НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»
ФАКУЛЬТЕТ КІБЕРБЕЗПЕКИ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Кафедра кібербезпеки

КВАЛІФІКАЦІЙНА РОБОТА

На тему:

«РОЗРОБКА КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ВІД АТАК, ЩО ВИКОРИСТОВУЮТЬ МЕТОДИ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ»

Виконав: здобувач 4 курсу
Рівень бакалавр
Галузь знань 12 «Інформаційні технології»,
спеціальність 125 «Кібербезпека»
Ханов Богдан Валентинович

Керівник: к.т.н., доцент
Бойко Віктор Дмитрович

Рецензент: к. ф.-м. н., доцент
Чепурна Олена Євгенівна

Одеса – 2025

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»
Факультет кібербезпеки та інформаційних технологій
Кафедра **кібербезпеки**
Галузь знань: **12 Інформаційні технології**
Спеціальність: **125 Кібербезпека**
Назва освітньої програми: **Кібербезпека**

ЗАТВЕРДЖУЮ
Завідувач кафедри кібербезпеки
професор С.А. Горбаченко
_____ «____ »_____ 20__
року

З А В Д А Н Н Я
на кваліфікаційну (бакалаврську) роботу
здобувачу Ханову Богдану Валентиновичу

1. Тема роботи: «Розробка комплексної системи захисту від атак, що використовують методи соціальної інженерії»
Керівник роботи: к.т.н, доцент Бойко Віктор Дмитрович
затверджені наказом НУ ОЮА від «18» березня 2025 року № 548-6
2. Строк подання здобувачем роботи «19» травня 2025 року
3. Дата видачі завдання «16» вересня 2024 року

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів бакалаврської роботи	Строк виконання етапів роботи	Примітка
1	Робота з літературою за темою роботи	Вересень-листопад 2024	
2	Робота над першим розділом	Грудень 2024	
3	Робота над другим розділом	Січень 2025	
4	Робота над третім розділом	Лютий 2025	
5	Виправлення зауважень керівника	Березень 2025	
6	Робота над введенням, висновками та оформленням роботи	Квітень 2025	
7	Подання на кафедру	19 травня 2025	
8	Захист роботи	12 червня 2025	

Здобувач _____
(підпис) (прізвище та ініціали)

Керівник роботи _____
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Кваліфікаційна робота на тему «Розробка комплексної системи захисту від атак, що використовують методи соціальної інженерії». Для здобуття першого (бакалаврського) рівня вищої освіти за спеціальністю 125 Кібербезпека. Робота виконана на сторінках загального тексту та сторінках основного тексту.

У сучасному цифровому світі темпи розвитку технологій супроводжуються зростанням кількості кіберзагроз, серед яких особливу небезпеку становлять атаки, що базуються на маніпуляції свідомістю користувачів. Дане дослідження присвячене створенню ефективного інструментарію для протидії таким атакам. Основна ціль роботи - розробити комплексну систему захисту, яка поєднує як технічні, так і організаційні заходи безпеки.

У теоретичній частині дослідження розглянуто класифікацію методів соціальної інженерії, їхні особливості та сценарії застосування. Детально проаналізовано чинні стратегії протидії, а також обґрунтовано необхідність інтеграції профілактичних заходів, включаючи навчання персоналу, моніторинг активності користувачів та впровадження відповідного програмного забезпечення. Запропонована система захисту включає декілька рівнів перевірки й реагування на інциденти, що дозволяє вчасно виявляти спроби маніпуляцій і нейтралізувати їх наслідки.

Розроблені в межах цієї роботи підходи можуть слугувати основою для подальшого впровадження практичних рішень у сфері захисту від соціальної інженерії. Вони стануть у пригоді фахівцям з інформаційної безпеки, аналітикам ризиків та керівникам організацій, які прагнуть сформувати ефективну систему захисту від маніпулятивних атак, що базуються на використанні людського чинника. Оскільки робота має теоретичний характер, вона спрямована на узагальнення знань і формування системного бачення проблеми.

КЛЮЧОВІ СЛОВА: СОЦІАЛЬНА ІНЖЕНЕРІЯ, КІБЕРБЕЗПЕКА, ЗАХИСТ, АТАКИ, НАВЧАННЯ ПЕРСОНАЛУ, МОНІТОРИНГ, РІВНІ ПЕРЕВІРКИ, ІНФОРМАЦІЙНА БЕЗПЕКА, АНАЛІЗ РИЗИКІВ.

ABSTRACT

Qualification Thesis on the Topic: "Development of a Comprehensive Protection System Against Attacks Using Social Engineering Techniques"

Submitted for the attainment of the first (bachelor's) level of higher education in the specialty 125 – Cybersecurity.

The thesis is presented on pages of total text and pages of main content.

In today’s digital era, the rapid advancement of technology is accompanied by a rise in cyber threats, among which attacks based on the manipulation of users’ behavior pose a particular danger. This thesis focuses on developing effective tools to counter such attacks. The main objective of the work is to design a comprehensive protection system that integrates both technical and organizational security measures.

The theoretical part of the study examines the classification of social engineering methods, their key features, and common use cases. Current defense strategies are thoroughly analyzed, and the necessity of implementing preventive measures such as staff education, user activity monitoring, and appropriate software solutions is substantiated.

The approaches developed within this thesis can serve as a foundation for future implementation of practical solutions in the field of social engineering defense. They may be useful for cybersecurity professionals, risk analysts, and organizational leaders seeking to establish an effective strategy against manipulation-based attacks that exploit the human factor. As a theoretical work, the thesis is aimed at consolidating knowledge and forming a comprehensive understanding of the issue.

KEY WORDS: SOCIAL ENGINEERING, CYBERSECURITY, PROTECTION, ATTACKS, STAFF TRAINING, MONITORING, LEVELS OF VERIFICATION, INFORMATION SECURITY, RISK ANALYSIS.

ЗМІСТ

ВСТУП

У світі, де інформація стала однією з найцінніших ресурсів, захист даних перетворився на критично важливе завдання для кожної організації. Зловмисники все частіше використовують не технічні вразливості, а людський фактор, що потребує нового підходу до побудови систем безпеки.

Актуальність теми. У сучасному інформаційному суспільстві, де цифрові технології проникають у всі сфери діяльності людини, питання кібербезпеки набувають особливої ваги. З розвитком технічних засобів захисту інформації зростає і рівень загроз, спрямованих не на технічні вразливості, а на найслабшу ланку будь-якої системи - людину. Одним із найнебезпечніших і водночас найменш контрольованих методів атак є соціальна інженерія - комплекс психологічних прийомів, спрямованих на маніпуляцію користувачами з метою отримання конфіденційної інформації або доступу до інформаційних систем.

На відміну від традиційних технічних атак, методи соціальної інженерії складно виявити й запобігти суто технічними засобами. Зловмисники дедалі частіше застосовують персоналізовані сценарії, фішингові повідомлення, телефонні дзвінки або навіть фізичні взаємодії для отримання бажаної інформації. Попри це, захист від подібних атак часто залишається поза увагою при проєктуванні систем інформаційної безпеки.

Аналіз сучасних підходів до протидії соціальній інженерії показує, що більшість з них є фрагментарними - зосереджені переважно на навчанні персоналу або виявленні фішингових листів. Проте відсутність цілісного, комплексного підходу, що об'єднує технічні та організаційні заходи, створює суттєві прогалини в системах захисту. Таким чином, актуальність теми дипломної роботи зумовлена необхідністю розробки інтегрованої системи, здатної ефективно протистояти атакам, що базуються на соціальній інженерії, шляхом виявлення, запобігання та реагування на подібні загрози.

Мета дослідження полягає у розробці комплексної системи захисту інформаційного середовища від атак, що використовують методи соціальної

інженерії, з урахуванням поєднання технічних, організаційних та освітніх компонентів.

Для досягнення поставленої мети необхідно вирішити наступні завдання:

- провести аналіз існуючих методів та засобів соціальної інженерії;
- дослідити сучасні підходи до виявлення та протидії таким атакам;
- обґрунтувати вимоги до системи комплексного захисту;
- запропонувати архітектуру системи, що забезпечує багаторівневий захист;
- описати механізми впровадження системи в інформаційну інфраструктуру;
- сформувати рекомендації щодо ефективного застосування елементів системи.

Об’єктом дослідження є процес здійснення соціально-інженерних атак як загрози для інформаційної безпеки організацій.

Предметом дослідження є засоби, методи та підходи до побудови комплексної системи захисту від соціальної інженерії в умовах сучасного інформаційного середовища.

Практичне значення роботи полягає у тому, що запропонована модель комплексного захисту може бути основою для створення реальних систем безпеки в організаціях, де є ризик використання соціальної інженерії проти персоналу чи клієнтів. Сформовані рекомендації можуть бути використані спеціалістами з кібербезпеки для проєктування політик безпеки, а також для розробки навчальних програм, орієнтованих на підвищення обізнаності співробітників щодо сучасних загроз. Теоретичні напрацювання цієї роботи можуть стати підґрунтям для подальших досліджень у сфері захисту інформації від нетехнічних методів атак.

1 ТЕОРЕТИЧНІ ОСНОВИ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ

1.1 Поняття та сутність соціальної інженерії

У сфері інформаційної безпеки існує чимало загроз, пов’язаних не лише з технічними вразливостями, а й із людським фактором, який дедалі частіше стає основною ціллю для зловмисників. Технології розвиваються, захисні системи вдосконалюються, однак саме користувач залишається найбільш вразливою ланкою будь-якої інформаційної системи. На цьому й ґрунтується явище соціальної інженерії - комплексу методів, що використовуються для маніпуляції людьми з метою отримання доступу до конфіденційної інформації або ресурсів.

Важливість вивчення цього поняття обумовлена тим, що соціальна інженерія стала одним із найпоширеніших інструментів кіберзлочинців у реальних умовах. Часто саме вона виступає першою фазою складніших атак, дозволяючи обійти технічний захист без використання спеціалізованих засобів злому. Тому для ефективного захисту сучасного інформаційного середовища необхідно глибоко розуміти, що являє собою соціальна інженерія, у чому полягає її сутність та чому вона настільки ефективна.

У цьому підпункті мною буде здійснено вступ до тематики соціальної інженерії, сформульовано її базові риси та розглянуто передумови, що сприяли її появі та поширенню. Це дозволить закласти необхідне теоретичне підґрунтя для подальшого аналізу методів, засобів та стратегій протидії даному виду загроз.

В загальному соціальна інженерія - це наука, що вивчає людську поведінку та фактори, які на неї впливають [1].

