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 ЗАГРОЗАМ В ОРГАНІЗАЦІЇ”

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

_____ Нікіта ГОРБАЧ
(підпис) *Ім’я, ПРІЗВИЩЕ здобувача*

Виконав: здобувач вищої освіти гр. УБД-41

Нікіта ГОРБАЧ
Ім’я, ПРІЗВИЩЕ

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

Рецензент: _____
_____ Ім’я, ПРІЗВИЩЕ

Київ 2026

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
“____”_____2026 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Горбачу Нікіті Олександровичу
(прізвище, ім’я, по батькові здобувача)

1. Тема кваліфікаційної роботи “Методи протидії соціоінженерним загрозам в організіції ”, керівник кваліфікаційної роботи ЗАПОРОЖЧЕНКО Михайло, доктор філософії з кібербезпеки
(ПРІЗВИЩЕ, Ім’я, науковий ступінь, вчене звання)

затверджені наказом Державного університету інформаційно-комунікаційних технологій від “20“ лютого 2026 року. №51.

2. Строк подання кваліфікаційної роботи “12” травня 2026 року.

3. Вихідні дані до кваліфікаційної роботи: *інформаційна безпека підприємства, методи та засоби управління персоналом з інформаційної безпеки, міжнародні стандарти, наукова та технічна література.*

4. Перелік питань, які мають бути розроблені:
4.1. Визначити сутність соціальної інженерії, класифікувати основні види технік та чинників, що впливають на сприйнятливість працівників.
4.2. Проаналізувати сучасні підходи до організації системи протидії соціоінженерним загрозам в організації.
4.3. Дослідити методи ідентифікації та оцінювання соціоінженерних ризиків, а також підходи до формування стратегії підвищення рівня обізнаності персоналу.
4.4. Провести аналіз стану захищеності організації від соціоінженерних атак, розробити рекомендації щодо вдосконалення системи протидії соціоінженерним загрозам та оцінити ефективність запропонованих заходів.

5. Перелік ілюстративного матеріалу: *презентація PowerPoint*

6. Дата видачі завдання “5“ березня 2026 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Етапи кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1.	Визначення об’єкту, предмету, мети та завдань дослідження.	18.03.2026	
2.	Збір та аналіз літератури.	30.03.2026	
3.	Аналіз теоретичних основ протидії соціоінженерним загрозам у сфері інформаційної безпеки.	08.04.2026	
4.	Дослідження методичних підходів до організації системи захисту від соціоінженерних загроз.	15.04.2026	
5.	Аналіз стану захищеності організації, розробка рекомендацій щодо протидії соціоінженерним загрозам та оцінювання їх ефективності.	22.04.2026	
6.	Формулювання висновків за результатами проведеногодослідження.	29.04.2026	
7.	Оформлення роботи.	06.05.2026	
8.	Оформлення презентації.	11.05.2026	
9.	Отримання рецензії на роботу.	10.06.2026	
10.	Захист в ЕК.	__.06.2026	

Здобувач вищої освіти _____ Нікіта ГОРБАЧ
(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 Горбач Н.О. 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 загрозам в організіції”

Кваліфікаційна робота і рецензія додаються.

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

Висновок керівника кваліфікаційної роботи

Здобувач ГОРБАЧ Нікіта у кваліфікаційній роботі дослідив методи протидії соціоінженерним загрозам в організації, проаналізував основні види атак соціальної інженерії та механізми їх впливу на персонал. У роботі розглянуто сучасні підходи до підвищення рівня інформаційної безпеки, а також розроблено рекомендації щодо впровадження організаційних і навчальних заходів для зменшення ризиків. У практичній частині запропоновано комплекс заходів із протидії соціоінженерним загрозам та проведено оцінку їх ефективності в умовах організації.

Робота демонструє високий рівень теоретичної підготовки та практичних навичок здобувача. ГОРБАЧ Нікіта проявила самостійність, відповідальність та вміння застосовувати здобуті знання. Результати дослідження апробовані на конференції.

Все це дозволяє оцінити кваліфікаційну роботу здобувача ГОРБАЧА Нікіти на оцінку “_____” та присвоїти йому кваліфікацію бакалавра з кібербезпеки за освітньою програмою Управління інформаційною та кібернетичною безпекою.

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

“____“_____2026 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач Горбач Н.О. 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 ГОРБАЧА Нікіти
на тему “ Методи протидії соціоінженерним загрозам в організіції ”

Актуальність. В умовах стрімкого розвитку інформаційно-комунікаційних технологій та розширення цифрового середовища соціоінженерні атаки залишаються однією з найсерйозніших загроз інформаційній безпеці організацій. Особливість таких атак полягає у використанні людського фактора як найбільш вразливої складової системи захисту, що дозволяє зловмисникам обходити навіть сучасні технічні засоби безпеки. Зростання кількості фішингових кампаній, випадків компрометації облікових даних та інших форм соціальної інженерії обумовлює необхідність удосконалення методів протидії таким загрозам.

У зв’язку з цим особливої актуальності набувають дослідження, спрямовані на аналіз механізмів реалізації соціоінженерних атак, оцінювання рівня вразливості організацій та розроблення комплексних організаційних і технічних заходів захисту. Отримані результати мають практичне значення для підвищення рівня інформаційної безпеки та стійкості організацій до сучасних кіберзагроз.

Позитивні сторони.

1. У роботі проведено ґрунтовний аналіз соціоінженерних загроз, їх класифікації, механізмів реалізації та психологічних чинників, що впливають на успішність атак.
2. Здійснено дослідження сучасних підходів до побудови системи протидії соціоінженерним загрозам, включаючи методи оцінювання ризиків, підвищення рівня обізнаності персоналу та впровадження організаційних і технічних заходів захисту.
3. У практичній частині виконано аналіз поточного стану захищеності організації від соціоінженерних атак, розроблено рекомендації щодо вдосконалення системи захисту та проведено оцінювання ефективності запропонованих заходів.

Недоліки.

Доцільним було б розширити практичну частину роботи шляхом проведення порівняльного аналізу сучасних програмних рішень для захисту від соціоінженерних атак, зокрема платформ симуляції фішингових кампаній, систем моніторингу поведінки користувачів та засобів підвищення обізнаності персоналу.

Зазначене зауваження має рекомендаційний характер і не впливає на загальну позитивну оцінку кваліфікаційної роботи.

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

Рецензент: _____ _____
підпис Ім’я, ПРІЗВИЩЕ
_____

РЕФЕРАТ

Кваліфікаційна робота присвячена дослідженню методів протидії соціоінженерним загрозам в організації. Робота складається зі вступу, трьох розділів, містить 6 рисунків, 25 таблиць, висновки та список використаних джерел із 87 найменувань. Загальний обсяг роботи становить 81 сторінка.

Метою роботи є дослідження соціоінженерних загроз та розроблення рекомендацій щодо вдосконалення системи протидії соціальній інженерії в організації.

Об'єктом дослідження є процес забезпечення інформаційної безпеки організації в умовах впливу соціоінженерних загроз.

Предметом дослідження є методи, механізми та підходи до протидії соціоінженерним атакам в організації.

Методи дослідження. Для досягнення поставленої мети в роботі використано методи аналізу та синтезу, узагальнення, систематизації, порівняння, структурного аналізу, моделювання та оцінювання ризиків. Для дослідження практичних аспектів забезпечення інформаційної безпеки застосовано методи аналізу організаційних процесів, оцінювання вразливостей та порівняльного аналізу ефективності заходів захисту.

Галузь застосування. Результати дослідження можуть бути використані для вдосконалення системи інформаційної безпеки державних установ, комерційних підприємств та інших організацій, діяльність яких пов'язана з використанням інформаційно-комунікаційних технологій. Запропоновані рекомендації спрямовані на підвищення рівня захищеності персоналу від соціоінженерних атак, удосконалення організаційних процедур безпеки та мінімізацію ризиків, пов'язаних із людським фактором.

Ключові слова: СОЦІАЛЬНА ІНЖЕНЕРІЯ, СОЦІОІНЖЕНЕРНІ АТАКИ, ІНФОРМАЦІЙНА БЕЗПЕКА, КІБЕРБЕЗПЕКА, ЛЮДСЬКИЙ ФАКТОР, ФІШИНГ, УПРАВЛІННЯ РИЗИКАМИ, ЗАХИСТ ІНФОРМАЦІЇ, ПРОТИДІЯ СОЦІОІНЖЕНЕРНИМ ЗАГРОЗАМ.

ABSTRACT

The qualification thesis is devoted to the study of methods for counteracting social engineering threats in organizations. The thesis consists of an introduction, three chapters, 6 figures, 25 tables, conclusions, and a list of 87 references. The total volume of the thesis is 81 pages.

The purpose of the thesis is to investigate social engineering threats and develop recommendations for improving the system of protection against social engineering attacks within an organization.

The object of the research is the process of ensuring information security of an organization under the influence of social engineering threats.

The subject of the research is methods, mechanisms, and approaches to counteracting social engineering attacks in organizations.

Research methods. To achieve the stated objective, the thesis employs methods of analysis and synthesis, generalization, systematization, comparison, structural analysis, modeling, and risk assessment. To investigate practical aspects of information security, methods of organizational process analysis, vulnerability assessment, and comparative analysis of the effectiveness of security measures were applied.

Field of application. The research results can be used to improve information security systems in government institutions, commercial enterprises, and other organizations whose activities involve the use of information and communication technologies. The proposed recommendations are aimed at increasing personnel resilience to social engineering attacks, improving organizational security procedures, and minimizing risks associated with the human factor.

Keywords: SOCIAL ENGINEERING, SOCIAL ENGINEERING ATTACKS, INFORMATION SECURITY, CYBERSECURITY, HUMAN FACTOR, PHISHING, RISK MANAGEMENT, INFORMATION PROTECTION, COUNTERMEASURES AGAINST SOCIAL ENGINEERING THREATS.

ЗМІСТ

ВСТУП

Актуальність теми. У сучасних умовах стрімкого розвитку інформаційно-комунікаційних технологій та глобальної цифровізації суспільства питання забезпечення інформаційної безпеки набуває особливої актуальності. Практично всі сфери діяльності сучасних організацій — управлінська, фінансова, наукова, освітня, виробнича та комунікаційна — безпосередньо залежать від використання цифрових ресурсів, електронного документообігу, мережевих сервісів і систем обробки інформації. Водночас розвиток інформаційного середовища супроводжується не лише розширенням можливостей для ефективної діяльності, але й появою нових загроз, здатних негативно впливати на стабільність функціонування організацій та безпеку їх інформаційних ресурсів.

Однією з найбільш небезпечних і водночас складних загроз сучасної інформаційної безпеки є соціальна інженерія. На відміну від традиційних кіберзагроз, орієнтованих переважно на технічні вразливості інформаційних систем, соціоінженерні атаки спрямовані на використання людського фактору як найбільш уразливого елементу будь-якої організації. Основним об’єктом впливу в такому випадку виступає людина, а головним інструментом реалізації атаки — психологічна маніпуляція, що дозволяє зловмиснику отримувати конфіденційну інформацію, несанкціонований доступ до систем або спонукати працівників до виконання дій, які порушують встановлені правила безпеки.

Актуальність дослідження обумовлена постійним зростанням кількості соціоінженерних атак та ускладненням механізмів їх реалізації. Сучасні зловмисники активно використовують електронну пошту, соціальні мережі, телефонний зв’язок, вебресурси та інші канали комунікації для здійснення психологічного впливу на користувачів. Особливу небезпеку становить те, що такі атаки часто мають високий рівень персоналізації, адаптуються до специфіки діяльності організації та маскуються під звичайні робочі процеси. У результаті навіть сучасні технічні засоби захисту можуть виявитися

недостатньо ефективними, якщо працівник самостійно передає конфіденційні дані або виконує небезпечні дії під впливом маніпуляцій.

Додаткової актуальності темі надає зростання ролі дистанційної роботи, використання хмарних сервісів, цифрових платформ і електронної взаємодії між організаціями. Розширення інформаційного середовища збільшує кількість потенційних точок впливу на персонал та ускладнює процес контролю інформаційних потоків. У таких умовах людський фактор перетворюється на ключовий елемент ризику, а проблема формування ефективної системи протидії соціоінженерним загрозам набуває стратегічного значення для забезпечення інформаційної безпеки.

Наукові дослідження у сфері соціальної інженерії свідчать про те, що ефективність соціоінженерних атак значною мірою визначається не технічними можливостями зловмисника, а рівнем обізнаності персоналу, особливостями організаційної культури, недосконалістю внутрішніх процедур безпеки та психологічними характеристиками працівників. Саме тому сучасний підхід до забезпечення інформаційної безпеки потребує комплексного поєднання технічних, організаційних та поведінкових заходів захисту.

Теоретичні та практичні аспекти протидії соціоінженерним загрозам досліджувалися у працях вітчизняних і зарубіжних науковців у галузях інформаційної безпеки, психології, менеджменту та кібербезпеки. Значний внесок у розвиток концепцій соціальної інженерії зробили дослідники, які вивчали механізми психологічного впливу, поведінкові аспекти інформаційної безпеки, управління ризиками та методи організації систем захисту. Проте динамічний розвиток цифрового середовища та постійна еволюція соціоінженерних методів зумовлюють необхідність подальшого вдосконалення підходів до забезпечення стійкості організацій до таких загроз.

Мета роботи – дослідження соціоінженерних загроз та розроблення рекомендацій щодо вдосконалення системи протидії соціальній інженерії в організації.

Об'єкт дослідження – процес забезпечення інформаційної безпеки організації в умовах впливу соціоінженерних загроз.

Предмет дослідження – методи , механізми та підходи до протидії соціоінженерним атакам в організації.

Для досягнення поставленої мети у роботі визначено такі **завдання**:

– визначити сутність соціальної інженерії, класифікувати основні види технік та чинників, що впливають на сприйнятливість працівників;

– проаналізувати сучасні підходи до організації системи протидії соціоінженерним загрозам в організації;

– дослідити методи ідентифікації та оцінювання соціоінженерних ризиків, а також підходи до формування стратегії підвищення рівня обізнаності персоналу;

– провести аналіз стану захищеності організації від соціоінженерних атак, розробити рекомендації щодо вдосконалення системи протидії соціоінженерним загрозам та оцінити ефективність запропонованих заходів.

Методи дослідження. У процесі дослідження було використано комплекс загальнонаукових і спеціальних методів, зокрема методи аналізу та синтезу, узагальнення, систематизації, порівняння, структурного аналізу, моделювання та оцінювання ризиків. Для дослідження практичних аспектів забезпечення інформаційної безпеки застосовано методи аналізу організаційних процесів, оцінювання вразливостей та порівняльного аналізу ефективності заходів захисту.

Практичне значення отриманих результатів полягає у можливості використання розроблених рекомендацій для вдосконалення системи інформаційної безпеки організацій, діяльність яких пов'язана з використанням інформаційно-комунікаційних технологій та електронних комунікацій. Запропоновані підходи можуть бути використані для підвищення рівня обізнаності персоналу, удосконалення організаційних процедур та мінімізації ризиків, пов'язаних із соціоінженерними атаками.

Практична частина дослідження виконана на базі Інституту

інформаційних технологій та систем НАН України, діяльність якого пов’язана з використанням сучасних цифрових технологій, інформаційних систем та електронної взаємодії. Це дозволило здійснити аналіз поточного стану захищеності установи від соціоінженерних загроз та сформувати практично орієнтовані рекомендації щодо вдосконалення системи протидії таким атакам.

Структура роботи обумовлена поставленою метою та завданнями дослідження. Робота складається зі вступу, трьох розділів, висновків, списку використаних джерел і додатків.

Апробація результатів кваліфікаційної роботи відбулася на Всеукраїнській науково-практичній конференції “Стратегії кіберстійкості: управління ризиками та безперервність бізнесу” 25 лютого 2026 року.

РОЗДІЛ 1 АНАЛІЗ СОЦІОІНЖЕНЕРНИХ ЗАГРОЗ ТА МЕХАНІЗМІВ ЇХ РЕАЛІЗАЦІЇ

1.1. Визначення ролі соціальної інженерії як чинника дестабілізації корпоративної інформаційної безпеки

У сучасних умовах цифровізації діяльності організацій питання забезпечення інформаційної безпеки набуває особливої актуальності. Активне впровадження інформаційно-комунікаційних технологій, розвиток віддалених форматів роботи, використання хмарних сервісів і корпоративних мереж призводять до значного розширення поверхні атак. У таких умовах навіть незначні порушення політик безпеки можуть мати критичні наслідки для функціонування організації.

Незважаючи на постійне вдосконалення технічних засобів захисту, таких як системи виявлення вторгнень, багатофакторна автентифікація, криптографічні механізми та антивірусне програмне забезпечення, людський фактор залишається найбільш уразливою складовою системи безпеки, що пояснюється тим, що поведінка людини є менш передбачуваною та не піддається повному формалізованому контролю [4, с. 75].

Саме цю вразливість активно експлуатують соціоінженерні атаки, які спрямовані не на технічні компоненти системи, а на користувачів як носіїв доступу до інформаційних ресурсів. Практика свідчить, що значна частина інцидентів інформаційної безпеки виникає саме через помилки або необачні дії персоналу.

Соціальна інженерія являє собою сукупність методів психологічного впливу на людину з метою отримання конфіденційної інформації або здійснення дій, що порушують безпеку інформаційної системи. На відміну від технічних атак, соціальна інженерія не потребує складних програмних інструментів, оскільки її основним об’єктом є людина, а ключовим

інструментом — маніпуляція її поведінкою.

