DOI: https://doi.org/10.6028/NIST.CSWP.29

34. Google. Security Whitepaper. 2021. URL: https://services.google.com/fh/files/misc/google_workspace_security_whitepaper_2021.pdf

35. Gophish. Open-Source Phishing Framework. 2017. URL: https://getgophish.com/

36. Keepnetlabs. Phishing Simulator. 2022. URL: https://keepnetlabs.com/products/phishing-simulator

37. Кладочний А.В. Основи практичного фішингу з Gophish. 2023. URL: https://dou.ua/forums/topic/41619/

38. Контроль доступу на основі ролей. 2025. URL: https://www.solix.com/uk/kb/role-based-access-control/

39. Що таке SIEM? Інформація про безпеку та управління подіями. 2025. URL: https://gridinsoft.ua/siem

40. ESKA. Системи аналізу поведінки користувачів та сутностей. 2023. URL: https://eska.global/solutions/ueba

41. Seeton. Автоматизація реагування на інциденти. 2024. URL: https://www.seeton.pro/cybersecurity/soar/

42. Microsoft. Захист і модернізація роботи організації за допомогою стратегії нульової довіри. 2025. URL: https://www.microsoft.com/uk-ua/security/business/zero-trust

43. Carlos Rivera. The Forrester Wave: Zero Trust Platform Providers. 2023. URL: https://reprint.forrester.com/reports/the-forrester-wave-tm-zero-trust-platform-providers-q3-2023-d8bc9ffa/index.html?culture=uk-ua&country=ua

44. Richard Addiscott. 3 ways to assess the effectiveness of security awareness training. 2021. URL: https://www.cybersecuritydive.com/news/gartner-security-awareness-training

45. ISO/IEC 27004: 2016. С. 29–34. URL: https://www.amnafzar.net/files/1/ISO%2027000/ISO%20IEC%2027004-2016.pdf

46. Куценко О.С. Фішинг. 2025. URL: https://docs.google.com/forms/d/e/1FAIpQLSfxBOjeP_QaTzMSVLfJm4ISnL8eCOLZnIr1aJpW_bNixlZVzA/viewform

47. Куценко О.С., Редькіна А.В. Оцінювання динаміки змін рівня обізнаності співробітників. 2025. URL: https://docs.google.com/forms/d/e/1FAIpQLScgTLSUHfkBQg_oJIhk8GFUBsZyrBAt0Pt2-Sv450i-8zKoqg/viewform

48. Max Edwards. ISO 27001:2022 Annex A 7.1 – Physical Security Perimeters. 2025. URL: https://www.isms.online/iso-27001/annex-a/7-1-physical-security-perimeters-2022/

49. NIST. Security and Privacy Controls for Information Systems and Organizations. 2020. С. 179-193 URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

50. Арвіднг Занг. Інциденти інформаційної безпеки: Співробітники як фактор успіху. 2022. URL: https://www.dqsglobal.com/uk-ua/navchajtesya/blog/incidenti-informacijnoyi-bezpeki-spivrobitniki-yak-faktor-uspihu

51. Універсальний мініатюрний зчитувач. 2023. URL: https://u-prox.systems/uproduct/u-prox-sl-mini-2/

52. CCTV Cameras Explained. URL: https://www.techcube.co.uk/blog/cctv-cameras-explained/

53. IT specialist. Побудова та аутсорсинг Оперативного Центру Кібербезпеки. 2020. URL: https://my-itspecialist.com/cybersecurity-solutions/security-operation-center

54. Shanika Wickramasinghe. SOC Metrics: Security Metrics & KPIs for Measuring SOC Success. 2023. URL: https://www.splunk.com/en_us/blog/learn/security-operations-metrics.html

55. MTTD Defined and Explained. 2023. URL: https://www.plutora.com/blog/mttd-mean-time-to-detect-defined-explained

56. Alex Circei. MTTR: A Comprehensive Overview of this important DORA Metric. 2023. URL: https://waydev.co/mean-time-to-recovery/

57. Легомінова С.В., Стежко М.В. Проблематика захищеності користувачів інформаційних систем від соціоінженерних атак. *Стратегії кіберстійкості: управління ризиками та безперервність бізнесу*: матеріали III Всеукраїн. наук.-практ. конф., м. Київ, 23 лютого 2023 р. С. 122-123.