Головна мета соціальної інженерії полягає у вивченні чинників, які визначають поведінку людини, а також впливу середовища, у якому вона формується. Це включає аналіз соціальних, культурних та психологічних умов, що сприяють становленню індивідуальної системи цінностей та, відповідно, впливають на прийняття рішень.

У роботі Бойка В.Д. і Василенко М.Д. пояснюється соціальний аспект кібербезпеки «розумного міста», зокрема підкреслюється зростання ризиків розкриття конфіденційної інформації. Автори зазначають, що це може призвести до деанонімізації особи, яка надалі використовується у схемах соціальної інженерії [2, с. 190]. Такий підхід демонструє, що соціальна інженерія - це не лише маніпуляція свідомістю, а й цілеспрямована атака на приватність людини через використання зібраних про неї персональних даних.

На основі таких досліджень можна встановити, які саме стимули або обставини змушують людину діяти певним чином у конкретних ситуаціях.

До прикладу, аналіз соціального оточення, у якому перебував злочинець, може пролити світло на принципи, які сформували його уявлення про світ. Це, у свою чергу, відкриває можливість створити таке соціальне середовище, яке сприятиме формуванню нових систем цінностей - тих, де на перше місце ставляться повага до людського життя, гідності та індивідуальності.

Термін *«соціальна інженерія»*, хоча й походить з контексту соціальних наук, сьогодні широко вживається у сфері інформаційної та кібербезпеки як позначення методів психологічного впливу, що використовуються для отримання несанкціонованого доступу до конфіденційної інформації. Ці методи спираються не на технічні вразливості, а на особливості людської поведінки, що дозволяє атакуючим досягати своїх цілей без прямого втручання в програмне або апаратне забезпечення [3].

Усі способи отримання несанкціонованого доступу умовно можна розділити на два типи: ті, що передбачають використання технічних засобів і вимагають високого рівня технічної підготовки, та ті, що базуються на соціальних і психологічних механізмах - тобто методи соціальної інженерії. У другому випадку зловмисник не зламує систему в технічному розумінні, а обходить її, впливаючи безпосередньо на користувача, змушуючи його розкрити чутливу інформацію.

Одним із психологічних механізмів, які лежать в основі соціальної інженерії, є когнітивні упередження - систематичні помилки в мисленні, які

властиві всім людям. Саме вони створюють умови, за яких користувачі можуть втратити пильність, довіритись неправдивим джерелам або виконати дії, що суперечать політиці безпеки. Таким чином, ефективність захисту інформаційної системи залежить не лише від її технічної надійності, а й від поведінки її користувачів. Навіть добре захищена система може бути скомпрометована внаслідок дій, викликаних помилковими переконаннями або довірою до зловмисника, який може видавати себе, наприклад, за адміністратора, техпідтримку або представника банку.

Попри наявність численних видів кібератак - таких як ін’єкції шкідливого коду, віруси, троянські програми тощо - соціальна інженерія вирізняється тим, що її мішенню є не система як така, а безпосередньо користувач [4, с. 4850]. Маніпулюючи емоціями, страхами або почуттям довіри, зловмисники можуть обійти навіть найсучасніші технічні засоби захисту. Це робить соціальну інженерію особливо небезпечною, адже такі атаки важко виявити заздалегідь, а ще складніше - повністю їм запобігти.

Ключовим інструментом соціальної інженерії є створення ситуацій, у яких користувач добровільно розкриває конфіденційні відомості - такі як паролі, банківські реквізити чи особисті дані. Це може відбуватись через спілкування телефоном, електронною поштою або за допомогою спеціально розроблених вебсайтів чи додатків. Одним із найрозповсюдженіших методів, що базується на таких принципах, є фішинг - техніка, при якій користувача спонукають взаємодіяти з шкідливим посиланням або вкладенням під виглядом легітимного ресурсу [5, с. 11895-11910]. Незважаючи на відносну відомість цього методу, його ефективність не знижується, що свідчить про недостатній рівень обізнаності користувачів щодо подібних загроз.

У ході аналізу поняття та сутності соціальної інженерії було встановлено, що це явище представляє собою сукупність методів психологічного впливу, спрямованих на отримання конфіденційної інформації або здійснення інших дій, вигідних зловмиснику, шляхом маніпулювання поведінкою людини. На відміну від технічних форм злому, соціальна інженерія ґрунтується на використанні

вразливостей у людській психології, таких як довіра, страх, співчуття або неуважність.

Соціальна інженерія має комплексний характер і часто є невід'ємною складовою складних кібератак. Найчастіше об'єктами впливу є як окремі особи, так і працівники організацій, які мають доступ до цінної інформації або систем управління. Застосування соціальної інженерії можливе як у фізичному середовищі (особисте спілкування), так і в цифровому (електронні листи, соціальні мережі, фішингові сайти тощо).

Поняття соціальної інженерії сьогодні тісно пов'язане із питаннями інформаційної безпеки, етичного хакінгу та правового регулювання кіберпростору. Її розуміння дозволяє ефективніше будувати захисні механізми в організаціях, а також здійснювати профілактику подібних загроз на рівні держави.

Таким чином, вивчення сутності соціальної інженерії є надзвичайно важливим у контексті сучасних викликів кібербезпеки, оскільки лише комплексний підхід - поєднання технічного та психологічного аналізу - здатен забезпечити належний рівень захисту від подібних атак.

1.2 Класифікація атак соціальної інженерії

Після з'ясування сутності соціальної інженерії як цілісного явища постає необхідність глибшого аналізу її внутрішньої структури, а саме – класифікації існуючих форм атак. Такий підхід дозволяє не лише систематизувати знання у цій сфері, а й зробити перший крок до формування ефективної стратегії протидії подібним загрозам. Класифікація допомагає виявити логіку, за якою діють зловмисники, зрозуміти основні принципи їхньої поведінки, а також розмежувати різні методи маніпулятивного впливу, які використовуються з метою доступу до цінної інформації або ресурсів.

Соціальна інженерія є динамічним феноменом, що постійно еволюціонує у відповідь на розвиток інформаційних технологій і зміну моделей людської

поведінки у цифровому середовищі. Саме тому класифікація її форм повинна враховувати не лише поточні тенденції, але й історичний контекст, технічний прогрес, а також соціально-культурні особливості середовища, в якому реалізується вплив. Важливо також розуміти, що різні типи атак мають неоднакову мету, ступінь складності та ризики для жертви, що зумовлює необхідність їх ретельного аналізу.

Крім того, структура класифікації дозволяє не лише ідентифікувати окремі види соціальної інженерії, а й з'ясувати принципи, за якими формується сценарій атаки: чи вона передбачає прямий контакт із жертвою, чи діє опосередковано, через цифрові або соціальні канали. Також аналіз класифікаційних підходів надає змогу визначити фактори успішності кожного методу, серед яких – рівень довіри, неуважність, психологічний тиск або використання фальшивих авторитетів.

У цьому підрозділі буде розглянуто найпоширеніші види атак соціальної інженерії, обґрунтовано критерії їх класифікації та охарактеризовано підходи, що використовуються в науковій та практичній площині для аналізу цього явища. Такий огляд дозволить створити цілісне уявлення про різноманіття інструментів соціального впливу, їхній потенційний вплив на безпеку інформаційного середовища, а також передумови їхнього виникнення та розповсюдження в умовах цифрової трансформації суспільства.

Людська психологія є принципом, що лежить в основі більшості атак соціальної інженерії. Згідно з дослідницькою групою Gartner, соціальна інженерія (SE) визначається як порушення систем безпеки за допомогою маніпуляції людьми замість машин [6, с. 264].

Згідно з роботою tripwire щодо безпеки в SE, фішингові атаки є найпоширенішим типом атак із застосуванням методів соціальної інженерії. Зловмисники використовують електронну пошту, соціальні мережі, обмін миттєвими повідомленнями та SMS, щоб обманом змусити жертв надати конфіденційну інформацію або відвідати шкідливу URL-адресу, намагаючись зламати свої системи.

На концептуальному рівні більшість фішингових атак базується на чітко структурованих підходах, спрямованих на досягнення трьох основних цілей, що об’єднують як технічні, так і психологічні аспекти впливу на потенційну жертву.

Першим і найбільш очевидним завданням є здобуття конфіденційної персональної інформації. До таких даних належать ідентифікаційні реквізити (наприклад, повне ім’я, домашня адреса, дата народження), а також особливо чутливі відомості, зокрема номери соціального страхування, банківські рахунки, логіни й паролі. Отримання подібної інформації відкриває перед зловмисниками можливості для викрадення особистості, несанкціонованого доступу до фінансових ресурсів або подальших шахрайських дій [7, с. 138-143].

Другим ключовим елементом є використання спеціально сформованих гіперпосилань, які на перший погляд можуть виглядати цілком безпечними або навіть знайомими. Часто зловмисники застосовують техніки скорочення URL-адрес (через сервіси типу bit.ly), або створюють адреси, що візуально нагадують легітимні веб-сайти (наприклад, підміна літер, використання подібних доменів). Такі посилання ведуть користувача на шкідливі онлайн-ресурси, де розміщено фішингові сторінки, що імітують офіційні портали банків, соціальних мереж або державних установ, спонукаючи людину ввести свої дані.

Третій напрям полягає у використанні психологічного тиску як інструменту маніпуляції. Автори фішингових повідомлень часто навмисне формують повідомлення з емоційним забарвленням - включаючи елементи страху, паніки або відчуття терміновості. Наприклад, це можуть бути фрази на кшталт «Ваш обліковий запис буде заблоковано протягом 24 годин», «Підтвердьте свою особу негайно» або «Ваша банківська картка використана несанкціоновано». Такі тактики створюють умови, за яких жертва діє поспіхом, не перевіряючи достовірність інформації, що й грає на руку зловмисникам [8].

Таким чином, фішингові атаки базуються на поєднанні соціотехнічних методів, які включають у себе як технічні засоби введення в оману, так і психологічні прийоми впливу. Усвідомлення цих трьох складових – крадіжки даних, використання підроблених посилань та створення штучної невідкладності

– є критично важливим для побудови надійної системи цифрової безпеки та підвищення рівня обізнаності користувачів щодо сучасних кіберзагроз.

Одними з найнебезпечніших і водночас найбільш поширених форм фішингових атак є такі підвиди соціальної інженерії, як спеар-фішинг (spear phishing), вішинг (vishing) та смішинг (smishing). Вони відзначаються не лише технічними особливостями реалізації, але й різною глибиною психологічного впливу, формуючи широкий арсенал засобів обману, що адаптуються до сучасних цифрових умов.