Важливо підкреслити, що ефективність соціальної інженерії обумовлена не лише недоліками технічного захисту, а передусім особливостями людського мислення, такими як довіра, схильність до автоматичних рішень, вплив авторитету та емоційні реакції. Це робить соціоінженерні атаки універсальним інструментом, який може бути застосований незалежно від рівня технічного оснащення організації.

З наукової точки зору, соціальна інженерія розглядається як складне міждисциплінарне явище, яке формується на перетині кількох галузей знань і практики. Її природа не може бути повноцінно пояснена виключно в межах технічного підходу до інформаційної безпеки, оскільки в основі соціоінженерного впливу лежить не стільки експлуатація програмних чи апаратних вразливостей, скільки використання особливостей людської поведінки, соціальної взаємодії та організаційного середовища. Саме тому науковий аналіз соціальної інженерії потребує комплексного розгляду її психологічних, соціологічних, безпекових і управлінських аспектів [34, с.95].

Передусім соціальна інженерія тісно пов’язана з психологією, оскільки її основним інструментом виступає цілеспрямований вплив на свідомість, емоції та поведінкові реакції людини. У межах психологічного підходу соціоінженерні атаки розглядаються як форма маніпулятивної комунікації, за якої зловмисник прагне змінити поведінку жертви у вигідному для себе напрямі. Такий вплив може реалізовуватися через переконання, навіювання, створення ілюзії терміновості, формування відчуття небезпеки або, навпаки, псевдобезпеки. Наприклад, працівник може отримати повідомлення, оформлене як офіційний запит від адміністратора системи, і під впливом авторитету без додаткової перевірки надати облікові дані чи виконати дію, що порушує правила безпеки.

Особливе значення у цьому контексті мають когнітивні упередження, тобто типові помилки мислення, притаманні людині в процесі прийняття рішень. Соціальні інженери активно використовують схильність людей

довіряти авторитетам, реагувати на термінові повідомлення без належного аналізу, уникати конфліктів, діяти за звичними шаблонами та орієнтуватися на поведінку більшості. Наприклад, якщо працівникові повідомляють, що «всі співробітники вже підтвердили свої дані в новій системі», це може активізувати механізм соціального наслідування. Якщо ж лист містить вимогу негайно змінити пароль у зв'язку з нібито виявленою загрозою, то спрацьовує фактор страху та терміновості, що знижує рівень критичного мислення. Отже, психологічний компонент соціальної інженерії полягає в експлуатації природних емоційних і когнітивних реакцій людини [34, с.85].

Не менш важливим є соціологічний вимір соціальної інженерії. Людина функціонує не ізольовано, а в межах певного соціального середовища, де її поведінка значною мірою визначається ролями, нормами, очікуваннями та міжособистісними зв'язками. Соціальна інженерія використовує саме цю соціальну природу комунікації. У межах організації працівники постійно взаємодіють один з одним, підпорядковуються формальній ієрархії, довіряють колегам, керівникам, представникам технічної підтримки, партнерам чи клієнтам. Зловмисник, який здатен переконливо відтворити одну з таких соціальних ролей, отримує суттєві переваги для реалізації атаки.

Соціологічний аспект також проявляється у феномені інституційної довіри. У багатьох організаціях працівники звикають сприймати внутрішні комунікації як апріорі достовірні, особливо якщо вони мають формальні ознаки офіційності: корпоративний стиль листа, посилання на внутрішні регламенти, згадку імен керівництва або назви структурного підрозділу. Така довіра є необхідною умовою ефективної роботи організації, однак водночас вона створює сприятливе середовище для маніпуляцій. Окрім цього, важливу роль відіграє групова поведінка: працівник часто орієнтується не лише на власну оцінку ситуації, а й на уявлення про те, як у подібній ситуації діють інші. Саме тому посилання на колектив, корпоративні норми чи загальноприйняту практику є дієвими елементами соціоінженерного сценарію [14, с. 84].

З позицій інформаційної безпеки соціальна інженерія виступає як специфічний механізм несанкціонованого доступу до інформаційних ресурсів, який реалізується шляхом обходу технічних засобів захисту через вплив на легітимного користувача. На відміну від класичних кіберзагроз, де основна увага зосереджена на пошуку технічних вразливостей у програмному забезпеченні, мережевій інфраструктурі або конфігурації систем, соціоінженерна атака орієнтується на експлуатацію «людської вразливості». Це означає, що об’єктом компрометації стає не система як така, а користувач, який має законні права доступу до неї [20, с. 75].

У цьому контексті соціальна інженерія прямо пов’язана з такими явищами, як компрометація облікових даних, розкриття конфіденційної інформації, несанкціоноване виконання дій у системі, встановлення шкідливого програмного забезпечення, порушення режиму доступу до приміщень або ресурсів. При цьому навіть добре захищена інфраструктура може виявитися вразливою, якщо працівник самостійно передає логін і пароль, відкриває шкідливе вкладення, переходить за фішинговим посиланням або дозволяє сторонній особі доступ до внутрішнього середовища організації. Таким чином, у сфері інформаційної безпеки соціальна інженерія розглядається як одна з найскладніших загроз саме через те, що вона руйнує традиційну логіку периметрового захисту: проникнення відбувається не шляхом злому, а через спонукання працівника до помилкових або небезпечних дій.

Окремого значення набуває управлінський аспект соціальної інженерії. Ефективність або, навпаки, вразливість організації до таких атак значною мірою визначається не лише індивідуальними якостями працівників, а й тим, як саме побудована система управління інформаційною безпекою. Менеджмент у цьому контексті охоплює організаційну культуру, політики безпеки, процедури реагування на інциденти, систему навчання персоналу та механізми контролю за дотриманням встановлених правил. Якщо в організації відсутні чіткі регламенти перевірки запитів, не проводиться навчання з розпізнавання шахрайських сценаріїв, а працівники не розуміють власної ролі

у забезпеченні безпеки, ризик успішної соціоінженерної атаки суттєво зростає [34, с. 8].

Організаційна культура має тут фундаментальне значення. У середовищі, де безпека сприймається як другорядне завдання, а пріоритет надається лише швидкості виконання операцій, працівники частіше ігнорують перевірку підозрілих повідомлень і діють автоматично. Натомість у тих організаціях, де сформовано культуру відповідального ставлення до інформації, працівник розглядається не як пасивний виконавець, а як активний елемент системи захисту. У такому випадку політики безпеки стають не формальним набором документів, а практичним інструментом, який регулює повсякденну діяльність персоналу [16, с. 74].

Управління ризиками також є невід'ємною складовою аналізу соціальної інженерії. Будь-яка організація повинна оцінювати не лише технічні ризики, а й ризики, пов'язані з поведінкою персоналу, рівнем обізнаності працівників, характером внутрішніх комунікацій, наявністю критичних посад, співробітники яких мають доступ до особливо цінних ресурсів. З позиції менеджменту соціальна інженерія є не просто видом шахрайства, а системною загрозою, яка потребує комплексного управлінського реагування: від розроблення нормативних документів і навчальних програм до проведення тестувань, аудиту поведінкових ризиків і впровадження механізмів багаторівневої перевірки критичних дій (табл. 1.1).

Таблиця 1.1

Міждисциплінарна природа соціальної інженерії

Галузь знань	**Основні аспекти застосування**	**Роль у соціальній інженерії**
Психологія	Маніпуляції, когнітивні викривлення	Формування поведінки жертви
Соціологія	Соціальні взаємодії, довіра	Використання соціальних ролей
Інформаційна безпека	Контроль доступу, захист даних	Обхід систем захисту
Менеджмент	Політики, процедури, культура безпеки	Створення або усунення вразливостей

Отже, міждисциплінарний характер соціальної інженерії пояснюється

тим, що вона функціонує одночасно у кількох площинах. Психологія дає змогу зрозуміти, яким чином здійснюється маніпулятивний вплив на окрему людину; соціологія пояснює роль довіри, соціальних норм і рольових моделей у процесі взаємодії; інформаційна безпека визначає наслідки такого впливу для конфіденційності, цілісності та доступності інформації; менеджмент формує організаційні умови, які або знижують, або підсилюють вразливість до соціоінженерних загроз. Саме тому дослідження соціальної інженерії в межах корпоративної інформаційної безпеки має здійснюватися комплексно, з урахуванням не лише технічних, а й поведінкових та управлінських чинників.

Соціальна інженерія відіграє дестабілізуючу роль у корпоративній інформаційній безпеці, оскільки дозволяє обходити формалізовані механізми контролю. Якщо технічні засоби орієнтовані на запобігання несанкціонованому доступу через системні вразливості, то соціоінженерні атаки спрямовані на легітимних користувачів, які самі надають доступ зловмиснику [35, с. 93].

З огляду на зазначені особливості соціоінженерного впливу доцільно узагальнити механізм реалізації таких атак у контексті дестабілізації корпоративної інформаційної безпеки. Важливим є розуміння того, що соціальна інженерія функціонує як поетапний процес, у якому ключову роль відіграє трансформація поведінки працівника під впливом зовнішніх маніпуляцій. Узагальнену логіку такого процесу представлено на рисунку 1.1.

Показаний механізм демонструє, що первинною точкою впливу є не інформаційна система, а людина як носій доступу до неї. Саме через зміну поведінки працівника відбувається порушення встановлених політик безпеки, що, у свою чергу, призводить до несанкціонованого доступу та виникнення інцидентів. Таким чином, людський фактор виступає ключовою ланкою, через яку реалізується більшість соціоінженерних загроз.

Рис. 1.1. Механізм дестабілізації через соціальну інженерію

Додатково слід зазначити, що рівень небезпеки соціальної інженерії значною мірою зумовлюється сукупністю її характерних властивостей, які відрізняють її від інших типів загроз інформаційній безпеці. Зокрема, соціоінженерні атаки характеризуються високим рівнем масштабованості, що проявляється у можливості одночасного впливу на значну кількість користувачів без істотного збільшення витрат ресурсів з боку зловмисника. Це дозволяє реалізовувати масові фішингові кампанії, спрямовані на широке коло працівників організації [22, с. 75].

Важливою особливістю є також скритність таких атак. Оскільки вони не супроводжуються явними технічними аномаліями в роботі систем, традиційні засоби моніторингу інформаційної безпеки часто не здатні своєчасно їх виявити. У більшості випадків дії працівника виглядають як легітимні, що значно ускладнює процес ідентифікації інциденту та його подальшого розслідування.

Не менш суттєвою характеристикою є адаптивність соціальної інженерії, яка полягає у здатності зловмисників швидко змінювати сценарії атак залежно від контексту, типу організації, специфіки діяльності та навіть індивідуальних

особливостей конкретних працівників. Це означає, що універсальних шаблонів протидії таким загрозам не існує, а ефективний захист потребує постійного оновлення знань та методів реагування.

Крім того, соціоінженерні атаки відзначаються відносно низькою вартістю реалізації, оскільки не потребують складної технічної інфраструктури або значних фінансових витрат. У багатьох випадках достатньо базових знань у сфері психології та доступу до відкритих джерел інформації для підготовки ефективної атаки, що робить соціальну інженерію доступним інструментом як для професійних кіберзлочинців, так і для менш підготовлених осіб [44, с. 94].

У сукупності зазначені характеристики формують високий рівень загрози для корпоративної інформаційної безпеки, оскільки поєднують ефективність впливу з низькою вартістю реалізації та складністю виявлення. Саме тому соціальна інженерія потребує особливої уваги з боку організацій у контексті побудови комплексної системи захисту інформації.

Таблиця 1.2

Ключові характеристики соціоінженерних атак

Характеристика	**Опис**	**Наслідки для організації**
Скритність	Відсутність технічних аномалій	Ускладнення виявлення
Адаптивність	Підлаштування під конкретну ситуацію	Зростання ефективності атак
Орієнтація на людину	Використання довіри та психології	Обхід систем захисту
Масовість	Можливість масштабування атак	Масові інциденти

Таким чином, соціальна інженерія є одним із ключових чинників дестабілізації корпоративної інформаційної безпеки, оскільки вона спрямована на експлуатацію людського фактору як найбільш вразливої складової будь-якої організаційної системи. На відміну від технічних загроз, які можуть бути виявлені, локалізовані та нейтралізовані за допомогою спеціалізованих засобів захисту, соціоінженерні атаки базуються на зміні поведінки користувача, що значно ускладнює їх своєчасне розпізнавання та запобігання.

Її небезпека полягає у здатності впливати на найбільш слабку ланку –

людину, яка, володіючи легітимними правами доступу до інформаційних ресурсів, може несвідомо стати інструментом порушення безпеки. У таких умовах навіть найсучасніші технічні засоби захисту, включаючи системи контролю доступу, шифрування та мережеві екрани, втрачають свою ефективність, якщо користувач добровільно передає конфіденційні дані або виконує дії, що суперечать встановленим політикам безпеки [3, с. 54].

Додаткову складність становить той факт, що соціальна інженерія часто маскується під звичайні робочі процеси, використовуючи елементи корпоративної комунікації, службової ієрархії та довірчих відносин між працівниками. Це створює ілюзію легітимності дій зловмисника та знижує рівень критичного сприйняття інформації з боку персоналу. У результаті працівники можуть не лише не розпізнати загрозу, але й активно сприяти її реалізації.

У цьому контексті стає очевидним, що забезпечення інформаційної безпеки не може обмежуватися виключно впровадженням технічних рішень. Необхідною умовою ефективного захисту є формування комплексного підходу, який передбачає підвищення рівня обізнаності персоналу, розвиток навичок критичного мислення, регулярне навчання та моделювання соціоінженерних атак з метою перевірки готовності працівників до їх розпізнавання [34, с.88].

Важливу роль відіграє також формування культури інформаційної безпеки в організації, яка передбачає усвідомлення кожним працівником своєї відповідальності за збереження інформаційних ресурсів. Така культура базується на чітко визначених правилах поведінки, підтримці з боку керівництва, відкритій комунікації щодо загроз та інцидентів, а також стимулюванні безпечної поведінки. Лише за умови поєднання технічних, організаційних і поведінкових заходів можливо забезпечити належний рівень стійкості організації до соціоінженерних загроз.

Соціальна інженерія виступає системною проблемою сучасної інформаційної безпеки, яка потребує не лише технологічного, але й глибокого поведінкового та управлінського підходу до її вирішення.

1.2. Класифікація соціоінженерних атак за векторами та каналами реалізації

Соціоінженерні атаки характеризуються значною різноманітністю форм і способів реалізації, що зумовлює необхідність їх систематизації. Класифікація таких атак дозволяє більш глибоко зрозуміти механізми їх здійснення, виявити типові сценарії впливу на персонал та сформувати ефективні підходи до протидії. Найбільш доцільним є розгляд соціоінженерних атак за двома ключовими ознаками: векторами впливу та каналами реалізації.

Під вектором атаки слід розуміти спосіб взаємодії зловмисника з потенційною жертвою, тобто напрямок і характер впливу, який визначає логіку побудови атаки. У свою чергу, канал реалізації відображає середовище або технічний засіб, через який здійснюється цей вплив [39, с. 94].

Класифікація за векторами впливу дозволяє визначити рівень цілеспрямованості атаки та ступінь її персоналізації. Зокрема, соціоінженерні атаки можуть мати масовий характер, коли однакові повідомлення або сценарії розсилаються великій кількості користувачів без урахування їх індивідуальних особливостей. Такий підхід часто використовується у фішингових кампаніях, де основною метою є отримання максимальної кількості відгуків за рахунок масштабності.

Водночас значну небезпеку становлять цільові атаки, орієнтовані на конкретну особу або групу осіб у межах організації. На відміну від масових атак, такі дії характеризуються високим рівнем підготовки та персоналізації. У процесі підготовки зловмисник здійснює попередній збір інформації про потенційну жертву, використовуючи як відкриті джерела (соціальні мережі, професійні платформи, корпоративні сайти), так і непрямі канали отримання даних. Аналізу підлягають посада працівника, його функціональні обов’язки, участь у проєктах, коло професійних контактів, стиль комунікації, а також внутрішні процеси організації.

Отримана інформація дозволяє сформувати максимально

правдоподібний сценарій взаємодії, який відповідає контексту діяльності жертви. Наприклад, зловмисник може імітувати лист від безпосереднього керівника, партнера або підрозділу технічної підтримки, використовуючи релевантну термінологію, внутрішні назви документів чи проєктів. Такий рівень деталізації значно знижує рівень підозри з боку працівника та сприяє формуванню довіри до отриманого повідомлення [61, с. 56].

Особливу небезпеку становить той факт, що цільові атаки часто спрямовуються на співробітників, які мають розширені права доступу до інформаційних систем, фінансових ресурсів або управлінських функцій. Компрометація облікових даних або дій таких осіб може призвести до масштабних наслідків, включаючи витік конфіденційної інформації, фінансові втрати або порушення операційної діяльності організації. Саме тому spear phishing розглядається як один із найбільш складних і небезпечних різновидів соціоінженерних атак, що потребує особливої уваги з боку системи інформаційної безпеки.

Окремо виділяють прямі та опосередковані вектори впливу, які відрізняються характером взаємодії між зловмисником і жертвою. Прямий вектор передбачає безпосередній контакт, у межах якого комунікація відбувається в режимі реального часу. Це може бути телефонний дзвінок, відеозв’язок або навіть особиста зустріч. Такий формат взаємодії дозволяє зловмиснику активно впливати на поведінку жертви, використовуючи інтонацію, швидкість мовлення, психологічний тиск або авторитет. Крім того, безпосередній контакт дає змогу оперативно реагувати на сумніви чи заперечення співрозмовника, змінювати аргументацію та адаптувати сценарій атаки залежно від ситуації [23, с. 54].