Спеар-фішинг представляє собою цілеспрямовану фішингову атаку, орієнтовану на конкретну особу, організацію або навіть окрему посадову особу в межах певної структури. На відміну від класичного фішингу, який має масовий і менш персоналізований характер, спеар-фішинг базується на ретельному зборі інформації про потенційну жертву. Для цього зловмисники використовують відкриті джерела, соціальні мережі, корпоративні веб-сайти та інші інструменти цифрового слідкування, аби сформувати максимально правдоподібний сценарій комунікації [9]. Типовими прикладами є фальшиві листи від імені колеги, керівника або партнера, в яких просять надати доступ до документації, здійснити грошовий переказ або натиснути на посилання, що веде на шкідливий ресурс. Надзвичайна ефективність спеар-фішингу пояснюється не лише глибиною персоналізації, а й високим ступенем довіри, що формується завдяки точному відтворенню стилю спілкування реальної особи.

Вішинг (від англ. voice phishing) – це форма фішингу, яка реалізується через голосовий зв’язок, найчастіше – за допомогою телефонних дзвінків [10, с. 454-466]. Атаки вішингу зазвичай ґрунтуються на використанні маніпулятивних технік, зокрема імітації дзвінків від банківських установ, державних органів або служб безпеки. Зловмисники повідомляють про "підозрілі транзакції", "блокування рахунку" або "ризики шахрайства", пропонуючи жертві терміново надати особисті дані або підтвердити доступ до облікових записів. Особливістю вішингу є використання емоційного тиску: у телефонній розмові важче зберегти критичне мислення, особливо якщо мова йде про фінанси або безпеку [11, с. 515].

Складність протидії цьому виду атаки зумовлюється також високим рівнем достовірності голосу, використанням підроблених номерів (спуфінг), а іноді й залученням реальних записів голосових повідомлень для створення ефекту автентичності.

Смішинг, у свою чергу, базується на розсилці шкідливих текстових повідомлень (SMS), які містять шкідливі або фішингові посилання. Жертва, натискаючи на таке посилання, може бути перенаправлена на підроблений веб-сайт, що імітує сторінку банку, поштової служби чи іншого сервісу, де її попросять ввести конфіденційні дані. У деяких випадках посилання веде до автоматичного завантаження шкідливого програмного забезпечення. Особливу небезпеку смішинг становить для користувачів мобільних пристроїв, де екрани менші, а перевірка легітимності посилань або сертифікатів є менш зручною, ніж на ПК. Крім того, через звичку швидко реагувати на текстові повідомлення, користувачі часто не приділяють належної уваги деталям повідомлення, що підвищує ймовірність успішної атаки [12, с. 667-689].

Усі три форми атак – спеар-фішинг, вішинг та смішинг – є прикладами адаптивної соціальної інженерії, що активно реагує на зміну цифрових середовищ та поведінкових моделей користувачів. Вони демонструють, що ключовим чинником у ланцюгу безпеки залишається людина, і саме людська помилка чи довірливість найчастіше стає слабким місцем у системі захисту. Таким чином, ефективна протидія цим загрозам вимагає не лише технічних рішень, а й розвитку цифрової грамотності, формування критичного мислення та впровадження регулярних навчань із кібербезпеки в межах організацій і суспільства в цілому.

Іншою важливою категорією є пре-текстинг – створення зловмисником вигаданого сценарію чи легенди, наприклад, від імені банківського працівника або співробітника технічної підтримки, щоб викликати довіру у жертви й змусити її надати потрібну інформацію.

Ще одним поширеним методом є бейтинґ, який базується на використанні привабливої "приманки" – від заражених флеш-накопичувачів до рекламних об’яв, що заохочують користувача натиснути на шкідливе посилання [13, с. 7-8].

Окреме місце займає тейлгейтінг – фізичне проникнення до охоронюваних зон шляхом обходу систем контролю доступу, наприклад, через слідування за співробітником без ідентифікаційного пропуску.

Інформаційно-психологічні маніпуляції проявляються також у вигляді квізингу – фальшивих опитувань або конкурсів, під час яких жертва добровільно ділиться особистими даними.

До подібних методів також належить імперсонація – повне перевтілення в іншу особу, найчастіше – в керівника або колегу, що дозволяє зловмиснику створити атмосферу довіри і здійснити маніпулятивний вплив.

Нарешті, в епоху цифрових комунікацій активно використовується метод соціального бомбардування (social bombing), що передбачає інтенсивний психологічний тиск, дезінформацію або послідовне нав’язування певного образу чи поведінкової моделі через соціальні мережі, форуми чи публічні платформи [14, с. 81-87].

У сучасних умовах технологічного розвитку зловмисники активно використовують штучний інтелект і відкриті дані для проведення соціальних атак. Наприклад, великі мовні моделі (ВММ або LLM), такі як ChatGPT або Gemini, – це нейромережі з мільйонами–мільярдами параметрів, навчені на величезних обсягах тексту [15]. Вони здатні генерувати дуже правдоподібні тексти, а останні дослідження показують, що за їх допомогою можна створювати цілком достовірні фішингові повідомлення, імітувати голос чи відео інших людей. Через це новітні «Генеративні AI» інструменти виводять соціальну інженерію на новий рівень: такі системи можуть автоматизувати частину або навіть увесь цикл атаки, генеруючи величезну кількість персоналізованих спам-повідомлень чи дзвінків.

Використання LLM зловмисниками проявляється у вигляді високоякісних підробок. Наприклад, поширеною тактикою є написання чат-ботом надзвичайно

переконливих електронних листів: вони містять актуальну інформацію про працівника, згадують його проєкти, імітують стиль листування керівника або клієнта. Лабораторні дослідження засвідчують, що навіть «із коробки» стандартні моделі ШІ здатні генерувати фішинговий контент дуже високої якості [16, с. 3]. Якщо на підприємстві не впроваджено надійного фільтра пошти та правил автентифікації кореспонденції (SPF/DKIM/DMARC), такі електронні листи можуть легко обдурити людей. Також зловмисники використовують аналогічні моделі для надсилання текстових повідомлень чи дзвінків у вигляді чат-бота, що імітує знайомий або уповноважений голос. Щоб протидіяти цьому, компаніям слід: навчати працівників перевіряти незвичайні запити у кілька каналів (наприклад, перед виконанням наказу про транзакцію обов’язково зателефонувати за відомим номером у бухгалтерію), вимагати офіційного підтвердження (підпис чи платіжні реквізити), а також застосовувати технології аналізу повідомлень (антивірус, антифішингові сканери).

На особистому рівні користувачеві не слід сліпо довіряти несподіваним листам чи повідомленням, навіть якщо текст звучить природно. Варто звертати увагу на невластиві фрази, неточності у відправнику, перевіряти повідомлення «навіть у картинках» (відкриття зображення з фішинговими посиланнями може активувати шкідливий код).

Загалом до будь-яких незвичних запитів потрібно ставитися насторожено: наприклад, якщо банківська підтримка просить надати пароль або підтвердити платіж – завершити розмову і передзвонити на офіційний номер банку, а в корпоративних ситуаціях використовувати попередньо погоджені кодові фрази чи процедури підтвердження особи.

Так само зловмисники широко застосовують цифрову імітацію - підробку голосу й відео (deepfake, голосові атаки). Із розвитком генеративного AI стало реально створювати «практично бездоганні» підробки. Наприклад, за даними ЗМІ, один працівник фінансового відділу переказав $25 млн, повіривши, що виконує розпорядження свого головного фінансового директора по відеодзвінку

[17, с .2]. Також описані випадки, коли шахраї синтезували голос CEO компанії, щоб змусити співробітників виконати нелегальні платіжні операції.

У таких атаках буває важко відрізнити підроблений голос чи обличчя від справжніх через правильну дикцію та вираз обличчя жертви. У зв'язку з цим компаніям рекомендується впроваджувати додаткові протоколи аутентифікації: наприклад, вимагати одночасно письмові підтвердження фінансових транзакцій, налаштувати подвійне погодження платежів різними особами або запровадити внутрішню кодову фразу, яку має назвати співрозмовник при дзвінку. Особливо корисно погоджувати правила безпеки «згори до низу» - коли будь-яка критична дія має бути затверджена не лише усно, а ще й через офіційний документ чи кілька незалежних каналів.

Для звичайних громадян підказкою про фальшивку може стати наприклад відсутність очікуваних візуальних чи звукових нюансів: у відеодзвінку намагаються помітити «пропади голосу», спотворення губ або нехарактерну поведінку камери. Якщо виникають сумніви, можна попросити абонента сказати попередньо узгоджене слово або переконатися в автентичності за допомогою відомого контактного номера.

Класифікація атак соціальної інженерії є ключовим етапом у формуванні системного підходу до розуміння загроз інформаційній безпеці. Проведений аналіз дозволив структурувати основні типи соціоінженерних впливів відповідно до методів їх реалізації, каналів комунікації та психологічних механізмів, які лежать в основі маніпуляцій. Така типологізація не лише сприяє поглибленню знань про сучасні засоби обману, а й дозволяє виявити спільні риси та відмінності між окремими формами атак.

1.3 Аналіз сучасних методів та інструментів соціальної інженерії

У контексті стрімкого розвитку цифрових технологій та зростаючої взаємозалежності в інформаційному просторі, методи та інструменти соціальної інженерії набувають дедалі більшої складності, багатогранності та ефективності.

Традиційні підходи, засновані виключно на маніпуляціях із використанням електронної пошти або телефонного зв’язку, сьогодні поступаються місцем багатоступеневим сценаріям, які інтегрують в собі психологічні прийоми, технічні засоби та глибокий аналіз поведінкових особливостей потенційних жертв. Така еволюція зумовлена не лише зростанням рівня обізнаності користувачів, а й вдосконаленням захисних технологій, що змушує зловмисників шукати нові, витончені форми впливу.

Сучасні інструменти соціальної інженерії не обмежуються окремими каналами комунікації - вони охоплюють увесь спектр цифрового середовища: від електронної пошти до соціальних мереж, месенджерів, мобільних додатків, фішингових веб-сайтів і навіть офлайн-інтеракцій. Вони можуть включати використання ботів, програм-імітацій, генераторів підроблених документів, алгоритмів збору даних з відкритих джерел (OSINT) і технологій соціального профілювання. Крім того, на перший план виходить використання штучного інтелекту та машинного навчання для персоналізації атак, підвищення їх достовірності та масштабування впливу.