Прямі атаки часто супроводжуються створенням атмосфери терміновості або критичності, що змушує жертву приймати рішення без належного аналізу. Наприклад, зловмисник може повідомити про нібито технічну проблему, яка потребує негайного втручання, або про необхідність термінового виконання фінансової операції. У таких умовах працівник

схильний діяти імпульсивно, що підвищує ймовірність помилки.

На противагу цьому, опосередкований вектор впливу реалізується через використання різноманітних каналів комунікації, які не передбачають миттєвої взаємодії. До них належать електронна пошта, месенджери, вебсайти або інші цифрові платформи. У цьому випадку зловмисник не має можливості безпосередньо впливати на реакцію жертви в реальному часі, однак компенсує це за рахунок ретельної підготовки контенту, використання візуальних елементів, що імітують офіційні ресурси, а також створення переконливих текстових повідомлень. Опосередковані атаки часто базуються на використанні фішингових сторінок, підроблених інтерфейсів або шкідливих посилань, які стимулюють користувача до самостійного виконання небезпечних дій. При цьому жертва має більше часу для аналізу отриманої інформації, однак через звичність цифрових комунікацій та перевантаження інформаційними потоками рівень критичного сприйняття часто знижується, що створює умови, за яких навіть очевидні ознаки шахрайства можуть залишатися непоміченими [26, с. 84].

Таким чином, як прямі, так і опосередковані вектори впливу мають свої особливості та переваги з точки зору зловмисника. Вибір конкретного підходу залежить від мети атаки, доступної інформації про жертву та необхідного рівня контролю над процесом взаємодії. У практиці соціальної інженерії ці вектори часто комбінуються, що дозволяє підвищити ефективність атак і значно ускладнює їх виявлення та попередження.

З метою узагальнення зазначеного підходу доцільно представити класифікацію соціоінженерних атак за векторами впливу у табл. 1.3.

Таблиця 1.3

Класифікація соціоінженерних атак за векторами впливу

Вектор атаки	**Характеристика**	**Рівень ризику**
Масовий	Орієнтація на широку аудиторію без персоналізації	Середній
Цільовий	Персоналізований вплив на конкретну особу	Високий
Прямий	Безпосередній контакт із жертвою	Високий
Опосередкований	Вплив через комунікаційні канали	Середній

Після розгляду векторів впливу доцільно перейти до аналізу каналів реалізації соціоінженерних атак, які визначають технічне або комунікаційне середовище, у якому відбувається взаємодія між зловмисником і жертвою. Саме вибір каналу значною мірою впливає на ефективність атаки, її масштабованість, рівень довіри з боку користувача та складність виявлення. У сучасних умовах розвитку цифрових технологій кількість таких каналів постійно зростає, що ускладнює процес їх контролю та підвищує ризики для організацій. Найбільш поширеним каналом є електронна пошта, яка використовується для розповсюдження фішингових повідомлень, що імітують офіційні запити від банків, керівництва або внутрішніх служб організації. Висока ефективність цього каналу пояснюється його універсальністю та звичністю для користувачів, адже електронна пошта є основним засобом ділової комунікації. Крім того, сучасні технології дозволяють зловмисникам створювати високоякісні підроблені повідомлення з використанням корпоративної символіки, підписів та навіть доменів, що візуально майже не відрізняються від справжніх. Це значно ускладнює процес ідентифікації загрози з боку працівників [33, с. 64].

Значного поширення також набули телефонні атаки, відомі як вішинг, у межах яких зловмисник, представляючись працівником служби підтримки, банку або керівництва, намагається отримати конфіденційну інформацію або змусити жертву виконати певні дії. Перевагою цього каналу є можливість безпосереднього психологічного впливу та встановлення довіри через голосову комунікацію. Інтонація, впевненість у голосі, використання професійної лексики та створення ситуації терміновості дозволяють зловмиснику ефективно впливати на емоційний стан жертви та знижувати рівень критичного мислення.

Окрім цього, активно використовуються текстові повідомлення, або так званий smishing, який передбачає надсилання коротких повідомлень із посиланнями на підроблені ресурси або з проханням виконати певні дії. Особливістю цього каналу є обмежений обсяг інформації, що змушує

зловмисників використовувати максимально лаконічні, але водночас емоційно насичені повідомлення, які апелюють до страху, терміновості або вигоди. Завдяки широкому використанню мобільних пристроїв такі атаки стають дедалі ефективнішими [24, с. 35].

Соціальні мережі також виступають важливим каналом реалізації соціоінженерних атак, оскільки надають зловмисникам доступ до значного обсягу персональної інформації про користувачів. Використовуючи підроблені або скомпрометовані акаунти, зловмисники можуть встановлювати довірчі контакти, поступово збирати додаткові відомості та реалізовувати складні багатоступеневі сценарії атак. Особливу небезпеку становить можливість імітації реальних осіб, що значно підвищує рівень довіри з боку жертви [38, с. 75].

Не менш важливими є фізичні канали реалізації, які передбачають безпосередній доступ до приміщень організації або використання матеріальних носіїв інформації. До таких методів належать підкидання заражених USB-носіїв, несанкціоноване проникнення в офіс під виглядом співробітника чи підрядника, а також спроби отримання інформації через особистий контакт. Незважаючи на розвиток цифрових технологій, фізичні атаки залишаються актуальними, оскільки дозволяють обійти значну частину технічних засобів захисту.

З метою систематизації наведених каналів реалізації соціоінженерних атак доцільно представити їх у табл. 1.4.

Аналіз представлених каналів дозволяє зробити висновок, що кожен із них має власні специфічні особливості, які визначають як спосіб реалізації атаки, так і рівень її ефективності. При цьому вибір каналу безпосередньо впливає на характер взаємодії між зловмисником і жертвою, швидкість поширення атаки, можливість її масштабування, а також складність виявлення та реагування.

Таблиця 1.4

Класифікація соціоінженерних атак за каналами реалізації

Канал реалізації	**Характеристика**	**Типові методи**	**Особливості впливу**	**Рівень ризику**
Електронна пошта	Масова цифрова комунікація	Фішинг, вкладення, посилання	Висока правдоподібність	Високий
Телефон	Голосова взаємодія в реальному часі	Вішинг	Сильний психологічний вплив	Високий
SMS	Короткі мобільні повідомлення	Smishing	Терміновість, обмежений аналіз	Середній
Соціальні мережі	Онлайн-платформи для комунікації	Фейкові профілі, шахрайство	Використання довіри та персональних даних	Високий
Вебресурси	Підроблені сайти або інтерфейси	Фішингові сторінки	Імітація офіційних сервісів	Високий
Фізичні канали	Безпосередній доступ або матеріальні носії	USB-атаки, проникнення	Обхід цифрових засобів захисту	Критичний

Наприклад, цифрові канали забезпечують високу швидкість і масовість розповсюдження атак, тоді як прямі або фізичні канали дозволяють досягти більшого рівня довіри та персоналізації впливу.

Водночас ключовим фактором успішності соціоінженерної атаки залишається не стільки технічний канал, скільки здатність зловмисника адаптувати зміст повідомлення до конкретного контексту діяльності організації та психологічних особливостей користувача. Саме контекстуалізація інформації, використання актуальних для працівника тем, внутрішньої термінології, посилання на реальні процеси або події значно підвищують рівень довіри до отриманого повідомлення. У поєднанні з урахуванням поведінкових характеристик користувача це дозволяє зловмиснику формувати максимально переконливі сценарії взаємодії, які важко ідентифікувати як загрозу навіть для досвідчених працівників [25, с. 74].

Крім того, слід враховувати, що ефективність каналу значною мірою залежить від рівня цифрової зрілості організації, особливостей її внутрішніх

комунікацій та наявних процедур перевірки інформації. У середовищах, де активно використовуються електронні сервіси та дистанційна взаємодія, підвищується вразливість до фішингових атак і підроблених вебресурсів. Водночас організації з відкритим доступом до фізичних приміщень або недостатнім контролем ідентифікації персоналу можуть бути більш уразливими до фізичних форм соціальної інженерії.

Таким чином, канали реалізації соціоінженерних атак виступають важливим елементом їх структури, оскільки визначають форму та умови взаємодії між зловмисником і жертвою. Вони не лише забезпечують технічну можливість здійснення атаки, але й формують її психологічний контекст, впливаючи на сприйняття інформації користувачем та його подальші дії.

Їх різноманітність та постійна еволюція зумовлюють необхідність застосування комплексного підходу до забезпечення інформаційної безпеки, який поєднує технічні, організаційні та поведінкові заходи. Зокрема, ефективна протидія соціоінженерним загрозам передбачає не лише впровадження сучасних засобів фільтрації та моніторингу, але й систематичне навчання персоналу, розвиток навичок критичного мислення, а також формування культури безпечної поведінки в інформаційному середовищі [29, с. 74].

Розуміння специфіки каналів реалізації соціоінженерних атак є необхідною умовою для побудови ефективної системи захисту, орієнтованої не лише на технічні аспекти безпеки, але й на управління людським фактором як ключовим елементом ризику.

1.3 Аналіз психологічних механізмів маніпуляції та чинників вразливості персоналу

Ефективність соціоінженерних атак значною мірою визначається використанням психологічних механізмів впливу на людину, які дозволяють зловмиснику змінювати поведінку жертви без застосування технічного

примусу. На відміну від класичних кіберзагроз, де основний акцент робиться на вразливостях програмного забезпечення, соціальна інженерія базується на експлуатації особливостей людського мислення, емоційних реакцій та соціальної поведінки.

Людина в умовах повсякденної діяльності часто приймає рішення не на основі раціонального аналізу, а керуючись автоматичними когнітивними процесами, що спрощують обробку інформації. Саме ці механізми стають основою для маніпуляцій, оскільки дозволяють зловмиснику впливати на жертву швидко та ефективно, мінімізуючи ймовірність критичного осмислення ситуації. Одним із ключових психологічних механізмів є принцип авторитету, відповідно до якого люди схильні довіряти інформації, що надходить від осіб або організацій, які сприймаються як компетентні або владні. У контексті соціальної інженерії це проявляється у використанні образу керівника, адміністратора системи або представника офіційної установи. Працівник, отримавши відповідний запит, може виконати його без додаткової перевірки, вважаючи його легітимним [28, с.64].

Іншим важливим механізмом є створення відчуття терміновості, яке обмежує час на прийняття рішення та знижує здатність до критичного мислення. Повідомлення, що містять формулювання на кшталт «терміново», «негайно» або
«обмежений час», стимулюють імпульсивну реакцію та підвищують ймовірність помилкових дій.

Також широко використовується принцип дефіциту, який базується на психологічній схильності людини надавати більшу цінність ресурсам або можливостям, доступ до яких обмежений у часі чи кількості. У соціоінженерних сценаріях це може проявлятися у вигляді повідомлень про обмежений доступ до сервісу або необхідність швидкого підтвердження даних.

Не менш важливим є механізм взаємності, який передбачає, що людина відчуває зобов’язання відповісти на отриману послугу або допомогу.

Зловмисники можуть спочатку створити ілюзію підтримки або надання корисної інформації, після чого звернутися із запитом, який виглядає як логічне продовження взаємодії [33, с. 64].

Крім того, значну роль відіграє соціальне підтвердження, коли люди орієнтуються на поведінку інших у процесі прийняття рішень. Повідомлення про те, що «інші працівники вже виконали певну дію», створює додатковий психологічний тиск і стимулює наслідування.

З метою систематизації зазначених механізмів доцільно представити їх у табл. 1.5.

Таблиця 1.5

Основні психологічні механізми соціоінженерного впливу

Механізм	**Суть впливу**	**Приклад застосування**
Авторитет	Довіра до посадових осіб	Лист від "керівника"
Терміновість	Обмеження часу на прийняття рішення	"Терміново змініть пароль"
Дефіцит	Страх втрати можливості	"Доступ буде заблоковано"
Взаємність	Почуття обов’язку	"Ми вам допомогли — підтвердьте дані"
Соціальне підтвердження	Орієнтація на дії інших	"Всі співробітники вже виконали"

Окрім психологічних механізмів, важливим аспектом є аналіз чинників вразливості персоналу, які визначають схильність працівників до соціоінженерного впливу. Саме ці чинники формують передумови, за яких навіть добре побудована система інформаційної безпеки може бути порушена внаслідок помилкових або необачних дій користувачів. Вразливість персоналу є комплексним явищем, що виникає під впливом як індивідуальних характеристик працівника, так і особливостей організаційного середовища, в якому він функціонує.

Індивідуальні чинники пов’язані з особистісними характеристиками працівника, рівнем його обізнаності у сфері інформаційної безпеки, професійним досвідом, когнітивними здібностями, а також емоційним станом. Рівень знань і навичок у сфері кібербезпеки безпосередньо впливає на здатність користувача розпізнавати потенційні загрози та адекватно реагувати

на них. Працівники, які не проходили спеціалізованого навчання або не мають практичного досвіду взаємодії з подібними загрозами, значно частіше стають жертвами соціоінженерних атак [28, с.73].

Окрему роль відіграють когнітивні особливості, зокрема здатність до критичного мислення, уважність до деталей та схильність перевіряти отриману інформацію. У ситуаціях інформаційного перевантаження або багатозадачності працівники часто використовують спрощені моделі прийняття рішень, що підвищує ризик помилок. Наприклад, перевантаженість роботою, дефіцит часу або необхідність швидкого реагування можуть призводити до поверхневого аналізу повідомлень і ігнорування ознак шахрайства.

Емоційний стан також суттєво впливає на рівень вразливості. Стрес, втома, тривожність або, навпаки, надмірна впевненість можуть знижувати здатність до раціонального оцінювання ситуації. У таких умовах працівник більш схильний діяти імпульсивно, покладаючись на перше враження або авторитет джерела інформації. Це створює сприятливі умови для реалізації атак, що апелюють до емоційних реакцій, таких як страх, терміновість або бажання уникнути негативних наслідків [34, с. 93].

Не менш важливим є рівень відповідальності та мотивації працівника щодо дотримання правил інформаційної безпеки. У випадках, коли безпека сприймається як формальність або другорядне завдання, користувачі можуть свідомо ігнорувати встановлені процедури, наприклад, не перевіряти джерело повідомлення або використовувати слабкі паролі. Таким чином, індивідуальні чинники формують поведінковий профіль працівника, який визначає його стійкість до маніпулятивного впливу.

Організаційні чинники визначаються особливостями внутрішнього середовища організації, зокрема структурою управління, наявністю чітко визначених політик безпеки, рівнем контролю за їх дотриманням, системою навчання персоналу та загальною культурою інформаційної безпеки. Відсутність або формальний характер політик безпеки призводить до того, що

працівники не мають чітких орієнтирів щодо безпечної поведінки, що значно підвищує ризик помилкових дій [19, с. 84].

Система навчання персоналу відіграє ключову роль у зниженні вразливості. Регулярні тренінги, моделювання атак та інформування про актуальні загрози сприяють формуванню навичок розпізнавання соціоінженерних сценаріїв. У разі відсутності таких заходів працівники залишаються неготовими до протидії сучасним формам шахрайства, які постійно еволюціонують.

Важливим фактором є також рівень контролю та відповідальності в організації. Якщо відсутні механізми перевірки виконання критичних дій, наприклад підтвердження фінансових операцій або доступу до конфіденційної інформації, зловмисники отримують можливість використовувати соціальну інженерію для обходу формальних обмежень. Крім того, надмірна централізація або, навпаки, недостатня регламентація процесів можуть створювати додаткові ризики [10, с. 74].

Особливе значення має організаційна культура, яка формує загальне ставлення працівників до питань безпеки. У середовищі, де заохочується відповідальне ставлення до інформації, відкрите обговорення інцидентів та підтримка з боку керівництва, працівники більш уважно ставляться до потенційних загроз. Натомість у культурах, де помилки караються або ігноруються, працівники можуть приховувати інциденти або не надавати їм належного значення, що ускладнює їх своєчасне виявлення [10, с. 74].

Таким чином, індивідуальні та організаційні чинники вразливості персоналу перебувають у тісному взаємозв’язку та взаємно підсилюють один одного. Навіть високий рівень технічного захисту не гарантує безпеки за умов низької обізнаності персоналу або недосконалості внутрішніх процесів. Тому ефективна протидія соціоінженерним загрозам потребує комплексного підходу, який враховує як поведінкові особливості працівників, так і організаційні умови їх діяльності.

З метою узагальнення та систематизації основних чинників, що

визначають вразливість персоналу до соціоінженерних атак, доцільно представити їх у структурованому вигляді. Такий підхід дозволяє чітко розмежувати індивідуальні та організаційні аспекти впливу, а також оцінити їх значущість у контексті забезпечення інформаційної безпеки (табл. 1.6).

Таблиця 1.6

Чинники вразливості персоналу

Категорія	**Фактор**	**Вплив на безпеку**
Індивідуальні	Низька обізнаність	Високий
	Стрес та перевантаження	Високий
	Недостатній досвід	Середній
Організаційні	Відсутність навчання	Критичний
	Слабкі політики безпеки	Критичний
	Недостатній контроль	Високий

Аналіз представлених у таблиці чинників свідчить, що вразливість персоналу формується під впливом як особистісних характеристик працівників, так і особливостей організаційного середовища. При цьому індивідуальні чинники визначають поведінкову реакцію конкретної особи на потенційні загрози, тоді як організаційні створюють умови, у яких така поведінка реалізується. Особливої уваги потребує взаємодія цих груп чинників, оскільки їх поєднання може суттєво підвищувати рівень ризику. Наприклад, низький рівень обізнаності працівника у поєднанні з відсутністю належного контролю або навчання в організації створює сприятливі умови для успішної реалізації соціоінженерної атаки. Водночас навіть високий рівень індивідуальної підготовки може бути недостатнім за умов недосконалих організаційних процесів [49, с. 94].

Таким чином, представлена систематизація чинників вразливості дозволяє не лише ідентифікувати ключові ризики, але й сформувати основу для розробки ефективних заходів протидії соціоінженерним загрозам, що мають враховувати як людський, так і організаційний аспект забезпечення інформаційної безпеки.

Для кращого розуміння взаємозв’язку між психологічними механізмами впливу та поведінкою працівника доцільно розглянути соціоінженерну атаку

як послідовний процес, що включає декілька взаємопов’язаних етапів. Такий підхід дозволяє не лише виявити ключові точки впливу на користувача, але й простежити, яким чином психологічні фактори трансформуються у конкретні дії, що призводять до порушення інформаційної безпеки.

У межах цього процесу зловмисник цілеспрямовано використовує певні психологічні тригери, які викликають у жертви відповідну емоційну реакцію, наприклад довіру, страх, терміновість або зацікавленість. Ці реакції, у свою чергу, знижують рівень критичного мислення та здатність до раціонального аналізу ситуації. У результаті працівник може прийняти рішення, яке суперечить встановленим правилам безпеки, але виглядає логічним у межах створеного зловмисником контексту.

Важливо зазначити, що цей процес має циклічний та адаптивний характер. Зловмисник може змінювати тактику впливу залежно від реакції жертви, підсилюючи або послаблюючи психологічний тиск. Крім того, на кожному етапі атаки використовуються різні механізми впливу, що підвищує її ефективність і ускладнює виявлення [16, с. 66].

З метою наочного відображення зазначених етапів та їх взаємозв’язку доцільно представити узагальнений психологічний механізм соціоінженерної атаки у вигляді схеми (рис. 1.2).

Показаний на рис. 1.2 механізм демонструє, що ключовим елементом атаки є трансформація зовнішнього впливу у внутрішню реакцію користувача, яка визначає його подальші дії. Саме на етапі емоційного реагування та зниження критичного мислення відбувається найбільша вразливість, оскільки працівник переходить від раціональної оцінки ситуації до автоматичних поведінкових моделей.

Крім того, схема ілюструє, що кінцевим результатом соціоінженерного впливу є не сам факт комунікації, а конкретна дія працівника, яка призводить до порушення інформаційної безпеки, наприклад передача конфіденційних даних, відкриття шкідливого файлу або надання доступу до системи. Це підкреслює, що основною метою зловмисника є саме поведінкова зміна, а не лише встановлення контакту.

Рис. 1.2 Психологічний механізм соціоінженерної атаки

Висновки до розділу 1

У розділі проведено комплексний аналіз соціоінженерних загроз як одного з найбільш небезпечних чинників дестабілізації корпоративної інформаційної безпеки. Встановлено, що соціальна інженерія являє собою сукупність методів психологічного впливу на людину, спрямованих на отримання конфіденційної інформації, несанкціонованого доступу до інформаційних ресурсів або спонукання працівників до виконання дій, що суперечать встановленим правилам безпеки.

Виявлено, що на відміну від традиційних кіберзагроз, соціоінженерні атаки орієнтовані насамперед на використання людського фактору як найбільш уразливої складової системи захисту. Визначено, що ефективність таких атак значною мірою зумовлюється особливостями людської поведінки, рівнем довіри, когнітивними викривленнями, емоційними реакціями та недостатньою обізнаністю персоналу щодо сучасних інформаційних загроз.

У розділі систематизовано основні види соціоінженерних атак та проведено їх класифікацію за векторами впливу і каналами реалізації. З’ясовано, що найбільш поширеними формами соціальної інженерії є фішинг, цільовий фішинг, телефонне шахрайство, претекстинг, baiting та інші методи маніпулятивного впливу. А також визначено, що сучасні соціоінженерні атаки характеризуються високим рівнем адаптивності, персоналізації та складністю своєчасного виявлення.

Особливу увагу приділено дослідженню психологічних механізмів маніпуляції та чинників вразливості персоналу. Встановлено, що успішність соціоінженерного впливу базується на використанні авторитету, терміновості, довіри, соціального наслідування, страху та інших психологічних факторів. Доведено, що рівень захищеності організації значною мірою залежить не лише від технічних засобів захисту, але й від рівня обізнаності працівників та сформованої культури інформаційної безпеки.

Загалом, результати дослідження в першому розділі підтверджують, що

соціальна інженерія є комплексною міждисциплінарною загрозою, яка потребує поєднання технічних, організаційних і поведінкових механізмів протидії.

Таким чином, представлення соціоінженерної атаки як послідовного психологічного процесу дозволяє глибше зрозуміти механізми її реалізації та визначити критичні точки, на які мають бути спрямовані заходи протидії, зокрема підвищення обізнаності персоналу та розвиток навичок розпізнавання маніпулятивного впливу [33, с. 64].

Ефективна протидія соціоінженерним загрозам неможлива без глибокого розуміння психологічних аспектів поведінки персоналу та створення умов, за яких працівники здатні своєчасно розпізнавати маніпуляції та приймати обґрунтовані рішення у сфері інформаційної безпеки.

РОЗДІЛ 2 МЕТОДИЧНІ ПІДХОДИ ДО ОРГАНІЗАЦІЇ СИСТЕМИ ЗАХИСТУ ВІД СОЦІОІНЖЕНЕРНИХ ЗАГРОЗ

2.1. Формування принципів побудови комплексної моделі протидії соціоінженерним загрозам

Сучасні умови функціонування організацій характеризуються зростаючою складністю інформаційного середовища та підвищенням рівня загроз, що пов’язані з людським фактором. Соціоінженерні атаки, які базуються на маніпуляції поведінкою персоналу, суттєво ускладнюють процес забезпечення інформаційної безпеки, оскільки їх реалізація не обмежується технічними вразливостями систем. У зв’язку з цим виникає необхідність формування комплексної моделі протидії, яка інтегрує технічні, організаційні та поведінкові аспекти захисту.

Методичне підґрунтя побудови такої моделі базується на розумінні соціальної інженерії як багатовимірного явища, що функціонує на перетині інформаційних технологій, психології та управління. Це зумовлює необхідність переходу від фрагментарних заходів захисту до системного підходу, в межах якого протидія загрозам розглядається як безперервний процес, інтегрований у загальну систему управління інформаційною безпекою організації [44, с. 95].

Формування принципів побудови комплексної моделі передбачає визначення базових положень, які забезпечують її цілісність, адаптивність та ефективність у динамічному середовищі загроз. Одним із ключових принципів є принцип системності, який передбачає розгляд соціоінженерних ризиків не ізольовано, а як складової загальної системи інформаційної безпеки. У межах цього підходу всі елементи захисту — технічні засоби, організаційні процедури та поведінкові аспекти — повинні функціонувати узгоджено, доповнюючи один одного.

Не менш важливим є принцип багаторівневості, відповідно до якого захист від соціоінженерних загроз реалізується на декількох рівнях:

індивідуальному, організаційному та технологічному. На індивідуальному рівні основна увага приділяється формуванню безпечної поведінки працівників, розвитку їх критичного мислення та здатності розпізнавати маніпулятивні впливи. Організаційний рівень передбачає впровадження політик безпеки, регламентів та процедур, які регулюють взаємодію персоналу з інформаційними ресурсами. Технологічний рівень забезпечує технічну підтримку цих процесів шляхом використання засобів контролю доступу, моніторингу та виявлення підозрілої активності [50, с.74].

Важливим принципом є також адаптивність, яка полягає у здатності системи захисту змінюватися відповідно до нових типів загроз та сценаріїв атак. Соціоінженерні методи постійно еволюціонують, що вимагає регулярного оновлення підходів до їх виявлення та нейтралізації. У цьому контексті особливого значення набуває безперервний моніторинг інцидентів, аналіз поведінки користувачів та актуалізація навчальних програм для персоналу.

Принцип проактивності передбачає орієнтацію не лише на реагування на вже реалізовані інциденти, але й на їх попередження. Це досягається шляхом ідентифікації потенційних вразливостей у поведінці персоналу, моделювання соціоінженерних атак та проведення превентивних заходів. Такий підхід дозволяє зменшити ймовірність успішної реалізації атак ще на ранніх етапах.

Окремої уваги заслуговує принцип інтегрованості, який полягає у включенні заходів протидії соціоінженерним загрозам до загальної системи управління ризиками організації. Це означає, що оцінка соціоінженерних ризиків повинна здійснюватися нарівні з іншими видами ризиків, а відповідні заходи — бути частиною стратегічного планування у сфері безпеки [46, с. 84].

З метою узагальнення основних принципів побудови комплексної моделі доцільно представити їх у структурованому вигляді (табл. 2.1).

Таблиця 2.1

Принципи побудови комплексної моделі протидії соціоінженерним загрозам

Принцип	**Суть**	**Практичне значення**
Системність	Узгодженість усіх елементів захисту	Забезпечення цілісності системи
Багаторівневість	Захист на індивідуальному, організаційному та технічному рівнях	Зниження ймовірності обходу захисту
Адаптивність	Гнучке реагування на нові загрози	Актуальність системи захисту
Проактивність	Попередження інцидентів	Зменшення ризиків
Інтегрованість	Включення у систему управління ризиками	Підвищення ефективності управління

Подальший розвиток комплексної моделі передбачає визначення її структурних компонентів, які забезпечують реалізацію зазначених принципів. У загальному вигляді така модель може бути представлена як сукупність взаємопов’язаних підсистем, кожна з яких виконує окрему функцію у процесі протидії соціоінженерним загрозам.

До ключових компонентів моделі належить підсистема ідентифікації загроз, яка забезпечує виявлення потенційних соціоінженерних сценаріїв на основі аналізу внутрішніх і зовнішніх факторів. Вона базується на зборі інформації про поведінку користувачів, аналізі комунікаційних каналів та виявленні аномалій, що можуть свідчити про спроби маніпуляції.

Наступним елементом є підсистема оцінювання ризиків, яка дозволяє визначити рівень загрози та потенційні наслідки соціоінженерних атак. У межах цієї підсистеми здійснюється аналіз вразливостей персоналу, критичності інформаційних ресурсів та ймовірності реалізації атак. Результати оцінювання використовуються для пріоритезації заходів захисту [48, с. 75].

Підсистема управління поведінкою персоналу є ключовою складовою комплексної моделі, оскільки саме людський фактор виступає основним об’єктом впливу соціальної інженерії. Вона включає заходи з підвищення обізнаності, навчання, формування культури безпеки та розвитку навичок розпізнавання маніпуляцій. Ефективність цієї підсистеми значною мірою

визначає загальний рівень стійкості організації до соціоінженерних загроз.

Технічна підсистема забезпечує підтримку організаційних та поведінкових заходів шляхом використання сучасних засобів інформаційної безпеки. До неї належать системи фільтрації електронної пошти, засоби багатофакторної автентифікації, системи моніторингу поведінки користувачів та інші інструменти, які дозволяють виявляти та блокувати підозрілу активність.

Завершальним елементом є підсистема реагування на інциденти, яка забезпечує своєчасне виявлення, локалізацію та усунення наслідків соціоінженерних атак. Вона включає процедури повідомлення про інциденти, аналіз їх причин та впровадження коригувальних заходів з метою запобігання повторенню [55, с. 84].

З метою наочного відображення структури комплексної моделі доцільно представити її у вигляді схеми (рис. 2.1).

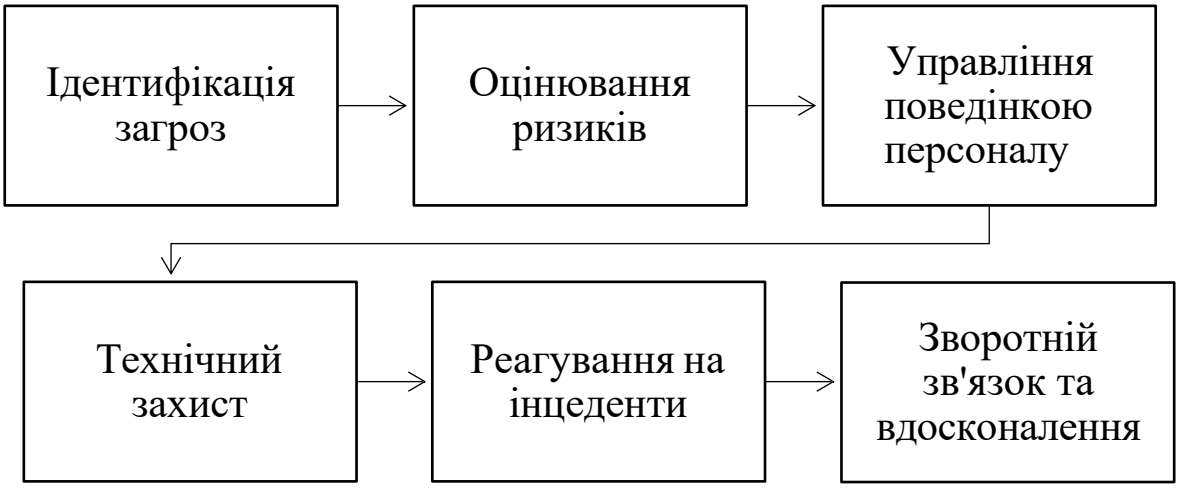

Рис. 2.1. Структура комплексної моделі протидії соціоінженерним загрозам

Представлена схема відображає циклічний характер функціонування системи, у межах якого результати реагування на інциденти використовуються для вдосконалення всіх попередніх етапів. Такий підхід забезпечує безперервний розвиток системи захисту та її адаптацію до нових умов [32, с 84].

Таким чином, формування принципів побудови комплексної моделі

протидії соціоінженерним загрозам є ключовим етапом у створенні ефективної системи інформаційної безпеки. Запропонований підхід дозволяє інтегрувати різні аспекти захисту в єдину систему, орієнтовану на управління людським фактором як основним джерелом ризику. Реалізація такої моделі створює передумови для підвищення стійкості організації до сучасних загроз та забезпечення належного рівня захисту інформаційних ресурсів.

2.2 Систематизація підходів до ідентифікації та оцінювання соціоінженерних ризиків

Ефективність побудови системи протидії соціоінженерним загрозам безпосередньо залежить від здатності організації своєчасно ідентифікувати відповідні ризики та здійснювати їх обґрунтоване оцінювання. На відміну від класичних кіберзагроз, які мають переважно технічну природу, соціоінженерні ризики формуються у площині поведінки персоналу, комунікаційних процесів та організаційного середовища. Це зумовлює необхідність застосування комплексних методичних підходів, що поєднують кількісні та якісні методи аналізу.

Ідентифікація соціоінженерних ризиків являє собою процес виявлення потенційних сценаріїв впливу на персонал, які можуть призвести до порушення інформаційної безпеки. Вона базується на аналізі внутрішніх процесів організації, характеру взаємодії працівників, використовуваних каналів комунікації та рівня обізнаності персоналу. Важливим аспектом є врахування специфіки діяльності організації, оскільки саме контекст визначає типові сценарії соціоінженерних атак [27, с. 64].

У межах методичного підходу до ідентифікації доцільно розглядати соціоінженерний ризик як функцію трьох взаємопов’язаних складових: наявності вразливості, ймовірності реалізації загрози та потенційних наслідків.

Такий підхід дозволяє структурувати процес аналізу та забезпечити його системність.

Процес ідентифікації ризиків включає декілька взаємопов’язаних етапів, що формують логічно завершений аналітичний цикл. На початковому етапі здійснюється аналіз активів організації, до яких належать інформаційні ресурси, облікові записи, фінансові системи та інші критичні елементи. Важливим є визначення тих активів, доступ до яких може бути отриманий через маніпуляцію персоналом.

Наступним етапом є виявлення потенційних вразливостей, які пов’язані не лише з технічними аспектами, але й з поведінковими характеристиками працівників. До таких вразливостей належать низький рівень обізнаності, відсутність процедур перевірки запитів, надмірна довіра до внутрішніх комунікацій, а також недосконалість організаційних регламентів.

Подальший аналіз передбачає визначення можливих сценаріїв реалізації соціоінженерних атак. У цьому контексті важливим є моделювання типових ситуацій, у яких зловмисник може впливати на працівника, використовуючи різні канали комунікації та психологічні механізми. Такий підхід дозволяє не лише виявити потенційні загрози, але й оцінити їх правдоподібність у конкретному організаційному середовищі [34, с. 82].

Завершальним етапом ідентифікації є формування переліку ризиків, що відображає взаємозв’язок між активами, вразливостями та можливими загрозами. Отриманий перелік слугує основою для подальшого оцінювання та управління ризиками.

З метою узагальнення підходів до ідентифікації соціоінженерних ризиків доцільно представити їх у табл. 2.2.