У такому контексті особливо важливим є аналіз не лише самих методів, а й інструментів, що слугують технічною основою для реалізації соціоінженерних стратегій. Цей аналіз дозволяє ідентифікувати найактуальніші загрози, зрозуміти логіку дій зловмисників, виявити прогалини в захисних системах і спрогнозувати можливі вектори майбутніх атак. Крім того, він створює основу для розробки ефективних превентивних заходів, орієнтованих не лише на технічну протидію, а й на підвищення рівня обізнаності користувачів, формування культури інформаційної безпеки та впровадження освітніх ініціатив.

У межах цього підрозділу буде розглянуто загальні тенденції, що визначають розвиток методів соціальної інженерії, а також окремі технологічні рішення, які активно використовуються в рамках атак. Такий підхід дозволить сформувати цілісне уявлення про динаміку загроз та надати обґрунтовану основу для подальших практичних рекомендацій у сфері кібербезпеки.

Методи соціальної інженерії - це сукупність цілеспрямованих психологічних, комунікативних і поведінкових прийомів, які використовуються зловмисниками для маніпулятивного впливу на людину з метою отримання доступу до конфіденційної інформації, ресурсів або систем. Ці методи базуються на знаннях людської психології, довіри, емоцій, звичок та соціальних ролей.

На відміну від технічних методів атак, які спрямовані на подолання цифрових захистів за допомогою шкідливого програмного забезпечення або уразливостей у коді, методи соціальної інженерії спрямовані на «людський фактор» - тобто на використання природної схильності людини довіряти, поспішати, уникати конфліктів або підкорятися авторитету.

Одним із базових методів є створення довіри (Rapport Building), що передбачає формування позитивного емоційного контакту між атакуючим і жертвою. Це дозволяє знизити психологічний захист, викликаючи відчуття безпеки. Часто використовується також апеляція до авторитету (Appeal to Authority) - імітація ролі впливової особи (керівника, державного службовця), що викликає підсвідому готовність до підкорення або співпраці.

Інший ефективний підхід - маніпуляція страхом або терміновістю (Fear and Urgency). Зловмисники створюють ситуацію штучної небезпеки або крайньої терміновості (наприклад, блокування рахунку), спонукаючи до необдуманих дій. Поряд із цим активно застосовується використання цікавості (Curiosity Exploitation), коли жертві пропонується щось незвичайне або сенсаційне, що стимулює бажання дізнатися більше, натиснути посилання або відкрити файл.

Не менш важливим є емоційний вплив (Emotional Manipulation) - викликання жалю, співчуття або потреби допомогти, зокрема через вигадані історії хвороб, катастроф чи втрат. Подібну ефективність демонструє метод соціальної валідації (Social Proof) - створення враження, що «всі вже зробили так само», підкріплене уявними коментарями, цифрами або скриншотами. Схожим є метод нормативного впливу (Normative Influence), де відтворюється поведінка більшості або знайомої групи, стимулюючи індивіда діяти аналогічно.

Ще одним поширеним прийомом є використання обману (Deception) - свідоме спотворення фактів, створення вигаданих ситуацій, фальшивих приводів. У зв'язку з цим часто застосовується підробка комунікації (Spoofing/Impersonation) - маскування під реальну особу, установу або сервіс. Це підсилює довіру до повідомлення та мінімізує підозру. Для більшої ефективності атаки зловмисники застосовують соціальне профілювання (Profiling) - глибокий аналіз поведінки, інтересів та звичок жертви, що дозволяє персоналізувати повідомлення [18, с. 7533-7538].

Деякі атаки будуються на постійності впливу (Persistence/Follow-up) - кількаразовому або довготривалому спілкуванні, яке поступово розмиває настороженість користувача. На завершення варто згадати метод раптового подарунка або заохочення (Reciprocity Principle): надання жертві уявної вигоди або бонусу (наприклад, виграшу), що психологічно зобов'язує до взаємної дії.

Сучасні методи соціальної інженерії демонструють складну психологічну природу й високу ефективність, що обумовлює необхідність їх глибокого вивчення для формування надійної системи кіберзахисту на рівні особи, організації та держави.

Інструменти соціальної інженерії - це технологічні, інформаційні або організаційні ресурси, що використовуються для збору інформації, маскування, комунікації з жертвою або реалізації конкретної атаки. Іншими словами - це технічне і ресурсне забезпечення методів соціальної інженерії.

Ці інструменти умовно поділяються на чотири функціональні групи: інформаційні, комунікаційні, технічні та програмні. Інформаційні інструменти призначені для збору первинної інформації про потенційну жертву.

Найбільш поширеними в цій категорії є платформи OSINT (Open Source Intelligence), такі як theHarvester, Maltego, Recon-ng і SpiderFoot. Вони дозволяють виявити електронні адреси, домени, IP-адреси, зв'язки між об'єктами тощо. Крім того, зловмисники активно використовують соціальні мережі - зокрема LinkedIn, Facebook, Instagram - для вивчення публічних профілів, кола спілкування, місця роботи та інтересів жертви. Додаткову

інформацію можна отримати за допомогою пошукових систем і баз даних витоків, таких як people search engines, Pastebin, HaveIBeenPwned, де зберігаються дані про зламані акаунти, паролі та адреси електронної пошти.

До комунікаційних інструментів належать засоби, які забезпечують безпосередній контакт з жертвою. Наприклад, сервіси для масової розсилки електронних листів і SMS, як-от Sendinblue, Twilio або спеціальні скрипти, використовуються для запуску фішингових кампаній. Для підвищення довіри застосовуються платформи підміни номерів (spoofing) - SpoofCard, MyPhoneRobot - які дозволяють змінювати ідентифікатор абонента. Анонімізатори та VPN-сервіси дають змогу приховати справжню IP-адресу атакуючого. Часто зловмисники створюють підроблені облікові записи у соціальних мережах або месенджерах, імітуючи відомі або близькі жертві особи, що сприяє створенню довіри й обману.

У рамках технічних інструментів виділяються генератори фішингових сторінок, зокрема SET (Social Engineering Toolkit) та Gophish, які дозволяють створювати копії веб-інтерфейсів легітимних сервісів - банків, корпоративних порталів, поштових платформ. Додатково використовуються заражені файли або фізичні носії, як-от USB Rubber Ducky чи BadUSB, які запускають шкідливий код при підключенні до пристрою. До цієї групи належать і редактори документів (Word, PDF) із вбудованими макросами, які активуються під час відкриття. Інструменти для створення фальшивих електронних листів та веб-сайтів - email spoofers, fake website builders - дозволяють зловмисникам візуально копіювати легітимні ресурси, вводячи користувача в оману.

Окрему групу становлять програмні засоби, замасковані під легітимні додатки. Серед них - мобільні застосунки, що запитують надмірні або приховані дозволи, використовуючи їх для збору персональної інформації, геолокації або запису даних.

Підсумовуючи вищевикладену інформацію, пропоную таку схему, в якій зазначаю повну класифікацію основних даних, пов’язаних з теорією соціальної інженерії (рисунок 1.1).

Рисунок 1.1 - Теоретичні основи соціальної інженерії

2 МЕТОДОЛОГІЯ ЗАХИСТУ ВІД АТАК СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ

2.1 Організаційні методи захисту

У сучасному цифровому середовищі, де технічні засоби захисту поступово вдосконалюються, зростає значення соціальної інженерії як інструменту обходу інформаційної безпеки. На відміну від прямих хакерських атак, методи соціальної інженерії базуються на впливі на поведінку людини - найвразливішої ланки будь-якої системи. Саме тому технічні заходи, як-от антивіруси, брандмауери чи шифрування, хоча й залишаються важливими, не здатні самостійно гарантувати повний захист від маніпулятивних впливів, спрямованих на співробітників, користувачів або клієнтів організацій.

У такому контексті особливу актуальність набувають організаційні методи захисту, які охоплюють управлінські, адміністративні та освітні заходи, спрямовані на зниження ризику успішного здійснення соціоінженерних атак. Ці методи формують культуру безпеки в організації, розвивають обізнаність персоналу щодо типових загроз і поведінкових сценаріїв, а також створюють нормативно-правові й інституційні умови для належного реагування на інциденти. До таких заходів належать політики інформаційної безпеки, внутрішні регламенти, система навчання й підвищення кваліфікації, контроль доступу, аудит поведінки персоналу, розслідування інцидентів тощо [19, с. 603-618].

У цьому підрозділі буде розглянуто основні напрями організаційного захисту від атак соціальної інженерії, їхнє значення, практичне застосування та ефективність у межах сучасної системи управління інформаційною безпекою. Вивчення цього аспекту є критично важливим для формування цілісного підходу до захисту даних, оскільки дозволяє не лише попередити загрози, але й підвищити рівень відповідальності та стійкості організації перед соціотехнічними ризиками.

Перед описом методології, додаю схему, що допоможе в комплексній оцінці інформації, наданої мною в даному розділі (рисунок 2.1)

Рисунок 2.1 – Методологія захисту від атак соціальної інженерії

Одним із фундаментальних елементів організаційного захисту є формування політики інформаційної безпеки. Вона передбачає розробку нормативних документів, що регламентують поводження з інформацією, порядок доступу до даних, а також поведінку персоналу в цифровому середовищі. Така політика повинна бути не лише юридичною формальністю, а реальним інструментом управління ризиками, що підтримується керівництвом і є обов'язковою для всіх працівників організації.

Важливу роль відіграє організація навчального процесу та підвищення обізнаності персоналу. Регулярні тренінги, семінари, внутрішні лекції та онлайн-курси дозволяють ознайомити працівників із найпоширенішими сценаріями соціоінженерних атак - такими як фішинг, спуфінг, телефонне шахрайство або маніпуляції в соціальних мережах. Ефективними є також симуляції фішингових атак, які дозволяють у контрольованих умовах оцінити рівень обізнаності та пильності працівників, виявити потенційно вразливі ланки й надати персоналізовані рекомендації.

Значну ефективність демонструють механізми розмежування доступу до інформації. Вони ґрунтуються на принципі «мінімально необхідного доступу», коли кожному працівникові надаються лише ті права, які є необхідними для виконання його функцій. Таким чином, навіть у разі успішного впливу на окремого співробітника потенційний збиток обмежується рамками його повноважень. Подібні моделі доступу дозволяють істотно знизити ризики несанкціонованого поширення чутливої інформації.

Крім того, обов’язковими є періодичні аудити інформаційної безпеки, які включають перевірку дотримання політик, аналіз логів, оцінку інцидентів та перевірку поведінкових патернів користувачів. Такі аудити дають змогу не лише оцінити стан захищеності організації, а й вчасно виявити ознаки потенційної атаки [20, с. 145-149].