Таблиця 2.2

Підходи до ідентифікації соціоінженерних ризиків

Підхід	**Суть**	**Особливості застосування**
Активно-орієнтований	Аналіз критичних ресурсів	Визначення цілей атак
Вразливісний	Виявлення слабких місць персоналу	Орієнтація на людський фактор

Продовження табл. 2.2

Підхід	**Суть**	**Особливості застосування**
Сценарний	Моделювання можливих атак	Висока гнучкість
Процесний	Аналіз бізнес-процесів	Виявлення ризиків у комунікації

Після ідентифікації ризиків виникає необхідність їх оцінювання, яке дозволяє визначити рівень небезпеки та пріоритетність реагування. Оцінювання соціоінженерних ризиків є складним завданням через неможливість повної формалізації поведінкових факторів. У зв'язку з цим застосовуються комбіновані методи, що поєднують експертні оцінки, статистичні дані та аналітичні моделі [39, с. 87].

У загальному вигляді оцінювання ризику передбачає визначення двох основних параметрів: ймовірності реалізації загрози та масштабу можливих наслідків. Ймовірність визначається на основі аналізу частоти подібних інцидентів, рівня підготовки персоналу та наявності захисних механізмів. Наслідки оцінюються з урахуванням потенційних втрат, які можуть бути як фінансовими, так і репутаційними або операційними.

У межах кількісного підходу ризик може бути представлений у вигляді функціональної залежності між зазначеними параметрами:

$$R = P \times I, \tag{2.1}$$

де, R – рівень ризику,

P – ймовірність реалізації,

I – масштаб наслідків.

Однак у випадку соціоінженерних загроз така модель має обмеження, оскільки не враховує поведінкову невизначеність. Тому на практиці широко застосовуються якісні методи оцінювання, які передбачають використання шкал та категорій ризику [62, с 88].

Одним із найбільш поширених інструментів є матриця ризиків, яка

дозволяє класифікувати ризики за рівнем їх критичності. Вона базується на перехресному аналізі ймовірності та наслідків і забезпечує наочне представлення результатів оцінювання (табл. 2.3).

Таблиця 2.3

Матриця оцінювання соціоінженерних ризиків

Ймовірність / Наслідки	**Низькі**	**Середні**	**Високі**
Низька	Низький	Низький	Середній
Середня	Низький	Середній	Високий
Висока	Середній	Високий	Критичний

Застосування матриці дозволяє визначити пріоритетність заходів реагування та оптимально розподілити ресурси організації. При цьому особлива увага приділяється ризикам, які мають високий або критичний рівень, оскільки саме вони становлять найбільшу загрозу для інформаційної безпеки.

Окремим напрямом є використання поведінкового аналізу, який дозволяє оцінити схильність персоналу до соціоінженерного впливу. Такий підхід базується на аналізі результатів тестувань, навчальних симуляцій атак, а також спостереженні за реальними діями працівників у процесі виконання службових обов’язків. Отримані дані дозволяють сформувати профіль ризику для окремих категорій персоналу та визначити найбільш уразливі групи [10, с. 74].

Важливим елементом оцінювання є також врахування організаційних факторів, зокрема рівня зрілості системи інформаційної безпеки, наявності політик та процедур, а також ефективності контролю. У цьому контексті доцільно використовувати інтегровані моделі, які поєднують технічні та поведінкові показники.

З метою узагальнення процесу оцінювання соціоінженерних ризиків доцільно представити його у вигляді послідовної схеми (рис. 2.2).

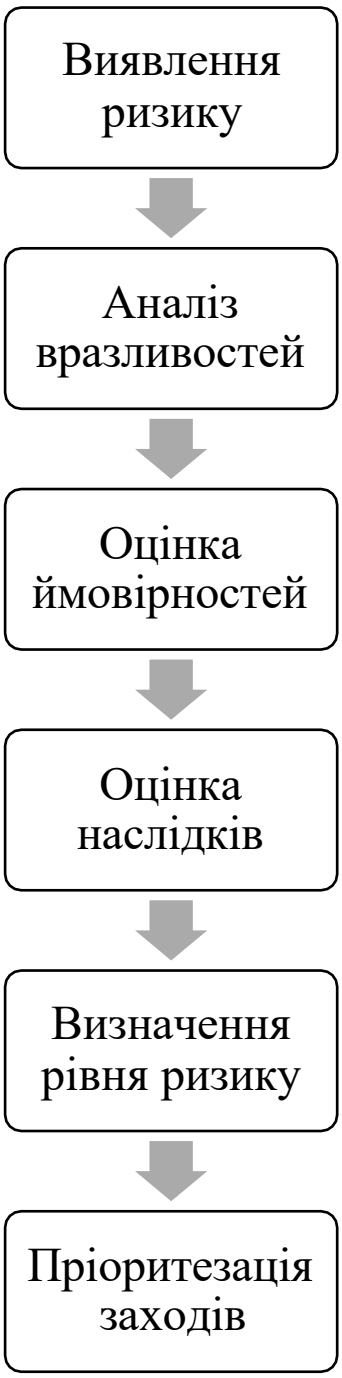

Рис. 2.2. Процес оцінювання соціоінженерних ризиків

Представлений процес демонструє, що оцінювання ризиків є не одноразовою процедурою, а безперервним циклом, який потребує регулярного оновлення, що зумовлено динамічністю соціоінженерних загроз та постійними змінами у поведінці персоналу та організаційному середовищі.

Таким чином, систематизація підходів до ідентифікації та оцінювання соціоінженерних ризиків дозволяє сформувати науково обґрунтовану основу

для побудови ефективної системи захисту. Поєднання різних методичних підходів забезпечує комплексність аналізу та підвищує точність оцінювання, що, у свою чергу, сприяє прийняттю обґрунтованих управлінських рішень у сфері інформаційної безпеки.

2.3 Аналіз підходів до формування стратегії підвищення рівня обізнаності персоналу

У сучасних умовах зростання ролі людського фактору у структурі інформаційних ризиків підвищення рівня обізнаності персоналу набуває стратегічного значення. Соціоінженерні загрози, які базуються на маніпуляції поведінкою користувачів, не можуть бути ефективно нейтралізовані виключно технічними засобами. У зв’язку з цим формування цілеспрямованої стратегії розвитку обізнаності персоналу виступає ключовим елементом комплексної системи захисту.

Стратегія підвищення обізнаності повинна розглядатися не як окремий захід, а як інтегрований управлінський процес, спрямований на формування стійких моделей безпечної поведінки працівників. Вона охоплює як освітній компонент, так і організаційні механізми, що забезпечують закріплення знань у практичній діяльності. У цьому контексті важливим є перехід від формального інформування до системного розвитку компетентностей у сфері інформаційної безпеки [1, с. 98].

Аналіз сучасних підходів дозволяє виокремити декілька концептуальних моделей формування такої стратегії, які відрізняються за змістом, інструментами реалізації та рівнем інтеграції в організаційну діяльність.

Перший підхід базується на традиційній освітній моделі, у межах якої основна увага приділяється передачі знань про загрози та правила безпечної поведінки. Його реалізація передбачає проведення навчальних заходів, інструктажів, лекцій та ознайомлення з нормативними документами. Незважаючи на свою поширеність, цей підхід має обмежену

ефективність, оскільки не забезпечує формування практичних навичок та не враховує поведінкові аспекти прийняття рішень.

Більш сучасним є поведінково-орієнтований підхід, який фокусується на зміні реальних дій працівників у процесі їхньої повсякденної діяльності. У його основі лежить розуміння того, що знання не завжди трансформуються у відповідну поведінку. Тому основний акцент робиться на формуванні звичок безпечної взаємодії з інформаційними ресурсами. Такий підхід передбачає використання регулярних тренувань, моделювання атак, аналізу поведінкових реакцій та надання зворотного зв'язку [23, с. 64].

Особливого значення набуває адаптивний підхід, який передбачає диференціацію навчальних заходів залежно від категорії персоналу, рівня доступу до інформаційних ресурсів та специфіки виконуваних функцій. У межах цього підходу стратегія будується з урахуванням того, що різні групи працівників мають різний рівень ризику та потребують індивідуалізованих програм підготовки. Наприклад, керівний склад та працівники фінансових підрозділів потребують більш глибокої підготовки щодо цільових атак, тоді як для інших категорій достатнім може бути базовий рівень обізнаності.

Інтеграційний підхід передбачає включення заходів з підвищення обізнаності до загальної системи управління інформаційною безпекою організації. У цьому випадку навчання персоналу стає невід'ємною частиною бізнес-процесів, а його результати враховуються при оцінюванні ризиків та прийнятті управлінських рішень. Такий підхід забезпечує узгодженість між політиками безпеки, технічними заходами та поведінковими аспектами діяльності персоналу [39, с.74].

З метою узагальнення розглянутих підходів доцільно представити їх у табл. 2.4

Таблиця 2.4

Підходи до формування стратегії підвищення обізнаності персоналу

Підхід	**Характеристика**	**Переваги**	**Обмеження**
Освітній	Передача знань	Простота реалізації	Низька поведінкова ефективність
Поведінковий	Формування навичок	Практична спрямованість	Потребує ресурсів

Продовження табл. 2.4

Підхід	Характеристика	Переваги	Обмеження
Адаптивний	Диференціація навчання	Врахування специфіки	Складність реалізації
Інтеграційний	Включення у систему управління	Комплексність	Необхідність змін у процесах

Формування ефективної стратегії передбачає поєднання зазначених підходів з урахуванням особливостей організації. Важливим аспектом є визначення цілей та критеріїв оцінювання результативності навчання. У цьому контексті доцільно розглядати не лише рівень знань персоналу, але й зміну їх поведінки, зниження кількості інцидентів та підвищення здатності до своєчасного розпізнавання загроз.

Суттєву роль відіграє вибір інструментів реалізації стратегії. До них належать навчальні програми, інтерактивні тренінги, симуляції соціоінженерних атак, інформаційні кампанії та регулярне тестування знань. Особливу ефективність демонструють методи, що поєднують теоретичне навчання з практичними вправами, оскільки вони дозволяють закріпити отримані знання у реальних умовах [28, с. 76].

Важливим елементом стратегії є формування культури інформаційної безпеки, яка визначає загальне ставлення персоналу до питань захисту інформації. Така культура базується на усвідомленні відповідальності кожного працівника, підтримці з боку керівництва та створенні умов для відкритого обговорення інцидентів. У цьому контексті стратегія підвищення обізнаності виступає не лише інструментом навчання, але й засобом трансформації організаційної поведінки.

З метою наочного відображення структури стратегії доцільно представити її у вигляді узагальненої моделі (рис. 2.3).

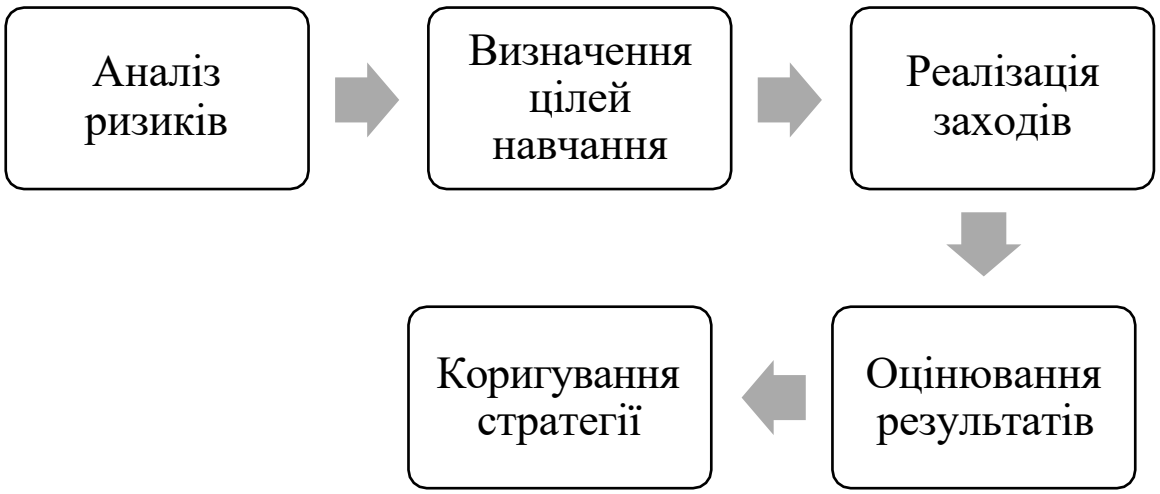

Рис. 2.3. Структура стратегії підвищення обізнаності персоналу

Представлена модель демонструє циклічний характер стратегії, у межах якого результати оцінювання використовуються для її постійного вдосконалення. Це забезпечує адаптацію до нових загроз та змін у поведінці персоналу.

Таким чином, аналіз підходів до формування стратегії підвищення рівня обізнаності персоналу свідчить про необхідність комплексного та системного підходу, який поєднує освітні, поведінкові та управлінські аспекти. Ефективна стратегія повинна бути інтегрована у загальну систему інформаційної безпеки, враховувати специфіку організації та забезпечувати безперервний розвиток компетентностей персоналу. Саме такий підхід створює передумови для зниження вразливості до соціоінженерних загроз та підвищення загального рівня захищеності організації.

2.4. Дослідження технічних та організаційних заходів мінімізації соціоінженерних ризиків

Забезпечення належного рівня захисту від соціоінженерних загроз потребує комплексного поєднання технічних та організаційних заходів, спрямованих на зниження ймовірності реалізації атак і мінімізацію їх потенційних наслідків. Специфіка соціальної інженерії, яка полягає у впливі

на поведінку персоналу, зумовлює необхідність синергії між технологічними інструментами та управлінськими механізмами, що регулюють діяльність працівників.

Технічні заходи відіграють важливу роль у створенні додаткових бар'єрів, які ускладнюють реалізацію соціоінженерних атак навіть у випадку помилкових дій користувачів. Водночас вони не можуть повністю усунути ризики, оскільки основним об'єктом впливу залишається людина. Саме тому їх ефективність значною мірою залежить від узгодженості з організаційними процедурами [34, с. 85].

Серед технічних заходів особливе значення має впровадження багатофакторної автентифікації, яка дозволяє знизити ризик несанкціонованого доступу у випадку компрометації облікових даних. Використання додаткових факторів підтвердження, таких як одноразові коди або біометричні параметри, суттєво ускладнює реалізацію атак, що базуються на отриманні паролів шляхом фішингу або інших методів маніпуляції.

Не менш важливим є застосування систем фільтрації електронної пошти та вебтрафіку, які дозволяють виявляти та блокувати підозрілі повідомлення, шкідливі вкладення та фішингові посилання. Сучасні рішення використовують алгоритми аналізу контенту, поведінкові моделі та бази відомих загроз, що забезпечує підвищення точності виявлення потенційно небезпечних елементів.

Окрему роль відіграють системи моніторингу поведінки користувачів, які дозволяють виявляти аномалії у діях персоналу. Такі системи аналізують типові сценарії роботи користувачів і фіксують відхилення, що можуть свідчити про компрометацію облікового запису або реалізацію соціоінженерної атаки. Наприклад, нетиповий час входу в систему або незвичайна активність щодо доступу до інформаційних ресурсів можуть бути сигналами потенційної загрози [47, с. 83].

Крім того, важливим технічним заходом є обмеження прав доступу відповідно до принципу мінімальних привілеїв. Це означає, що кожен працівник має доступ лише до тих ресурсів, які необхідні для виконання його

функціональних обов’язків. Такий підхід дозволяє локалізувати наслідки потенційної атаки та запобігти поширенню загрози в межах організації.

Водночас технічні заходи не можуть забезпечити повний захист без належного організаційного супроводу. Організаційні заходи спрямовані на регулювання поведінки персоналу, формування чітких процедур та створення умов для безпечної взаємодії з інформаційними ресурсами.

Одним із ключових організаційних заходів є розробка та впровадження політик інформаційної безпеки, які визначають правила поводження з інформацією, порядок доступу до ресурсів та вимоги до обробки даних. Важливо, щоб такі політики були не лише формалізованими, але й зрозумілими для працівників, а також інтегрованими у повсякденну діяльність [30, с. 74].

Значну роль відіграє впровадження процедур перевірки критичних дій, зокрема фінансових операцій або доступу до конфіденційної інформації. Наприклад, підтвердження запитів через альтернативні канали комунікації або застосування принципу «подвійного контролю» дозволяє знизити ризик виконання небезпечних дій під впливом соціальної інженерії.

Не менш важливим є регулярне навчання персоналу, яке забезпечує формування навичок розпізнавання соціоінженерних атак та правильного реагування на них. Практичні тренування, моделювання атак та аналіз типових сценаріїв дозволяють підвищити рівень готовності працівників до протидії загрозам.

Особливу увагу слід приділяти формуванню культури інформаційної безпеки, яка визначає ставлення персоналу до питань захисту інформації. У цьому контексті важливим є створення середовища, у якому працівники не бояться повідомляти про підозрілі ситуації або власні помилки, що сприяє своєчасному виявленню інцидентів [24, с. 44].

З метою узагальнення технічних та організаційних заходів доцільно представити їх у табл. 2.5.

Таблиця 2.5

Технічні та організаційні заходи мінімізації соціоінженерних ризиків

Тип заходу	Захід	Суть	Очікуваний ефект
Технічний	Багатофакторна автентифікація	Додаткове підтвердження доступу	Зниження ризику компрометації
	Фільтрація пошти	Виявлення фішингу	Блокування загроз
	Моніторинг поведінки	Аналіз активності користувачів	Виявлення аномалій
	Контроль доступу	Обмеження прав	Локалізація ризиків
Організаційний	Політики безпеки	Регламентація дій	Підвищення дисципліни
	Процедури перевірки	Контроль критичних операцій	Зниження помилок
	Навчання персоналу	Підвищення обізнаності	Формування навичок
	Культура безпеки	Формування відповідальності	Стійкість до загроз

Слід підкреслити, що ефективність зазначених заходів досягається лише за умови їх комплексного застосування. Ізольоване впровадження окремих рішень не забезпечує належного рівня захисту, оскільки соціоінженерні атаки можуть адаптуватися до існуючих обмежень. Саме тому важливим є створення інтегрованої системи, у межах якої технічні та організаційні заходи взаємодіють між собою [16, с. 74].

Висновки до розділу 2

У розділі досліджено методичні підходи до організації системи протидії соціоінженерним загрозам в сучасних організаціях. Проведений аналіз дозволив визначити основні принципи побудови комплексної моделі захисту, яка передбачає поєднання технічних, організаційних та освітніх заходів для забезпечення стійкості до соціоінженерних атак.

В ході дослідження встановлено, що ефективна система протидії соціальній інженерії повинна базуватися на принципах комплексності, безперервності, адаптивності та ризик-орієнтованого підходу. З’ясовано, що

забезпечення належного рівня захисту можливе лише за умови інтеграції політик інформаційної безпеки, процедур контролю доступу, механізмів управління ризиками та систематичного навчання персоналу.

У межах дослідження проведено систематизацію підходів до ідентифікації та оцінювання соціоінженерних ризиків. А також встановлено, що процес оцінювання має враховувати як технічні характеристики інформаційного середовища, так і поведінкові особливості працівників, рівень їх обізнаності та характер організаційних процесів, та підтверджено, що своєчасна ідентифікація потенційних вразливостей дозволяє зменшити ймовірність успішної реалізації соціоінженерних сценаріїв.

Окрему увагу приділено дослідженню підходів до формування стратегії підвищення рівня обізнаності персоналу. Встановлено, що навчання працівників є одним із найбільш ефективних інструментів протидії соціоінженерним атакам, оскільки дозволяє формувати навички розпізнавання загроз, критичного оцінювання інформації та безпечної поведінки в цифровому середовищі. Доведено доцільність використання регулярних тренінгів, тестувань, симуляцій фішингових атак та інших практикоорієнтованих методів навчання.

Таким чином, результати другого розділу свідчать про необхідність впровадження комплексного підходу до протидії соціоінженерним загрозам, який враховує як технологічні, так і людські фактори. Сформовані методичні положення можуть бути використані як основа для практичного вдосконалення системи захисту організації.

Отже, дослідження технічних та організаційних заходів свідчить про необхідність їх інтегрованого застосування у межах єдиної системи інформаційної безпеки. Такий підхід дозволяє не лише зменшити ймовірність реалізації соціоінженерних атак, але й мінімізувати їх наслідки, забезпечуючи належний рівень захисту інформаційних ресурсів організації.

РОЗДІЛ 3 ПРАКТИЧНА РЕАЛІЗАЦІЯ ЗАХОДІВ ПРОТИДІЇ ТА ОЦІНЮВАННЯ ЇХ ЕФЕКТИВНОСТІ

3.1. Аналіз поточного стану захищеності організації від соціоінженерних атак

Практичне дослідження поточного стану захищеності організації від соціоінженерних атак доцільно здійснювати на прикладі Інституту інформаційних технологій та систем Національної академії наук України. Інститут є державною науковою установою, що належить до сфери управління Національної академії наук України, розташований у місті Києві та здійснює діяльність у сфері інформаційних технологій, технічних, математичних, природничих наук, а також напрямів, пов’язаних із національною безпекою та охороною здоров’я. За даними відкритих державних і академічних ресурсів, установа заснована у 1997 році, має державну форму власності, а її діяльність поєднує науково-дослідний, освітній та інформаційно-технологічний напрями.

Специфіка діяльності Інституту безпосередньо пов’язана з використанням інформаційно-комунікаційних технологій, електронних сервісів, наукових баз даних, службового листування, цифрових ресурсів і результатів наукових досліджень. Відкриті джерела вказують, що серед напрямів роботи установи є розроблення інтелектуальних комп’ютерних технологій і систем, інтелектуалізація інформаційних технологій, створення системних інформаційних технологій, розроблення комп’ютерних технологій навчання, а також підготовка кадрів через аспірантуру та докторантуру. Такий профіль діяльності формує підвищені вимоги до захисту інформаційного середовища, оскільки об’єктами потенційного впливу можуть бути не лише технічні ресурси, а й працівники, науковці, адміністративний персонал, здобувачі освіти та зовнішні партнери [2, с. 74].

З позиції дослідження соціоінженерних ризиків Інститут можна

розглядати як організацію з розгалуженою системою інформаційної взаємодії. Установі притаманні наукові, освітні, адміністративні та комунікаційні процеси, кожен із яких передбачає обмін інформацією між працівниками, структурними підрозділами, зовнішніми організаціями, державними установами, науковими партнерами та здобувачами освіти. Наявність офіційних контактних каналів, зокрема електронної пошти, телефону та вебсайту, підтверджує активне використання відкритих комунікаційних засобів, які, з одного боку, забезпечують доступність установи, а з іншого — можуть бути використані зловмисниками для підготовки соціоінженерних сценаріїв.

Поточний стан захищеності Інституту від соціоінженерних атак доцільно оцінювати за трьома основними складовими: організаційною, технічною та поведінковою. Організаційна складова охоплює наявність управлінських процедур, регламентів інформаційної безпеки, правил доступу до інформації та порядку реагування на підозрілі ситуації. Технічна складова пов’язана з використанням засобів захисту інформаційних систем, контролю доступу, антивірусного захисту, фільтрації електронної пошти та автентифікації користувачів. Поведінкова складова відображає рівень обізнаності персоналу, здатність працівників розпізнавати маніпулятивні повідомлення, перевіряти достовірність запитів і дотримуватися правил безпечної роботи з інформацією [33, с 95].

З огляду на відкритий характер наукової діяльності установи одним із найбільш імовірних каналів реалізації соціоінженерних атак є електронна пошта. Через електронне листування можуть надходити фішингові повідомлення, підроблені запити від імені адміністрації, партнерських організацій, наукових журналів, конференцій, державних установ або технічної підтримки. Особливу небезпеку становлять листи, що імітують службову комунікацію та містять вкладення або посилання на зовнішні ресурси. Для наукової установи такий ризик є особливо актуальним, оскільки працівники регулярно взаємодіють із зовнішнім академічним середовищем,

отримують запрошення до участі в конференціях, рецензуваннях, грантових конкурсах, публікаційних процесах і наукових проєктах. Другим важливим каналом соціоінженерного впливу є телефонна комунікація. Оскільки офіційні контактні дані установи є відкритими, зловмисник теоретично може використовувати їх для встановлення першого контакту, уточнення інформації про працівників, структуру підрозділів або внутрішні процеси. У межах вішингових атак зловмисник може представлятися працівником державної установи, технічної служби, партнерської організації або представником адміністрації. Основна небезпека таких атак полягає в тому, що голосова комунікація дозволяє створити ефект терміновості, авторитетності та довіри [59, с. 87].

Окрему групу ризиків становлять атаки, пов’язані з використанням відкритої інформації про діяльність Інституту. На офіційних і державних ресурсах наявні відомості про керівництво, адресу, напрями діяльності, контакти та науковий профіль установи. Такі дані є необхідними для публічної діяльності наукової організації, однак у контексті соціальної інженерії вони можуть бути використані для підготовки персоналізованих атак. Наприклад, зловмисник може сформувати правдоподібне повідомлення, посилаючись на реальний напрям досліджень, прізвище посадової особи, назву установи або актуальний науковий проєкт. Це підвищує рівень довіри до повідомлення та знижує ймовірність його критичного аналізу з боку отримувача.

З урахуванням профілю Інституту особливого значення набуває захист результатів наукової діяльності, службової документації, персональних даних працівників і здобувачів освіти, а також інформації, пов’язаної з науково-технічними проєктами. Наявність у відкритих джерелах відомостей про наукові напрями, зокрема дослідження у сфері інформаційних технологій, технічних наук, національної безпеки та медичних інформаційних систем, свідчить про потенційну цінність інформаційних активів установи. Отже, соціоінженерні атаки можуть бути спрямовані не лише на отримання облікових даних, але й на доступ до дослідницьких матеріалів, службового

листування, проєктної документації або внутрішніх організаційних процесів [14, с. 83]. Для узагальнення потенційних соціоінженерних ризиків Інституту доцільно подати їх у вигляді табл. 3.1.

Таблиця 3.1

Потенційні соціоінженерні ризики для Інституту інформаційних технологій та систем НАН України

Напрям ризику	**Можливий сценарій атаки**	**Ймовірні наслідки**	**Рівень ризику**
Електронна пошта	Надсилання фішингового листа від імені партнера, конференції або адміністрації	Компрометація облікових даних, відкриття шкідливого вкладення	Високий
Телефонна комунікація	Дзвінок від імені технічної служби або державної установи	Розкриття службової інформації, передача контактних даних	Середній
Відкриті джерела	Використання публічної інформації про установу для персоналізації атаки	Підвищення правдоподібності соціоінженерного сценарію	Високий
Наукова діяльність	Підроблені запити щодо участі в конференціях, грантах або публікаціях	Витік наукових матеріалів або службового листування	Високий
Адміністративні процеси	Імітація службового запиту від керівництва або підрозділу	Виконання несанкціонованих дій працівником	Середній
Робота з персональними даними	Запит на уточнення даних працівників або здобувачів освіти	Порушення конфіденційності персональної інформації	Високий

Аналіз наведених ризиків свідчить, що найбільш уразливими напрямами є електронна комунікація, взаємодія із зовнішніми організаціями та використання відкритої інформації про установу. Це пояснюється тим, що наукова організація за своєю природою має бути відкритою до співпраці, комунікації та обміну інформацією. Водночас саме ця відкритість створює додаткові передумови для реалізації соціоінженерних атак.

Організаційна захищеність установи значною мірою залежить від наявності внутрішніх процедур перевірки запитів, правил роботи з електронною поштою, регламентів доступу до інформаційних ресурсів і

порядку повідомлення про підозрілі інциденти. Якщо такі процедури є формальними або недостатньо відомими працівникам, ризик успішної атаки зростає. Особливо це стосується ситуацій, коли працівник отримує терміновий запит, що нібито надходить від керівництва, технічної служби або зовнішнього партнера.

Технічний рівень захищеності може включати використання антивірусного програмного забезпечення, паролів, обмеження доступу до окремих ресурсів, резервне копіювання та базові засоби захисту корпоративної пошти. Однак у випадку соціальної інженерії технічні інструменти мають допоміжний характер, оскільки навіть наявність фільтрів і засобів автентифікації не гарантує повної безпеки, якщо працівник самостійно передає дані, відкриває шкідливий файл або переходить за фішинговим посиланням. Саме тому ключовим елементом захисту залишається поведінкова стійкість персоналу [58, с.74].

Поведінковий компонент захищеності Інституту доцільно оцінювати через рівень обізнаності працівників щодо типових ознак соціоінженерних атак. До таких ознак належать терміновість запиту, нетипова адреса відправника, прохання надати пароль або іншу конфіденційну інформацію, вкладення незрозумілого походження, граматичні помилки, заклики до негайної дії або посилання на зовнішній ресурс. Якщо працівники не мають достатнього практичного досвіду розпізнавання таких ознак, імовірність реалізації атаки зростає навіть за наявності базових технічних засобів захисту.

У межах аналізу доцільно виокремити сильні та слабкі сторони поточного стану захищеності установи. Сильними сторонами є інформаційно-технологічний профіль Інституту, наявність фахового середовища, орієнтованого на роботу з цифровими технологіями, а також належність до системи Національної академії наук України, що передбачає певний рівень організаційної регламентації. Водночас потенційними слабкими сторонами можуть бути відкритість контактної інформації, активна зовнішня комунікація, участь у наукових і освітніх процесах, а також можливість використання публічних даних для персоналізації атак.

Таблиця 3.2

Узагальнена оцінка поточного стану захищеності Інституту інформаційних технологій та систем НАН України від соціоінженерних атак

Компонент захищеності	**Поточна характеристика**	**Рівень вразливості**
Організаційний	Наявність управлінської структури та формалізованої діяльності установи	Середній
Технічний	Використання інформаційно-комунікаційних технологій у науковій та адміністративній діяльності	Середній
Комунікаційний	Активна взаємодія із зовнішніми установами, партнерами та науковою спільнотою	Високий
Поведінковий	Залежність рівня захисту від уважності та обізнаності персоналу	Високий
Інформаційний	Наявність відкритих даних про установу, напрями діяльності та контакти	Середній

Для наочного відображення логіки формування соціоінженерного ризику в умовах діяльності Інституту можна використати таку схему.

З метою наочного відображення результатів аналізу доцільно використовувати узагальнену модель оцінювання (рис. 3.1).

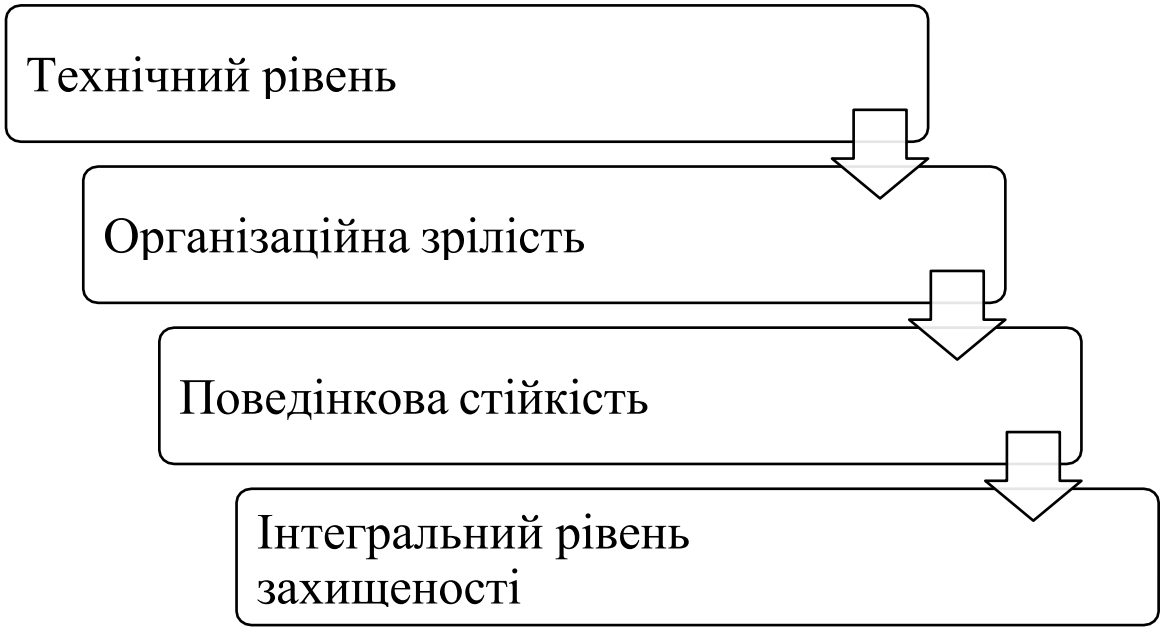

Рис. 3.1. Модель оцінювання поточного стану захищеності.

Отже, поточний стан захищеності Інституту інформаційних технологій та систем НАН України від соціоінженерних атак можна оцінити як такий, що має достатні передумови для побудови ефективної системи протидії, однак потребує посилення саме поведінкового та організаційно-комунікаційного компонентів. Найбільш суттєві ризики пов’язані з електронною поштою, зовнішніми контактами, відкритістю наукової діяльності та можливістю використання публічної інформації для персоналізованих атак [55, с. 98].

Таким чином, аналіз показує, що для підвищення рівня захищеності установи необхідно зосередити увагу не лише на технічних засобах захисту, а й на формуванні сталої культури інформаційної безпеки, регулярному навчанні персоналу, впровадженні процедур перевірки підозрілих запитів і створенні зрозумілого механізму повідомлення про потенційні соціоінженерні інциденти. Саме ці напрями мають стати основою для подальшої розробки рекомендацій щодо вдосконалення системи протидії соціоінженерним загрозам в установі.

3.2. Розробка рекомендацій щодо вдосконалення системи протидії соціоінженерним загрозам

Результати проведеного аналізу поточного стану захищеності Інституту інформаційних технологій та систем НАН України свідчать про наявність низки факторів, які можуть сприяти реалізації соціоінженерних атак. Основними серед них є активна зовнішня комунікація, використання відкритих інформаційних ресурсів, людський фактор, а також недостатня формалізація окремих процедур реагування на підозрілі ситуації. У зв’язку з цим виникає необхідність розроблення комплексу рекомендацій, спрямованих на підвищення рівня стійкості установи до соціоінженерних загроз [4, с. 90].

Формування таких рекомендацій повинно базуватися на принципі комплексності, відповідно до якого захист інформаційного середовища

забезпечується шляхом поєднання організаційних, технічних та поведінкових заходів. Окреме застосування лише технічних рішень або виключно навчальних заходів не забезпечує належного рівня ефективності, оскільки соціальна інженерія адаптується до існуючих умов та використовує найуразливіші елементи системи.