Одним із ефективних напрямів є впровадження систем фіксації та реагування на інциденти, що включають в себе логування спроб доступу, підозрілих дій, отримання небезпечних листів або повідомлень. Усі інциденти повинні реєструватися, аналізуватися, а також супроводжуватися негайним інформуванням відповідальних осіб. Чітко прописані процедури реагування дозволяють уникнути паніки та забезпечують координовані дії під час реальної загрози.

Не менш важливими є засоби ідентифікації та контролю доступу. До них належать двофакторна аутентифікація, використання службових ID-карток, паролів з високим рівнем складності, а також фізичні засоби контролю входу в

офіси чи серверні кімнати. Надійна система контролю доступу не лише перешкоджає прямому проникненню, а й знижує ймовірність успішного впливу на персонал.

Додатково до цього впроваджуються процедури щодо обмеження використання особистих пристроїв (BYOD). Організації часто формують окрему політику щодо підключення смартфонів, ноутбуків або інших гаджетів до корпоративної мережі, адже це суттєвий ризик витоку або зараження даних. Рекомендується використовувати ізольовані середовища, моніторинг пристроїв та сегментацію мереж.

Нарешті, одним із найменш технічних, але найбільш важливих напрямів є формування культури інформаційної безпеки в колективі. Це означає, що кожен співробітник усвідомлює свою відповідальність за збереження даних, здатен критично мислити у взаємодії з зовнішніми джерелами і несе персональну відповідальність за дотримання правил. Формування такої культури можливе лише за умови системної просвітницької роботи, підтримки з боку керівництва, відкритої комунікації щодо ризиків та заохочення до ініціативної поведінки у сфері кіберзахисту.

Одним з ефективних методів виявлення вразливостей, зокрема пов’язаних із соціальною інженерією, є тестування на проникнення (penetration testing). Горбаченко С.А. та Бойко В.Д. наголошують, що така процедура, зокрема у форматі Red Team, має виконуватися зовнішньою командою, аби не лише виявити технічні слабкі місця, а й підвищити рівень пильності та алертності персоналу [21, с. 23-29]. Подібні тестування моделюють реальні сценарії атак, у тому числі фішингових або спрямованих на психологічний тиск, що дозволяє працівникам на практиці побачити можливі шляхи зловживання довірою. Таким чином, пентест слугує не лише технічним інструментом, а й організаційним та навчальним заходом, який формує критичне мислення та обережність серед співробітників у питаннях інформаційної безпеки.

У сфері інформаційної безпеки організаційні методи відіграють особливу роль, оскільки дозволяють зміцнювати захист не лише за рахунок технічних

рішень, а й через підвищення рівня відповідальності, дисципліни та свідомості серед персоналу. Соціальна інженерія як явище постійно адаптується до змін середовища, стає дедалі витонченішою, гнучкішою, а отже - більш небезпечною. Протистояти їй лише технічними засобами неможливо, адже ціль атак - не комп'ютер чи сервер, а конкретна людина. Саме тому організаційна складова набуває вирішального значення.

Ефективні організаційні заходи не є разовими чи формальними - вони формують динамічну, адаптивну систему управління безпекою, де враховано поведінкові моделі, можливі сценарії ризиків і особливості корпоративного середовища. Комплексність цих методів полягає у поєднанні нормативного регулювання, освітніх ініціатив, контролю та моніторингу, а також у формуванні сталих звичок безпечної поведінки. Організаційні рішення впливають не тільки на окремі випадки взаємодії із загрозами, але й трансформують саму корпоративну культуру, де цінність інформації стає спільно розділеним пріоритетом.

Не менш важливо, що організаційні методи мають значний превентивний потенціал. Їх впровадження знижує ймовірність несанкціонованого доступу ще до того, як атака буде здійснена. Саме така проактивна модель захисту виявляється найбільш ефективною в умовах постійних трансформацій цифрових ризиків. Водночас ці методи є масштабованими, що дає змогу застосовувати їх як у великих корпораціях, так і в малих підприємствах або освітніх установах.

Загалом, організаційні методи захисту є не просто доповненням до технічних заходів, а повноцінною і самостійною основою кіберстійкості. Їх значущість постійно зростає, оскільки лише через поєднання правил, знань, етичної відповідальності та контролю можливо створити безпечне інформаційне середовище, стійке до впливу соціотехнічних загроз.

2.2 Технічні засоби захисту

Актуальність проблеми захисту від атак соціальної інженерії обумовлена тим, що навіть найскладніші інформаційно-технічні системи можуть бути скомпрометовані через одну помилку людини. Незважаючи на те, що сутність соціальної інженерії полягає передусім у впливі на психологічні та поведінкові характеристики жертви, технічні засоби відіграють критичну роль у побудові ефективної системи захисту. Вони дозволяють мінімізувати ризики, вчасно виявляти ознаки атаки, блокувати потенційно небезпечні дії та підтримувати цифрову гігієну користувачів.

Технічні засоби захисту мають широкий спектр реалізації - від фільтрації електронної пошти та мережевого трафіку до багаторівневої аутентифікації, моніторингу активності в реальному часі, аналізу поведінки користувачів та впровадження штучного інтелекту для виявлення аномалій. Багато з них є автоматизованими або напівавтоматизованими, що дозволяє оперативно реагувати на загрози без втручання людини, компенсуючи таким чином її потенційну вразливість до маніпуляцій.

У межах цього підпункту буде розглянуто основні технічні рішення, які використовуються для запобігання атакам соціальної інженерії. Йтиметься як про інфраструктурні засоби (фаєрволи, системи виявлення вторгнень, антивірусне ПЗ), так і про спеціалізовані інструменти - фішинг-фільтри, антиспуфінг-технології, системи валідації відправників тощо. Крім того, буде приділено увагу взаємозв’язку технічних засобів із політиками інформаційної безпеки та їх інтеграції в єдину архітектуру захисту.

Технічні засоби захисту, спрямовані на запобігання або мінімізацію наслідків соціоінженерних впливів, набувають особливої ваги як частина багаторівневої системи інформаційної безпеки.

Одним із базових та водночас найбільш критично важливих технічних інструментів у боротьбі з атаками соціальної інженерії є системи виявлення та блокування підозрілої комунікації. Їх головна мета - фільтрація вхідного

інформаційного потоку, зокрема електронної пошти, з метою недопущення доставки повідомлень, які можуть містити шкідливий вміст або бути використані зловмисниками для маніпуляції користувачем. Сучасні поштові сервіси, зокрема Gmail, Outlook, Yahoo Mail, ProtonMail та Zoho Mail, оснащені вбудованими інтелектуальними антифішинговими фільтрами, які автоматично аналізують як заголовки листів, так і зміст повідомлень, а також сканують вкладення та URL-посилання на предмет фішингових шаблонів або ознак соціотехнічного впливу.

Для корпоративного середовища, де масштаби інформаційного обміну значно більші, використовуються розширені поштові шлюзи безпеки, зокрема Proofpoint Email Protection, Barracuda Email Security Gateway, Mimecast Email Security, які інтегруються у внутрішні системи організації. Ці платформи забезпечують багаторівневу фільтрацію вхідної пошти, здійснюють аналіз репутації відправника, структури посилань, метаданих, поведінкових шаблонів, а також підтримують автоматичне карантинування підозрілих повідомлень. Вони також дають змогу налаштовувати політики безпеки - наприклад, блокувати листи з певних географічних регіонів або з використанням нетипових доменів.

Особливо важливу роль відіграють протоколи перевірки достовірності відправника - SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail) та DMARC (Domain-based Message Authentication, Reporting and Conformance). SPF дозволяє перевірити, чи має сервер-джерело право надсилати пошту від імені вказаного домену. DKIM забезпечує криптографічну перевірку цілісності повідомлення за допомогою цифрового підпису. У свою чергу, DMARC є політикою, що об'єднує SPF та DKIM, і дозволяє одержувачу застосовувати певні дії до листів, які не проходять аутентифікацію - наприклад, видалення або переміщення в карантин. Сукупність цих технологій дозволяє мінімізувати кількість фальшивих листів, що приходять від імені відомих компаній або внутрішніх корпоративних адрес, що є типовим для фішингових атак, зокрема spear-phishing [22, с. 186-209].

Додатковим механізмом є фільтрація вмісту повідомлень (content filtering), яка передбачає аналіз тексту на наявність типових ознак соціальної інженерії: ключових фраз, закликів до дії, терміновості, погроз або обіцянок вигоди. Такі системи також здатні виявляти модифіковані URL-адреси (заміна літер, схожі символи, нестандартні домени) та автоматично замінювати або знеактивовувати небезпечні елементи листа. Окремі рішення дозволяють здійснювати «sandboxing» - тобто запуск підозрілих вкладень у віртуальному середовищі для перевірки їхньої поведінки без ризику зараження основної системи [23, с. 79-82].

Наступним критично важливим елементом у структурі технічного захисту від атак соціальної інженерії є системи аутентифікації та контролю доступу, які забезпечують перевірку особистості користувача та обмежують несанкціоноване використання інформаційних ресурсів. Їх призначення полягає у запобіганні доступу до системи з боку сторонніх осіб, навіть у випадках, коли зловмиснику вдалося отримати логін і пароль за допомогою фішингу або іншої форми соціальної маніпуляції.

Особливу ефективність демонструє двофакторна аутентифікація (2FA) - сучасний стандарт безпеки, що передбачає використання двох незалежних елементів для підтвердження особи: щось, що знає користувач (пароль) і щось, що він має (пристрій, токен, біометричний параметр) [24, с.130]. Цей підхід значно ускладнює реалізацію атаки, оскільки для успішного входу недостатньо лише перехопити пароль - потрібно також мати доступ до другого фактору. У практиці це реалізується за допомогою SMS-кодів, одноразових паролів (OTP), згенерованих у мобільному додатку, або апаратних ключів, як-от YubiKey.

Серед найбільш поширених і доступних платформ для реалізації двофакторної аутентифікації на рівні окремих користувачів вирізняються Google Authenticator, Microsoft Authenticator, Authy та FreeOTP. Ці мобільні додатки дозволяють генерувати коди доступу з обмеженим терміном дії, які прив’язані до конкретного пристрою. На корпоративному рівні активно використовуються такі масштабовані рішення, як Okta Identity Cloud, Cisco Duo Security, Microsoft Entra ID (раніше Azure Active Directory). Вони забезпечують централізоване

управління автентифікацією в межах організації, дозволяючи інтегрувати багатоетапну перевірку особистості з внутрішніми системами, хмарними платформами (наприклад, Microsoft 365, AWS, Google Workspace), а також мобільними пристроями працівників (BYOD-політика).