Одним із ключових напрямів удосконалення системи протидії є посилення організаційного компоненту інформаційної безпеки. Насамперед доцільним є впровадження чітко регламентованих процедур перевірки критичних запитів, які надходять через електронну пошту, телефонний зв'язок або інші канали комунікації. Особливо це стосується запитів, пов'язаних із наданням доступу до інформаційних ресурсів, передачею службової інформації, фінансовими операціями або зміною облікових даних.

Важливим кроком має стати розроблення внутрішнього регламенту реагування на соціоінженерні інциденти. Такий документ повинен визначати порядок дій працівників у разі отримання підозрілих повідомлень, виявлення фішингових листів або спроб психологічного впливу. Наявність чітких інструкцій дозволить зменшити рівень невизначеності та забезпечить більш оперативне реагування на потенційні загрози [4, с. 98].

Окремого значення набуває створення системи внутрішнього повідомлення про інциденти інформаційної безпеки. Працівники повинні мати зрозумілий механізм передачі інформації про підозрілі ситуації без ризику негативних наслідків або покарання за помилкове повідомлення. Такий підхід сприятиме формуванню відкритої культури безпеки та забезпечить своєчасне виявлення потенційних загроз.

Водночас ключовим напрямом удосконалення залишається підвищення рівня обізнаності персоналу. Проведений аналіз показав, що саме людський фактор є найбільш уразливим елементом системи безпеки. У зв'язку з цим доцільно впровадити систему регулярного навчання працівників з питань протидії соціоінженерним атакам.

Навчальні заходи повинні мати не лише теоретичний, але й практичний

характер. Найбільш ефективним є використання моделювання реальних соціоінженерних сценаріїв, зокрема фішингових розсилок, телефонних атак або ситуацій психологічного тиску. Такий підхід дозволяє працівникам не лише отримувати інформацію, але й формувати навички розпізнавання загроз у реальних умовах.

Особливу увагу необхідно приділяти категоріям працівників, які мають доступ до критичних інформаційних ресурсів або здійснюють активну зовнішню комунікацію. До таких категорій належать адміністративний персонал, працівники бухгалтерії, керівний склад, відповідальні за інформаційні системи, а також особи, які взаємодіють із зовнішніми науковими організаціями та партнерами. Саме вони найчастіше стають об’єктами цільових соціоінженерних атак [20, с. 88].

Паралельно з організаційними та навчальними заходами необхідно вдосконалити технічний компонент системи захисту. Насамперед доцільним є посилення механізмів захисту електронної пошти, оскільки саме цей канал є найбільш поширеним серед соціоінженерних атак. Рекомендується впровадження сучасних систем фільтрації фішингових повідомлень, аналізу вкладень та перевірки доменів відправників.

Важливим технічним заходом є також розширення використання багатофакторної автентифікації для доступу до службових ресурсів. Навіть у випадку компрометації паролів це дозволить суттєво знизити ризик несанкціонованого доступу до інформаційних систем.

Окрему увагу слід приділити контролю доступу до внутрішніх ресурсів. Доцільним є застосування принципу мінімальних привілеїв, відповідно до якого кожен працівник отримує лише той рівень доступу, який необхідний для виконання його функціональних обов’язків. Це дозволить мінімізувати наслідки потенційної компрометації облікового запису [60, с. 87].

З метою узагальнення запропонованих рекомендацій доцільно представити їх у структурованому вигляді (табл. 3.3).

Таблиця 3.3

Рекомендації щодо вдосконалення системи протидії соціоінженерним загрозам

Напрям удосконалення	**Рекомендований захід**	**Очікуваний результат**
Організаційний	Розроблення регламентів перевірки запитів	Зниження ймовірності помилкових дій
	Створення механізму повідомлення про інциденти	Оперативне реагування на загрози
Освітній	Регулярне навчання персоналу	Підвищення рівня обізнаності
	Проведення симуляцій фішингових атак	Формування практичних навичок
Технічний	Посилення захисту електронної пошти	Зменшення кількості фішингових інцидентів
	Впровадження багатофакторної автентифікації	Зниження ризику компрометації акаунтів
	Обмеження прав доступу	Локалізація потенційних наслідків атак

Важливим аспектом удосконалення системи захисту є також формування культури інформаційної безпеки в установі. Працівники повинні сприймати безпеку не як формальну вимогу, а як невід’ємний елемент професійної діяльності. Для цього необхідно забезпечити регулярну комунікацію щодо актуальних загроз, інформування про типові сценарії атак та підтримку безпечної поведінки з боку керівництва.

Доцільним є впровадження періодичного оцінювання рівня обізнаності персоналу, яке дозволить визначати ефективність навчальних заходів та своєчасно коригувати стратегію підготовки працівників. Таке оцінювання може здійснюватися шляхом тестування, анкетування або аналізу результатів моделювання соціоінженерних атак [17, с. 87].

Таким чином, розроблені рекомендації спрямовані на формування комплексної системи протидії соціоінженерним загрозам в Інституті інформаційних технологій та систем НАН України. Їх реалізація дозволить підвищити рівень захищеності інформаційного середовища, знизити вразливість персоналу до маніпулятивного впливу та забезпечити більш ефективне реагування на потенційні інциденти інформаційної безпеки.

3.3. Оцінювання ефективності запропонованих заходів

Важливим етапом формування системи протидії соціоінженерним загрозам є оцінювання ефективності запропонованих заходів. Саме цей процес дозволяє визначити, наскільки впроваджені організаційні, технічні та поведінкові рішення здатні знижувати рівень ризику, підвищувати стійкість персоналу до маніпулятивного впливу та забезпечувати належний рівень захисту інформаційного середовища організації.

У контексті діяльності Інституту інформаційних технологій та систем НАН України оцінювання ефективності має особливе значення, оскільки специфіка наукової установи передбачає постійну взаємодію з великою кількістю зовнішніх інформаційних джерел, використання електронної комунікації, обмін науковими матеріалами та активну цифрову діяльність персоналу. У таких умовах навіть незначне зниження рівня вразливості персоналу може суттєво впливати на загальний рівень інформаційної безпеки [39, с. 87].

Методично оцінювання ефективності запропонованих заходів доцільно здійснювати на основі порівняльного аналізу стану захищеності до та після впровадження рекомендацій. Такий підхід дозволяє визначити динаміку змін і встановити ступінь впливу окремих заходів на рівень соціоінженерних ризиків.

У межах дослідження ефективність запропонованих рішень доцільно оцінювати за трьома основними напрямами: поведінковим, організаційним та технічним. Поведінковий напрям характеризує рівень обізнаності персоналу та його здатність розпізнавати соціоінженерні загрози. Організаційний напрям відображає рівень формалізації процедур безпеки та готовність установи до реагування на інциденти. Технічний напрям пов’язаний із здатністю інформаційної інфраструктури виявляти та блокувати потенційно небезпечні дії. Одним із ключових показників ефективності є зниження ймовірності успішної реалізації соціоінженерних атак. У практичному

вимірі це може проявлятися у зменшенні кількості випадків переходу працівників за підозрілими посиланнями, передачі конфіденційної інформації або виконання несанкціонованих дій під впливом психологічних маніпуляцій [34, с. 98].

Важливим критерієм оцінювання виступає також рівень готовності персоналу до реагування на підозрілі ситуації. Якщо до впровадження запропонованих заходів працівники переважно не ідентифікували ознаки фішингових повідомлень або соціоінженерних сценаріїв, то після проходження навчання та практичних тренувань очікується підвищення рівня уважності та критичного сприйняття інформації.

Окремого значення набуває оцінювання організаційної ефективності. Упровадження чітких процедур перевірки запитів, механізмів повідомлення про інциденти та регламентів взаємодії дозволяє суттєво скоротити час реагування на потенційні загрози та знизити ризик помилкових дій працівників. Крім того, формалізація процесів безпеки сприяє підвищенню дисципліни та відповідальності персоналу [48, с. 98].

Технічна ефективність запропонованих заходів проявляється у підвищенні рівня контролю за інформаційними потоками та зниженні кількості потенційно небезпечних повідомлень, що потрапляють до користувачів. Використання систем фільтрації електронної пошти, багатофакторної автентифікації та контролю доступу створює додаткові бар’єри для реалізації атак навіть у випадку помилкових дій працівника.

Для узагальнення очікуваних результатів доцільно представити оцінювання ефективності заходів у табл. 3.4.

Аналіз очікуваної ефективності свідчить, що найбільший вплив на зниження соціоінженерних ризиків мають заходи, спрямовані на зміну поведінки персоналу, що пояснюється тим, що соціальна інженерія насамперед орієнтована на людський фактор, а тому саме підвищення рівня обізнаності та розвиток навичок критичного мислення дозволяють найбільш суттєво зменшити вразливість організації.

Таблиця 3.4

Оцінювання ефективності запропонованих заходів

Напрям заходів	**Очікуваний результат**	**Вплив на рівень ризику**
Навчання персоналу	Підвищення рівня обізнаності	Значне зниження
Симуляція фішингових атак	Формування практичних навичок	Значне зниження
Регламентація перевірки запитів	Зменшення помилкових дій	Середнє зниження
Багатофакторна автентифікація	Захист облікових записів	Значне зниження
Фільтрація електронної пошти	Блокування підозрілих повідомлень	Середнє зниження
Контроль доступу	Обмеження наслідків атаки	Помірне зниження
Формування культури безпеки	Стійка безпечна поведінка	Довгострокове зниження

Водночас технічні заходи виконують важливу допоміжну функцію, створюючи додаткові рівні захисту та компенсуючи окремі помилки користувачів. Особливо це стосується багатофакторної автентифікації та систем фільтрації електронної пошти, які здатні значно ускладнити реалізацію фішингових атак [51, с. 45].

Оцінювання ефективності доцільно здійснювати також через аналіз інтегрального рівня захищеності організації. Для цього можна використовувати умовну шкалу оцінювання, яка дозволяє визначити загальний рівень стійкості до соціоінженерних загроз до та після впровадження запропонованих заходів (табл. 3.5).

Таблиця 3.5

Динаміка рівня захищеності організації

Компонент захищеності	**До впровадження заходів**	**Після впровадження заходів**
Обізнаність персоналу	Низький–середній	Середній–високий
Організаційна готовність	Середній	Високий
Технічний захист	Середній	Високий
Реагування на інциденти	Низький	Середній–високий
Загальний рівень захищеності	Середній	Високий

Представлені результати демонструють, що впровадження комплексної

системи протидії соціоінженерним загрозам забезпечує суттєве підвищення рівня інформаційної безпеки установи. При цьому найбільш помітні зміни відбуваються у сфері поведінкової стійкості персоналу та організаційної готовності до реагування на інциденти.

Важливим аспектом оцінювання є також довгостроковий ефект запропонованих заходів. Соціоінженерні загрози характеризуються високим рівнем адаптивності, тому навіть ефективна система захисту потребує постійного оновлення та вдосконалення. У зв’язку з цим оцінювання ефективності повинно здійснюватися не одноразово, а на регулярній основі, із врахуванням змін у середовищі загроз та результатів практичного функціонування системи безпеки.

Доцільним є проведення періодичних внутрішніх аудитів, тестувань персоналу та симуляцій соціоінженерних атак, результати яких можуть використовуватися для коригування навчальних програм, оновлення політик безпеки та вдосконалення технічних механізмів захисту [58, с.45].

Висновки до розділу 3

У третьому розділі здійснено практичне дослідження стану захищеності організації від соціоінженерних загроз та розроблено рекомендації щодо вдосконалення системи протидії таким атакам. Проведений аналіз дозволив оцінити поточний рівень інформаційної безпеки, визначити найбільш суттєві ризики та виявити напрями підвищення ефективності існуючих заходів захисту.

У результаті дослідження встановлено, що основними факторами вразливості залишаються недостатній рівень обізнаності працівників щодо сучасних соціоінженерних методів, недостатня увага до процедур перевірки інформації, а також вплив психологічних чинників під час прийняття рішень. З’ясовано, що навіть за наявності технічних засобів захисту людський фактор продовжує залишатися одним із ключових джерел ризику для інформаційної

безпеки організації.

На основі отриманих результатів сформовано комплекс практичних рекомендацій щодо вдосконалення системи протидії соціоінженерним загрозам. Запропоновані заходи передбачають регулярне навчання персоналу, впровадження програм підвищення обізнаності, проведення контрольних тестувань і симуляцій соціоінженерних атак, удосконалення внутрішніх політик інформаційної безпеки та посилення контролю критичних операцій.

Проведене оцінювання ефективності запропонованих заходів показало, що їх впровадження сприяє зниженню ймовірності успішної реалізації соціоінженерних атак, підвищенню рівня готовності персоналу до виявлення загроз та загальному зміцненню системи інформаційної безпеки організації. Встановлено, що найбільшого результату можна досягти за умови систематичного застосування як організаційних, так і технічних заходів захисту.

Таким чином, практична частина дослідження підтвердила доцільність використання комплексного підходу до протидії соціоінженерним загрозам. Отримані результати можуть бути використані для вдосконалення системи інформаційної безпеки організацій та підвищення їх стійкості до сучасних соціоінженерних атак.

Отже, проведене оцінювання свідчить, що запропоновані рекомендації здатні суттєво підвищити рівень захищеності Інституту інформаційних технологій та систем НАН України від соціоінженерних загроз. Найбільш ефективними є заходи, спрямовані на підвищення рівня обізнаності персоналу, формування культури інформаційної безпеки та впровадження чітких організаційних процедур реагування на потенційні інциденти. Комплексна реалізація запропонованих рішень створює передумови для формування стійкої системи інформаційної безпеки, здатної ефективно протидіяти сучасним соціоінженерним загрозам.

ВИСНОВКИ

У результаті проведеного дослідження було розглянуто теоретичні, методичні та практичні аспекти протидії соціоінженерним загрозам в організації, а також сформовано комплексний підхід до побудови системи захисту від маніпулятивного впливу на персонал. Актуальність обраної тематики обумовлена постійним зростанням кількості соціоінженерних атак, орієнтованих на використання людського фактору як найбільш уразливого елементу інформаційної безпеки.

У межах першого розділу було досліджено сутність соціальної інженерії як чинника дестабілізації корпоративної інформаційної безпеки. Встановлено, що соціоінженерні атаки суттєво відрізняються від класичних технічних загроз, оскільки їх основним об’єктом виступає людина, а ключовим інструментом реалізації – психологічний вплив. Доведено, що ефективність таких атак базується на використанні когнітивних особливостей людського мислення, довіри, емоційних реакцій, соціальних ролей та автоматизованих моделей прийняття рішень. У роботі обґрунтовано міждисциплінарний характер соціальної інженерії, яка поєднує психологічні, соціологічні, управлінські та безпекові аспекти.

У процесі дослідження було систематизовано основні види соціоінженерних атак за векторами та каналами реалізації. Визначено, що найбільш поширеними каналами здійснення атак є електронна пошта, телефонний зв’язок, соціальні мережі, вебресурси та фізичні способи взаємодії. Встановлено, що сучасні соціоінженерні атаки характеризуються високим рівнем адаптивності, персоналізації та скритності, що значно ускладнює їх своєчасне виявлення. Особливу увагу приділено психологічним механізмам маніпуляції та чинникам вразливості персоналу. Доведено, що рівень захищеності організації значною мірою залежить не лише від технічних засобів безпеки, але й від рівня обізнаності працівників, організаційної

культури та ефективності внутрішніх процедур контролю.

У другому розділі було сформовано методичні підходи до організації системи захисту від соціоінженерних загроз. Визначено основні принципи побудови комплексної моделі протидії соціальній інженерії, серед яких системність, багаторівневість, адаптивність, інтегрованість та проактивність. Обґрунтовано необхідність поєднання організаційних, поведінкових і технічних механізмів захисту в межах єдиної системи управління інформаційною безпекою. У роботі було систематизовано підходи до ідентифікації та оцінювання соціоінженерних ризиків. Доведено, що ефективне управління такими ризиками потребує врахування не лише технічних вразливостей, але й поведінкових характеристик персоналу, особливостей внутрішніх комунікацій та специфіки діяльності організації. Запропоновано використовувати комплексний підхід до оцінювання ризиків, який базується на аналізі ймовірності реалізації загроз, рівня вразливості та потенційних наслідків.

Окрему увагу приділено аналізу підходів до формування стратегії підвищення рівня обізнаності персоналу. Установлено, що найбільш ефективними є підходи, орієнтовані не лише на передачу теоретичних знань, але й на формування практичних навичок безпечної поведінки. Доведено доцільність використання навчальних симуляцій, моделювання соціоінженерних атак, тестувань та регулярного інформування працівників щодо актуальних загроз.

У межах другого розділу також досліджено технічні та організаційні заходи мінімізації соціоінженерних ризиків. Встановлено, що ефективний захист потребує впровадження багатофакторної автентифікації, систем фільтрації електронної пошти, контролю доступу, моніторингу поведінки користувачів, а також чітко регламентованих організаційних процедур і системи внутрішнього контролю.

У третьому розділі проведено практичний аналіз поточного стану захищеності Інституту інформаційних технологій та систем НАН України від

соціоінженерних атак. Визначено, що специфіка діяльності наукової установи, пов’язана з активною зовнішньою комунікацією, використанням електронних сервісів та відкритістю інформаційного середовища, створює додаткові передумови для реалізації соціоінженерних загроз. Установлено, що найбільш уразливими напрямами є електронне листування, використання відкритих даних про діяльність установи та недостатній рівень поведінкової стійкості окремих категорій персоналу.

На основі проведеного аналізу було розроблено рекомендації щодо вдосконалення системи протидії соціоінженерним загрозам в Інституті інформаційних технологій та систем НАН України. Запропоновано комплекс заходів, який включає вдосконалення організаційних процедур перевірки запитів, впровадження механізмів повідомлення про інциденти, проведення регулярного навчання персоналу, використання симуляцій фішингових атак, посилення захисту електронної пошти, впровадження багатофакторної автентифікації та обмеження прав доступу до інформаційних ресурсів.

У процесі оцінювання ефективності запропонованих заходів встановлено, що їх комплексна реалізація здатна суттєво підвищити рівень захищеності організації від соціоінженерних загроз. Найбільший ефект очікується від заходів, спрямованих на підвищення рівня обізнаності персоналу та формування культури інформаційної безпеки, оскільки саме людський фактор залишається основною ціллю соціальної інженерії. Водночас технічні механізми забезпечують додатковий рівень контролю та мінімізують наслідки потенційних помилок користувачів.

Отже, проведене дослідження підтвердило, що соціальна інженерія є однією з найбільш складних і небезпечних загроз сучасної інформаційної безпеки, оскільки вона спрямована на експлуатацію поведінкових особливостей людини. Ефективна протидія таким загрозам можлива лише за умови реалізації комплексного підходу, який поєднує технічні засоби захисту, організаційні процедури, управління ризиками та системне підвищення рівня обізнаності персоналу. Практична реалізація запропонованих у роботі заходів

створює передумови для формування стійкої системи інформаційної безпеки, здатної ефективно протидіяти сучасним соціоінженерним загрозам у діяльності наукових та інших організацій.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Бохонько О., Лисенко С. Методи виявлення кібератак соціальної інженерії. Вісник Хмельницького національного університету. Технічні науки. 2023. Том327,№5(2).С.231-236.URL: https://heraldts.khmnu.edu.ua/index. php/heraldts/article/view/534
2. Запорожченко М.М. Базові стратегії попередження загроз соціальної інженерії. Актуальні проблеми кібербезпеки: матеріали всеукр. наук.-практ. конф., м. Київ, 27 жовтня 2022 р. С. 103-106. URL: https://dut.edu.ua/uploads/p_2121_20358827.pdf
3. Запорожченко М.М. Принципи проведення аудиту інформаційної безпеки методами соціальної інженерії. Стратегії кіберстійкості: управління ризиками та безперервність бізнесу: матеріали всеукр. наук.-практ. Інтернет-конф., м. Київ, 24 лютого 2022 р. С. 48-50. URL: https://dut.edu.ua/uploads/p_2121_33783557.pdf
4. Запорожченко М.М. Проблема фішингу для інформаційної безпеки підприємств. Організаційні способи протидії. Інформаційна безпека та 191 інформаційні технології: збірник тез доповідей V всеукр. наук.-практ. конф. молодих учених, студентів і курсантів, м. Львів, 26 листопада 2021 р. С. 40- 42.URL: https://drive.google.com/file/d/1QehUi1v4kGNY5DWcm33Yd_YT7MhNYWI/view?usp=drivesdk
5. Запорожченко М.М. Фішинг як послуга. Стратегії кіберстійкості: управління ризиками та безперервність бізнесу: матеріали всеукр. наук.-практ. конф., м. Київ, 23 лютого 2023 р. С. 47-49. URL: https://duikt.edu.ua/uploads/p_2626_38605375.pdf?file=p_2626_38605375.pdf
6. Запорожченко М.М., Якименко Ю.М. Аудит як метод запобігання атакам соціальної інженерії. The world of modern technologies and

inventions: матеріали IV міжнар. наук.-практ. конф., м. Відень, 10-13 жовтня 2023 р. С.275-279.URL:https://isg-konf.com/wp-content/uploads/2023/10/THEWORLD-OF-MODERN-TECHNOLOGIES-AND-INVENTIONS.pdf

7. Легомінова С.В., Щавінський Ю.В., Рабчун Д.І., Запорожченко М.М., Будзинський О.В. Небезпека інструментів OSINT та способи пом'якшення наслідків їх використання для організації. Кібербезпека: освіта, наука, техніка. 2024. Том 1, № 25. С.294-303. URL: https://csecurity.kubg.edu.ua/index.php/journal/article/view/630/516

8. Легомінова С.В., Якименко Ю.М., Запорожченко М.М. Вплив соціальних мереж на інформаційну безпеку. ITSec: Безпека інформаційних технологій: матеріали XIII міжнар. наук.-техн. конф., м. Львів, 9-11 травня 2024 р. С. 142-143. URL: http://bit.nau.edu.ua/wp-content/uploads/2024/05/2024- ITSec_zbirnyk.pdf
9. Про захист інформації в інформаційно-комунікаційних системах : Закон України від 05.07.1994 р. № 80/94-ВР. Дата оновлення: 28.06.2024. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text

10. Про захист персональних даних : Закон України від 01.06.2010 р. № 2297- VI. Дата оновлення: 31.12.2024. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text 190
11. Про інформацію : Закон України від 02.10.1992 р. № 2657-XII. Дата оновлення: 15.11.2024. URL: https://zakon.rada.gov.ua/laws/show/2657-12/ed20241115#Text

12. Про національну безпеку України : Закон України від 21.06.2018 р. № 2469- VIII. Дата оновлення: 09.08.2024. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text
13. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 р. №2163-VIII. Дата оновлення: 28.06.2024.URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text

14. Якименко Ю.М., Запорожченко М.М. Основи психологічного захисту від соціальної інженерії. Стратегічні комунікації у сфері забезпечення національної безпеки та оборони: проблеми, досвід, перспективи: матеріали IV міжнар. наук.-практ. конф., м. Київ, 27 вересня 2023 р. С. 399- 403. URL: https://sites.google.com/edu.nuou.org.ua/stratcomconf/archive?authuser=0
15. Якименко Ю.М., Рабчун Д.І., Запорожченко М.М. Місце соціальної інженерії в проблемі витоку даних та організаційні аспекти захисту корпоративного середовища від фішингових атак з використанням електронної пошти. Кібербезпека: освіта, наука, техніка. 2021. Том 1, № 13.С.6-15.URL: https://csecurity.kubg.edu.ua/index.php/journal/article/view/278/238
16. Якименко Ю.М., Рабчун Д.І., Мужанова Т.М., Запорожченко М.М., Щавінський Ю.В. Технічний аудит захищеності інформаційно-телекомунікаційних систем підприємства. Кібербезпека: освіта, наука, техніка. 2023. № 4 (20). С. 45-61. URL: https://doi.org/10.28925/2663-4023.2023.20.4561
17. Alahmed Y., Abadla R., Ansari M.J.A. Exploring the potential implications of AI-generated content in social engineering attacks. 2024 International Conference 195 on Multimedia Computing, Networking and Applications (MCNA), Valencia, October 9, 2024. P. 64-73. URL: https://doi.org/10.1109/MCNA63144.2024.10703950
18. Albladi S., Weir G.R.S. A conceptual model to predict social engineering victims. 2019 IEEE 12th International Conference on Global Security, Safety and Sustainability (ICGS3), London, January 16-18, 2019. P. 212-212. URL: https://doi.org/10.1109/ICGS3.2019.8688352
19. Albladi S., Weir G.R.S. Predicting individuals' vulnerability to social engineering in social networks. Cybersecurity. 2020. Vol. 3. 7. URL: https://doi.org/10.1186/s42400-020-00047-5

20. AlbladiS.M.,WeirG.R.S. User characteristics that influence judgment of social engineering attacks in social networks. Human-centric computing andinformation sciences. 2018. Vol. 8. 5. URL: https://doi.org/10.1186/s13673-018-0128-7

21. Almutairi B., Alghamdi A. The role of social engineering in cybersecurity and its impact. Journal of Information Security. 2022. Vol. 13. P. 363-379. URL: https://doi.org/10.4236/jis.2022.134020

22. Alzaabi F.R., Mehmood A. A review of recent advances, challenges, and opportunities in malicious insider threat detection using machine learning methods. IEEE Access. 2024. Vol. 12. P. 30907-30927. URL: https://doi.org/10.1109/ACCESS.2024.3369906

23. Arabia-Obedoza M.R., Rodriguez G., Johnston A., Salahdine F., Kaabouch N. Social engineering attacks a reconnaissance synthesis analysis. 2020 11th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), New York, October 28-31, 2020. P. 843-848. URL: https://doi.org/10.1109/UEMCON51285.2020.9298100

24. Artioli P., Maci A., Magrì A. A comprehensive investigation of clustering algorithms for user and entity behavior analytics. Frontiers in Big Data. 2024. Vol. 7. P. 1-25. URL: https://doi.org/10.3389/fdata.2024.1375818

25. Ayyad W.R., Al-Haija Q.A., Al-Masri H.M. Human factors in cybersecurity. Smart and Agile Cybersecurity for IoT and IIoT Environments. IGI Global Scientific Publishing. 2024. P. 235-256. URL: https://doi.org/10.4018/979-8-3693-3451-5.ch011

26. Benavides-Astudillo E. et al. Analysis of vulnerabilities associated with social engineering attacks based on user behavior. Applied Technologies. 2022. Vol. 1535. P. 351-364. URL: https://doi.org/10.1007/978-3-031-03884-6_26

27. Benavides-Astudillo, E. et al. A framework based on personality traits to identify vulnerabilities to social engineering attacks. Proceedings of third international conference “Applied Technologies”, Quito, October 27-29, 2021. P. 381-394. URL: https://doi.org/10.1007/978-3-031-03884-6_28

28. Burda P., Allodi L., Zannone N. Dissecting social engineering attacks through the lenses of cognition. 2021 IEEE European symposium on security and privacy workshops (EuroS&PW), Vienna, September 6-10, 2021. P. 149-160. URL: https://doi.org/10.1109/eurospw54576.2021.00024
29. Collier H. AI: the future of social engineering! Proceedings of the 23rd European conference on Cyber warfare and security. 2024. Vol. 23, № 1. P. 143- 147. URL: https://doi.org/10.34190/eccws.23.1.2117
30. Ferrucio R. et al. Social network analysis for social engineering footprinting. 8th Iberian conference on information systems and technology, Lisbon, October, 2013. URL: https://doi.org/10.13140/RG.2.1.4842.0964
31. Ficco M., Choraś, M., Kozik R. Simulation platform for cyber-security and vulnerability analysis of critical infrastructures. Journal of computational science. 2017. Vol. 22. P.179-186.URL: https://doi.org/10.1016/j.jocs.2017.03.025
32. Fuertes W. et al. Impact of social engineering attacks: a literature review. Smart Innovation, Systems and Technologies. 2021. Vol. 255. P. 25-35. URL: https://doi.org/10.1007/978-981-16-4884-7_3 194
33. González-Granadillo G., González-Zarzosa S., Diaz R. Security information and event management (SIEM): analysis, trends, and usage in critical infrastructures. Sensors. 2021. Vol. 21, № 14. 4759. URL: https://doi.org/10.3390/s21144759
34. Heartfield R., Loukas G., Gan D. You are probably not the weakest link: towards practical prediction of susceptibility to semantic social engineering attacks. IEEE Access. 2016. № 4. P. 6910-6928. URL: https://doi.org/10.1109/ACCESS.2016.2616285
35. Huseynov F., Ozdenizci Kose B. Using machine learning algorithms to predict individuals' tendency to be victim of social engineering attacks. Information development. 2024. Vol. 40, №2 P.298-318. URL: https://doi.org/10.1177/02666669221116336 188
36. Kapan S., Sora Gunal E. Improved phishing attack detection with machine

learning: a comprehensive evaluation of classifiers and features. Applied Sciences 2023. Vol. 13, № 24. 13269.URL: https://doi.org/10.3390/app132413269

37. Khan S. A. Social engineering. Computer and networks security – final's presentation, Antigonish, November 2023.URL: https://www.researchgate.net/publication/376266487_Social_Engineering

38. Kirichenko L., Radivilova T., Carlsson A. Detecting cyber threats through social network analysis: short survey. 2018. https://doi.org/10.48550/arXiv.1805.06680

39. Mattera M., Chowdhury M.M. Social engineering: the looming threat. 2021 IEEE International Conference on Electro Information Technology (EIT), Mt. Pleasant, July 26, 2021. P. 56-61. URL: https://doi.org/10.1109/EIT51626.2021.9491884

40. Mazzarolo G., Jurcut A.D. Insider threats in cyber security: the enemy within the gates. European cybersecurity journal. 2020. Vol. 6, № 1. P. 57-63. URL: https://doi.org/10.48550/arXiv.1911.09575

41. Olaniyan R., Rakshit S., Vajjhala N.R. Application of user and entity behavioral analytics (UEBA) in the detection of cyber threats and vulnerabilities management. Lecture notes in electrical engineering. 2023. Vol. 984. P. 419-426. URL: https://doi.org/10.1007/978-981-19-8493-8_32

42. Olusanya A., Oluwatosin A., Afolake A., Oluwaseun A. Analysing social engineering attacks and its impact. 2023. URL: https://doi.org/10.13140/RG.2.2.16300.85120

43. Parsons K., McCormac A., Butavicius M., Ferguson L. Human factors and information security: individual, culture and security environment. Command, Control, Communications and Intelligence Division DSTO Defence Science and Technology Organisation. 2010. 46p. URL: https://apps.dtic.mil/sti/pdfs/ADA535944.pdf

44. Perera S., Jin X., Maurushat A., Opoku D.-G.J. Factors affecting reputational damage to organisations due to cyberattacks. Informatics. 2022. Vol. 9, № 1.

28. URL: https://doi.org/10.3390/informatics9010028

45. Prathipa. A. R. Integrating predictive analytics with SIEM for enhanced threat detection. Indian journal of information technology (INDJIT). 2024. Vol. 4, № 1 P.1-11. https://www.researchgate.net/publication/381807317_INTEGRATING_PREDICTIVE_ANALYTICS_WITH_SIEM_FOR_ENHANCED_THREAT_DETECTION
46. Sathvik K., Gupta P., Sitra S.S., Subhashini N., Muthulakshmi S. Social engineering attack detection using machine learning. Advances in distributed computing and machine learning. Lecture notes in networks and systems. 2023. Vol. 660. P. 321-331. URL: https://doi.org/10.1007/978-981-99-1203-2_27
47. Scherb C., Heitz L., Grimberg F., Grieder H., Maure M. A cyber attack simulation for teaching cybersecurity. Proceedings of society 5.0 conference. 2023. Vol. 93. P. 129-140. URL: https://doi.org/10.29007/dkdw
48. Schmitt M., Flechais I. Digital deception: generative artificial intelligence in social engineering and phishing. Artificial intelligence review. 2024. Vol. 57, № 12. 324. URL: https://doi.org/10.1007/s10462-024-10973-2
49. Siddiqi M. A., Pak W., Siddiqi M. A. A study on the psychology of social engineering-based cyberattacks and existing countermeasures. Applied sciences. 2022. Vol. 12, № 12. 6042. URL: https://doi.org/10.3390/app12126042
50. Singh M., Mehtre B.M., Sangeetha S., Govindaraju V. User behaviour based insider threat detection using a hybrid learning approach. Journal of Ambient Intelligence and Humanized Computing. 2023. Vol. 14. P. 4573-4593. URL: https://doi.org/10.1007/s12652-023-04581-1
51. Svitlana Lehominova, Mykhailo Zaporozhchenko, Yurii Shchavinsky, Tetiana Muzhanova, Vitalii Tyshchenko, Matvii Yushchenko. Methodology for determining means of monitoring information security by the method of

expert assessment. International Journal of Computing. 2024. Vol. 23, № 4. P. 681-691. URL: https://computingonline.net/files/journals/1/archieve/IJC_2024_23_4_17.pdf

52. Svitlana Lehominova, Yurii Shchavinsky, Tetiana Muzhanova, Dmytro Rabchun, Mykhailo Zaporozhchenko. Application of Sentiment Analysis to Prevent Cyberattacks on Objects of Critical Information Infrastructure. International Journal of Computing. 2023. Vol. 22, № 4. P. 534-540. URL: https://doi.org/10.47839/ijc.22.4.3362
53. Tetiana Muzhanova, Yuriy Yakymenko, Mykhailo Zaporozhchenko, Vitalii Tyshchenko. International vendor-neutral certification for information security professionals. Cybersecurity: education, science, technique. 2022. Vol. 4,№ 16. P. 129- 141.URL: https://csecurity.kubg.edu.ua/index.php/journal/article/view/369/306
54. Tshimula J.M. et al. Psychological profiling in cybersecurity: a look at LLMs and psycholinguistic features. 2024. URL: https://doi.org/10.48550/arXiv.2406.18783 189
55. Wang Z., Ren Y., Zhu H., Sun L. Threat detection for general social engineering attack using machine learning techniques. 2022. URL: https://doi.org/10.48550/arXiv.2203.07933
56. Yurii Shchavinsky, Tetiana Muzhanova, Yuriy Yakymenko, Mykhailo Zaporozhchenko. Application of artificial intelligence for improving situational training of cybersecurity specialists. ITLT. 2023. Vol. 97, № 5. P. 215-226. URL: https://doi.org/10.33407/itlt.v97i5.5424
57. Zambrano P., Torres J., Tello O.L., Yánez, Á., Velásquez L. On the modeling of cyber-attacks associated with social engineering: a parental control prototype. Journal of information security and applications. 2023. Vol 75, № 4. 103501. URL: https://doi.org/10.1016/j.jisa.2023.103501