Додатково до цього все ширше застосовуються біометричні методи аутентифікації, які ґрунтуються на унікальних фізіологічних характеристиках користувача. Найчастіше реалізується сканування відбитків пальців, розпізнавання обличчя (Face ID), райдужної оболонки ока, а також розпізнавання голосу. Такі методи практично неможливо підробити, а отже, вони забезпечують високий рівень впевненості в ідентичності користувача [25]. Біометричні технології сьогодні інтегруються не лише в мобільні пристрої та ноутбуки, а й у банківські системи, платіжні сервіси, медичні інформаційні ресурси, що особливо актуально в умовах зростання вимог до захисту персональних даних.

Не менш важливим аспектом контролю доступу є принцип рольового розмежування прав (RBAC - Role-Based Access Control), згідно з яким користувач отримує доступ лише до тих ресурсів, які необхідні йому для виконання службових обов’язків. Такий підхід дозволяє мінімізувати шкоду у разі компрометації окремого облікового запису, а також значно підвищує керованість інформаційної системи. У поєднанні з журналами доступу, автоматичним блокуванням облікових записів у разі виявлення підозрілих спроб входу та впровадженням політик складності паролів, системи аутентифікації формують перший бар’єр на шляху соціоінженерних атак, зокрема фішингу, вішингу та атак на паролі.

Важливим напрямом захисту від атак є моніторинг активності користувачів. Тут застосовуються системи поведінкового аналізу, такі як Splunk UBA або Microsoft Sentinel UEBA, що дозволяють виявляти відхилення від стандартної поведінки співробітника - наприклад, раптовий доступ до великої кількості файлів, зміну IP-адреси чи виконання нетипових запитів. Крім цього, SIEM-системи (Security Information and Event Management), серед яких найвідоміші - IBM QRadar, ArcSight, Graylog, - дозволяють здійснювати

централізований збір і аналіз подій безпеки, швидко виявляючи індикатори компрометації, пов’язані з соціальними маніпуляціями або підозрілими діями з боку користувачів.

Ще одним критично важливим елементом є забезпечення кібергігієни на рівні кінцевих пристроїв. Антивірусне програмне забезпечення з модулями антифішингу, таке як Kaspersky Endpoint Security, ESET NOD32 чи Bitdefender, дозволяє блокувати фішингові посилання в реальному часі, перевіряти вкладення, сканувати документи та попереджати користувача про потенційну загрозу ще до її активації [26]. Мережеві брандмауери (фаєрволи), як-от Fortinet чи Palo Alto Networks, регулюють вхідний і вихідний трафік, забезпечуючи автоматичне блокування підозрілих з'єднань. Також критично важливим є регулярне оновлення операційних систем і програмного забезпечення, що здійснюється, зокрема, за допомогою платформ централізованого управління патчами, таких як ManageEngine Patch Manager Plus.

У корпоративному середовищі дедалі ширше застосовуються спеціалізовані платформи класу EDR (Endpoint Detection and Response), які дозволяють контролювати активність на рівні кінцевих пристроїв і оперативно реагувати на аномальні сценарії. Серед них - CrowdStrike Falcon, Symantec EDR, Sophos Intercept X. Вони дають змогу не лише зупиняти потенційні загрози, а й детально досліджувати хронологію атаки. Не менш ефективними є платформи кіберрозвідки, наприклад Recorded Future або ThreatConnect, які збирають інформацію про нові техніки атак соціальної інженерії ще до їх поширення в реальному середовищі, надаючи організаціям можливість превентивного захисту [27]. Деякі компанії також впроваджують рішення для внутрішнього тестування персоналу - наприклад, KnowBe4 - що дозволяє змоделювати фішингові атаки в контрольованих умовах і проаналізувати поведінку співробітників у реальному часі.

На завершення варто зазначити, що технічні засоби повинні також охоплювати заходи протидії фізичним проявам соціальної інженерії. Зокрема, використання фільтрів конфіденційності для екранів дозволяє мінімізувати

ризики зчитування даних третіми особами (наприклад, у публічних місцях). Програми для виявлення кейлогерів - SpyShelter, Zemana AntiLogger - запобігають несанкціонованому зчитуванню паролів, особливо на комп'ютерах загального користування [28].

Аналіз технічних засобів захисту від атак соціальної інженерії демонструє, що ефективність інформаційної безпеки сьогодні напряму залежить не лише від наявності певних захисних рішень, а від рівня їх інтеграції, адаптивності та здатності до співпраці в межах єдиної цифрової екосистеми. З огляду на стрімку еволюцію кіберзагроз, основним критерієм ефективності технічних засобів стає не їхня технічна досконалість, а здатність працювати на випередження - виявляти потенційні загрози до того, як вони встигнуть завдати шкоди.

Водночас важливо усвідомлювати, що жодна система, навіть найбільш автоматизована чи «розумна», не є універсальним щитом. Слабке місце будь-якої архітектури кіберзахисту - це людина. Саме тому технічні засоби повинні розглядатися не як самодостатній елемент, а як частина комплексної системи захисту, в якій вони функціонують у тісному зв'язку з організаційними заходами, нормативною базою та освітніми ініціативами. Вони створюють сприятливе середовище, в якому користувачеві легше уникнути помилок, а система здатна оперативно виявляти підозрілі дії та реагувати на них.

Крім того, на особливу увагу заслуговує гнучкість сучасних платформ: можливість масштабування, кастомізації під конкретні бізнес-процеси, хмарна інтеграція, а також розвиток засобів на базі штучного інтелекту відкривають нові горизонти у сфері протидії соціальним атакам. Інвестування у такі рішення вже не сприймається як витрата - це стратегічна інвестиція у стабільність, довіру клієнтів та репутацію організації.

У перспективі слід очікувати подальшого розширення функціоналу захисних платформ, їх глибшої інтеграції з аналітикою поведінки користувачів та здатності до самонавчання. Відповідно, майбутній фокус буде зміщуватися не лише на запобігання атакам, а й на виявлення прихованих шаблонів, прогнозування загроз і формування антикризових сценаріїв на основі великих

даних. Такий підхід відкриває можливості не лише для оборони, а й для стратегічного управління ризиками в цифрову епоху.

2.3 Психологічні аспекти протидії соціальній інженерії

У добу стрімкої цифровізації, коли більшість комунікацій, транзакцій та рішень здійснюються через інформаційні технології, зростає залежність суспільства від безпеки цифрового середовища. Однак поряд із розвитком технічних засобів захисту постає загроза, яка не ґрунтується на складних алгоритмах чи шкідливому програмному забезпеченні - мова йде про соціальну інженерію. Її суть полягає у психологічному впливі на людину задля досягнення кіберзлочинних цілей: шахраї апелюють до емоцій, навичок, очікувань і реакцій користувача, змушуючи його діяти у спосіб, вигідний атакуючому. Така форма атаки є однією з найнебезпечніших саме тому, що вона оминає технічні бар'єри та фокусується на слабкій ланці - людині. Це зумовлює необхідність вивчення психологічних аспектів як ключового чинника у побудові ефективної системи захисту від сучасних кіберзагроз [29].

Соціальна інженерія, яка є сучасною формою маніпулятивного впливу в цифровому середовищі, використовує не технології як основний інструмент атаки, а людину - її поведінку, сприйняття, помилки мислення, емоції. Успішність такого підходу прямо залежить від глибокого знання психологічних механізмів, що керують людською реакцією в умовах стресу, терміновості або довіри. У цьому контексті психологічні аспекти стають не лише фоновим фактором, а й головною ціллю атаки. Саме тому протидія соціальній інженерії має враховувати не лише технічні або організаційні заходи, а й обов'язково включати елементи психологічного захисту - формування внутрішньої стійкості до маніпуляцій, розвиток навичок критичного мислення, емоційної саморегуляції та цифрової обережності.

Одним із базових методів впливу є апеляція до авторитету - одна з найдавніших і водночас найпотужніших когнітивних стратегій, які

використовуються в маніпулятивній комунікації. Люди з дитинства навчені слухатися тих, кого сприймають як фахівців, начальників, експертів. Це стосується не лише фізичної присутності авторитету, а й візуального або текстового натяку на нього. Соціальні інженери використовують цю схильність, підробляючи імена, електронні адреси, підпис електронного листа, використовуючи стиль корпоративного спілкування, логотипи банків або установ. У результаті людина, не маючи об'єктивних доказів справжності, піддається на переконання і виконує інструкції - надає доступ до даних, переказує кошти, відкриває шкідливі документи. Надійною лінією оборони тут є формування звички критичної верифікації джерел - звіряння електронних адрес, перевірка інформації через офіційні контакти та відмова виконувати будь-які дії лише на основі одного каналу комунікації. Метод «перехресної перевірки» - звернення до іншого джерела або особи - значно знижує ефективність маніпуляції.

Не менш важливою є стратегія створення тиску через терміновість і страх. Соціальні інженери чудово розуміють, що у стані стресу мислення людини переходить з раціонального на реактивне: вона намагається якомога швидше вирішити проблему, мінімізуючи ризик. Тому повідомлення типу «ваш рахунок буде заблоковано через 5 хвилин», «ми виявили спробу входу до вашого акаунта» викликають миттєву реакцію - страх або тривогу, які спричиняють дію без належного обмірковування. Особливо чутливими до таких атак є літні люди, емоційно нестабільні користувачі, а також ті, хто працює в умовах інформаційного перенавантаження. Практика захисту в таких ситуаціях передбачає навички усвідомлення емоційного стану - вміння розпізнати стресову реакцію, зупинитися, зробити кілька глибоких вдихів, оцінити джерело повідомлення і лише потім приймати рішення. Універсальне правило: жодне важливе рішення не ухвалюється у стані тиску або поспіху.

Ще одним важливим вектором впливу є соціальне наслідування - так званий ефект «соціального доказу». Зловмисники посилаються на вигадані приклади: «всі співробітники вже підтвердили свої дані», «більшість

користувачів перейшли за цим посиланням». Цей механізм активує глибинну соціальну потребу людини не випадати з групи, бути «як усі». Він особливо ефективний у середовищах з жорсткою ієрархією або низьким рівнем цифрової грамотності. Протидія подібним прийомам полягає в індивідуалізації мислення: користувач має звикнути питати себе, чи дійсно це його особиста необхідність, чи це лише спроба маніпулювати його поведінкою. У цьому контексті ефективною є практика ментального «кроку назад» - виходу з потоку нав'язаних рішень для формування власного судження.

Маніпуляції через емоції - зокрема співчуття, жалість, страх - є окремим напрямом атак соціальної інженерії. Повідомлення з фотографіями постраждалих, прохання про допомогу дітям, гуманітарні історії - все це створює потужний емоційний вплив. Людина починає відчувати провину або сором за бездіяльність і піддається спонуканню «зробити щось хороше». Соціальні інженери використовують ці емоції як приманку для збору персональних даних або переказу грошей. Тут захист базується на розмежуванні емоції та дії: важливо навчитися відокремлювати почуття від факту, проводити перевірку джерела, шукати підтвердження від авторитетних благодійних організацій, не діяти за першим емоційним імпульсом. Психологічна гігієна передбачає вміння зберігати співчуття, не втрачаючи раціональності.

Сильним каналом впливу також є інтерес або цікавість. Люди інстинктивно реагують на несподівані або особисті повідомлення: «відео про вас», «ваше ім'я згадане в інтернеті», «новий рейтинг вашого профілю». Це викликає потяг дізнатись більше, і користувач самостійно відкриває фішингові посилання. Саме тому найуспішніші атаки часто замасковані під новини, тестування, соціальні мережі. Формування стійкого психологічного захисту вимагає розвитку звички сумніву: якщо повідомлення викликає миттєвий інтерес, треба поставити собі запитання: «Чи не занадто це провокаційно?», «Чи дійсно це достовірне джерело?». Усвідомлення того, що цікавість - слабке місце для маніпуляції, дозволяє перехопити контроль над власною поведінкою.

Небезпечним фактором є також автоматизм дій, особливо в умовах когнітивної втоми. Під кінець робочого дня, у п’ятницю ввечері або після тривалих нарад люди втрачають здатність повноцінно аналізувати інформацію. У цей момент активізуються шаблони: клацнути на лист, ввести пароль, не читаючи тексту. Це - золота пора для соціального інженера. Для протидії важливо впроваджувати регламенти, що обмежують доступ до критичних систем у години низької продуктивності, а також створювати індивідуальні ритуали: «перевірка вдруге», «нічого не відкривати без контексту», «ввечері - тільки читати, не діяти».

Нарешті, надзвичайно небезпечною є ілюзія безпеки, яку створюють зловмисники, імітуючи знайомі середовища: логотип банку, дизайн вебсайту, інтерфейс платформи. Людина бачить знайомий вигляд і перестає бути пильною. Вона вводить пароль, номер карти, ім’я, не помічаючи деталей - наприклад, помилки в адресі, заміни букв у домені, відсутності сертифіката. Єдиний надійний спосіб протидії - формування ментальної звички завжди перевіряти URL, користуватись закладками, не довіряти навіть «знайомому» зовнішньому вигляду без перевірки технічних параметрів сторінки.

З погляду когнітивної психології, соціальна інженерія апелює до когнітивних упереджень - систематичних помилок у мисленні, які притаманні більшості людей. Наприклад, евристика доступності змушує людину приймати рішення, ґрунтуючись на останньому або найемоційнішому досвіді, тоді як ефект знайомості підвищує довіру до відправників, з якими раніше вже відбувалася взаємодія, навіть якщо вони цього разу - підроблені. Зловмисники використовують ці особливості для формування переконливих сценаріїв обману, які здаються цілком логічними і прийнятними в момент дії.

Протидія подібним впливам передбачає не лише технологічні бар’єри, а й формування психологічної грамотності користувачів. Це означає, що кожна людина має вміти розпізнати ознаки маніпуляції: різке емоційне збудження, заплутану термінологію, викривлену логіку в комунікації, заклики до дії без пояснення наслідків. Ключовим елементом у цьому процесі виступає розвиток

критичного мислення, що ґрунтується на аналізі джерел, перевірці фактів, формуванні гнучкості мислення та здатності утримуватися від імпульсивних реакцій.

Важливу роль у захисті відіграє також емоційна саморегуляція, особливо в умовах високого навантаження, інформаційного шуму та цифрового перевантаження. Люди, які вміють зберігати спокій і розсудливість у стресових ситуаціях, значно рідше стають жертвами соціоінженерних атак. Саме тому в сучасних тренінгових програмах для працівників ІТ-сектору або держустанов усе частіше з'являються модулі з емоційної стійкості, психології обману, невербального розпізнавання шахрайських намірів у комунікації.

Окремий напрям протидії - формування інформаційної культури в організації, де кожен працівник не лише дотримується політик, а й активно бере участь у побудові «психологічного імунітету» колективу. Це включає внутрішню комунікацію про ризики, відкритість до повідомлень про інциденти, спільне навчання, обговорення нових типів атак, впровадження принципу «запитання краще, ніж дія без впевненості». Ефективна організація повинна створювати не атмосферу страху помилитися, а атмосферу довіри до обговорення сумнівних ситуацій.

Наукові дослідження підтверджують, що поєднання психологічної підготовки з технічними засобами (антифішинг, моніторинг поведінки, політика доступу) знижує ймовірність успішної соціоінженерної атаки у десятки разів. Саме люди, які проходили регулярні тренінги, продемонстрували більшу здатність до розпізнавання загроз, відмови від сумнівних дій та повідомлення про інциденти вчасно [30]. Таким чином, психологічна стійкість не є чимось абстрактним - вона має цілком практичне значення для кіберзахисту.

У майбутньому важливими напрямами розвитку стануть використання штучного інтелекту для аналізу психологічних реакцій користувачів, створення адаптивних навчальних систем, які автоматично моделюють атаки відповідно до індивідуального рівня сприйнятливості, а також впровадження психологічних профілів кіберризику для персоналу. Такі інновації дозволять побудувати дійсно

комплексну, персоналізовану систему захисту, де психологічний аспект перестане бути другорядним і стане повноцінним інструментом безпеки.

Психологічні аспекти соціальної інженерії є ключовим напрямом дослідження, оскільки саме через них реалізуються більшість атак: апеляція до авторитету, створення відчуття терміновості, використання страху, маніпулювання співчуттям чи цікавістю. Вивчення цих механізмів дозволяє не лише краще розуміти логіку дій зловмисника, але й розробити ефективні заходи протидії, які спиратимуться на психологічну стійкість, критичне мислення та освіченість користувачів.

Психологічний підхід до інформаційної безпеки стає обов’язковим елементом сучасної кіберзахисної стратегії. Розуміння внутрішніх механізмів сприйняття, реакції на стрес, впливу емоцій на рішення - усе це формує підґрунтя для формування особистої та колективної інформаційної культури.

Розгляд психологічних аспектів протидії соціальній інженерії дозволяє усвідомити, що ефективна інформаційна безпека в умовах сучасної цифрової реальності вимагає не лише технічної озброєності, а насамперед - ментальної готовності користувача до виявлення маніпулятивних впливів. Людський фактор, який ще донедавна сприймався як слабка ланка кіберзахисту, сьогодні все більше розглядається як ключовий ресурс протидії - за умови правильного формування інформаційної культури, поведінкової гнучкості та емоційної стійкості.

Успішна протидія соціоінженерним атакам базується не на запам’ятовуванні окремих прикладів загроз, а на формуванні нової звички - ставити під сумнів усе, що порушує звичний хід мислення або емоційно вибиває з рівноваги. Саме таке критичне ставлення до інформаційної взаємодії здатне перетворити користувача з потенційної жертви на активного елементу захисту. Варто підкреслити, що психологічна обізнаність є не точковим заходом, а процесом, що потребує постійного оновлення знань, рефлексії власних реакцій, міжособистісного обговорення ризиків і впровадження поведінкових шаблонів безпечної комунікації.

Отже, сучасна парадигма кіберзахисту дедалі більше акцентує увагу не на технічному відокремленні користувача від загроз, а на його включеності у процес безпеки. І в цій динаміці психологічні інструменти - освіта, емоційна компетентність, ментальна стійкість - відіграють ключову роль. Їх системне застосування здатне сформувати нову якість цифрової безпеки, де людина стає не жертвою, а активним суб’єктом кіберпростору.

3 РОЗРОБКА КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ВІД АТАК СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ

3.1 Архітектура системи захисту

Формування ефективної системи захисту від соціоінженерних загроз вимагає цілісного, структурованого підходу, який виходить за межі окремих технічних рішень чи індивідуальних заходів. У зв’язку з цим постає потреба у розробці архітектури - продуманої, інтегрованої моделі, що поєднує в собі інструменти технічного, організаційного, психологічного та правового рівнів. Така архітектура виконує роль каркасу інформаційної безпеки, де кожен її елемент взаємодіє з іншими, утворюючи багаторівневу систему протидії.

Особливість захисту від соціальної інженерії полягає в необхідності врахування людського фактору як основного об'єкта атаки. Як зазначено в роботі, присвяченій моделюванню інформаційно-комунікаційних мереж, ефективна архітектура має передбачати не лише захист від зовнішніх загроз, але й від можливих помилок персоналу. Зокрема, підкреслюється, що застосування концепції CSM ICN сприяє підвищенню живучості та стійкості мережі в умовах атак, помилкових дій співробітників і навіть форс-мажорних обставин [31, с. 13-19]. Це означає, що проєктування системи має базуватись на принципах резервування, самодіагностики та швидкого відновлення, що мінімізує потенційні наслідки внутрішніх організаційних або індивідуальних помилок. Тож, людський фактор повинен враховуватись не лише в рамках навчання, а й на рівні технічної побудови системи.

У межах даного пункту буде розглянуто основні компоненти архітектури системи захисту і взаємозв’язки між підсистемами. Це дозволить сформувати цілісне уявлення про захисне середовище, яке здатне ефективно протистояти атакам, що базуються не на технологіях, а на маніпуляціях свідомістю людини.

Насамперед хотілося б визначити, що побудова архітектури системи захисту від атак соціальної інженерії повинна ґрунтуватися на принципах комплексності, багаторівневості та інтеграції. Соціальна інженерія є

багатогранним викликом, який не обмежується технічними загрозами - вона передусім фокусується на маніпулюванні людською поведінкою. Саме тому ефективна система має включати кілька функціональних рівнів, кожен з яких виконує унікальну роль у протидії потенційним загрозам.

Технічний рівень, або інфраструктурна безпека, становить базовий захисний шар, що забезпечує безперервну фільтрацію комунікацій та контроль за цілісністю цифрового середовища. До цього рівня відносяться системи фільтрації електронної пошти, які дозволяють виявляти фішингові листи, спам і підозрілі вкладення. Брандмауери, антивіруси та EDR-рішення (Endpoint Detection and Response) формують активну оборону кінцевих точок доступу до мережі, запобігаючи несанкціонованому проникненню та реагуючи на аномальну активність. Особливо важливою складовою є використання багатофакторної аутентифікації (2FA/MFA), яка значно ускладнює можливість компрометації облікових даних навіть у разі фішингу. Додаткову захищеність забезпечує застосування VPN, шифрування трафіку та цифрових сертифікатів. Для забезпечення постійного моніторингу та аналізу інцидентів у реальному часі інтегруються SIEM-платформи, що здійснюють централізований збір і аналіз подій безпеки.

Організаційний рівень охоплює нормативно-процедурний аспект захисту. Він передбачає розробку політик інформаційної безпеки, які регламентують порядок дій працівників у випадку виявлення підозрілих запитів чи ситуацій. Особливе значення має визначення чітких регламентів доступу до конфіденційної інформації відповідно до принципу найменших привілеїв. Обов’язковим компонентом є постійне навчання персоналу, тренінги з моделювання фішингових сценаріїв та реагування на інциденти. Кадровий контроль, включаючи перевірку співробітників під час прийому на роботу та регулярну ротацію доступів, знижує ймовірність внутрішніх загроз.

Поведінковий рівень - це психологічна складова архітектури захисту, яка фокусується на формуванні цифрової свідомості користувачів. До нього належать програми розвитку критичного мислення, тренінги з розпізнавання

маніпулятивних технік - таких як апеляція до авторитету, терміновість дії, виклик співчуття. Створення безпечного середовища для обговорення інцидентів без страху бути покараним сприяє оперативному реагуванню. Не менш важливим є заохочення проактивної поведінки - коли співробітники самі ініціюють повідомлення про потенційні загрози.

Аналітичний рівень передбачає збір, обробку та інтерпретацію інформації про інциденти безпеки. Побудова моделей поведінкових ризиків та аналіз типових векторів соціоінженерного впливу дозволяє створити системи раннього попередження. Поведінкова аналітика сприяє виявленню відхилень у динаміці дій користувача, що може свідчити про спробу маніпуляції або компрометації.

Правовий та нормативний рівень виступає як основа для легітимності всієї архітектури. Він забезпечує відповідність міжнародним стандартам (зокрема ISO/IEC 27001, GDPR), чітко визначає юридичні наслідки за порушення внутрішніх правил безпеки та встановлює процедури документального супроводу інцидентів. Регулярний аудит політик та контроль дотримання вимог дозволяє забезпечити не лише формальну, а й реальну ефективність захисних заходів.

Завершальним, але не менш важливим компонентом архітектури є інформаційно-комунікаційна підсистема. Вона забезпечує постійне інформування співробітників про нові загрози, поширення інструкцій, інфографіки, запуск внутрішніх кампаній з підвищення рівня обізнаності. Також важливо створити ефективні механізми зворотного зв’язку - гарячі лінії, електронні адреси, платформи для анонімного повідомлення про інциденти. Підсилення мотивації співробітників до дотримання правил - ще один ключовий чинник цієї підсистеми.

Остаточний вигляд обов’язкових складових системи захисту виглядає так:

Таблиця 3.1 - Складові системи захисту

Рівень	Опис компонентів
Технічний рівень (інфраструктурна безпека)	- Системи фільтрації електронної пошти (антифішинг, спам-фільтри) - Брандмауери, антивіруси, EDR-рішення - Системи багатофакторної аутентифікації (2FA/MFA) - VPN, шифрування трафіку, цифрові сертифікати - SIEM-платформи для моніторингу та реагування на інциденти
Організаційний рівень	- Політики інформаційної безпеки (інструкції, протоколи реагування) - Регламенти доступу до критичної інформації - Навчання персоналу, тренінги та симуляції фішингових атак - Кадровий контроль (перевірка співробітників, ротація доступів)
Поведінковий рівень (психологічна складова)	- Програми розвитку критичного мислення у співробітників - Навички розпізнавання маніпуляцій (авторитет, терміновість, співчуття) - Створення безпечного середовища для обговорення інцидентів - Заохочення проактивної кіберповедінки
Аналітичний рівень	- Збір, обробка та аналіз інцидентів - Побудова моделей соціоінженерних впливів - Поведінкова аналітика та профілювання користувачів
Правовий та нормативний рівень	- Впровадження відповідності до стандартів (ISO/IEC 27001, GDPR) - Юридичне оформлення процедур відповідальності - Аудит дотримання політик безпеки
Інформаційно-комунікаційна підсистема	- Внутрішні інформаційні кампанії про кіберзагрози - Механізми зворотного зв’язку (гарячі лінії, пошта для інцидентів) - Платформи для тестування знань та мотиваційні програми

3.2 Реалізація програми навчання персоналу

Успішне протистояння сучасним загрозам потребує не лише технологічних бар'єрів, а й високої інформаційної культури користувачів. Саме тому у центрі сучасної стратегії безпеки дедалі більше уваги приділяється створенню умов, за яких персонал виступає активним учасником захисного процесу - не лише дотримуючись правил, а й розуміючи їхню доцільність та потенційну ціну помилки.

Навчання у сфері протидії соціальній інженерії не зводиться до одноразового ознайомлення з інструкціями чи правил користування системою. Це має бути постійний, інтерактивний процес, що включає симуляції реальних загроз, моделювання атак, психологічну підготовку, оцінювання рівня кіберграмотності й зворотний зв’язок. Такий підхід дозволяє не лише підвищити інформованість співробітників, але й сформувати культуру безпеки - атмосферу, в якій обережність, відповідальність і проактивність стають нормою цифрової поведінки.

У межах цього пункту буде розглянуто структуру програми навчання, її ключові етапи, інструменти реалізації, а також підходи до адаптації освітнього контенту відповідно до рівня підготовки персоналу й специфіки діяльності організації. Такий аналіз дозволить обґрунтувати доцільність інвестицій у людський потенціал як один з основоположних факторів ефективного кіберзахисту.

Успішне протистояння загрозам соціальної інженерії в сучасному цифровому середовищі неможливе без активного залучення людського чинника як основи ефективного кіберзахисту. Оскільки переважна більшість атак соціоінженерного характеру націлена не на технічну інфраструктуру, а на поведінкові та психологічні слабкості користувачів, ключову роль відіграє рівень їхньої поінформованості, критичного мислення та здатності протидіяти маніпулятивному впливу. Саме тому впровадження комплексної, системної

програми навчання персоналу виступає як фундаментальний елемент безпеки організації [32, с. 183-187].

Структура навчальної програми повинна бути чітко продуманою, багаторівневою та гнучкою. Перший етап - базовий рівень - передбачає ознайомлення співробітників з основними поняттями соціальної інженерії: що це таке, як вона працює, які існують форми атак (фішинг, смішинг, вішинг, бейтинг тощо), якими є загальні принципи кібергігієни. Цей блок має на меті сформувати первинне розуміння сутності загроз та прищепити основні звички обережного поводження з інформацією. На цьому рівні активно використовуються прості мультимедійні матеріали, короткі відеоуроки, інфографіка, кейси з реального життя.

Наступний компонент - функціональний модуль - передбачає деталізацію знань відповідно до функціонального навантаження працівників. Для співробітників ІТ-відділу це можуть бути теми виявлення аномальної активності в мережі, аналіз логів, впровадження політик безпеки. Працівники фінансових служб отримують знання про шахрайські схеми, пов’язані з рахунками, електронними переказами або псевдоінвойсами. Служби підтримки навчаються розпізнавати маніпулятивні звернення, підроблені запити та інші способи соціального тиску.

Особливо важливим елементом програми є практичний блок, який передбачає залучення співробітників до симуляцій реальних загроз. Це може бути фішингова розсилка, підроблене повідомлення нібито від керівника, телефонний дзвінок із проханням терміново надати доступ чи підтвердити паролі. Участь у таких ситуаціях дозволяє закріпити теоретичні знання на практиці, виявити прогалини у поведінці, сформувати автоматизм захисних реакцій. Ефективність цього блоку полягає не лише у створенні навчального тиску, але й у його подальшому аналізі - зворотний зв’язок надається в індивідуальній формі, без осуду, із чіткими рекомендаціями.

Далі слідує етап підсумкової оцінки, що охоплює не лише тестування знань, але й повноцінну поведінкову аналітику. Важливо оцінювати не просто

запам’ятовування матеріалу, а здатність застосувати його в реальних ситуаціях. Це може включати автоматизоване тестування в LMS-системах, аналіз результатів участі в симуляціях, порівняння до- та післятренінгових реакцій.

Завершальним, проте критично важливим компонентом структури є безперервне оновлення знань. Загрози соціальної інженерії еволюціонують надзвичайно швидко, з’являються нові схеми, змінюються інструменти, які використовують зловмисники. Відтак, програма має включати календар періодичного оновлення: щомісячні розсилки новин про новітні загрози, щоквартальні повторні тести, щорічне переатестування, семінари з розбором інцидентів у світовій практиці.

Реалізація навчання включає кілька ключових етапів. Перший - діагностика - проводиться для встановлення базового рівня знань і розуміння серед працівників. Це може бути онлайн-анкетування або короткий вступний тест. Другий етап - подання навчального матеріалу - реалізується в різних форматах: лекції, відеоуроки, інтерактивні модулі, вебінари. Третій - практична симуляція - передбачає імітацію інцидентів, що дозволяє дослідити реальні реакції співробітників. Четвертий - оцінка ефективності - виявлення сильних і слабких сторін у засвоєнні матеріалу. П’ятий - зворотний зв’язок і вдосконалення - включає індивідуальні рекомендації, доповнення матеріалів, персоналізацію наступного навчального блоку.

Сучасні інструменти реалізації навчання забезпечують високу ефективність та автоматизацію процесів. Найбільш поширені - LMS-платформи (Learning Management System), які дозволяють централізовано керувати курсами, відслідковувати проходження, зберігати статистику. До таких платформ належать Moodle, TalentLMS, iSpring. Значну роль відіграють інтерактивні відео, що дозволяють користувачам приймати рішення у реальному часі, занурюючи їх у сценарії атак. Окремо варто згадати спеціалізовані сервіси, як-от KnowBe4 або PhishLabs, що дозволяють проводити реалістичні фішингові атаки з подальшим аналізом. Також використовуються інформаційні кампанії: постери, інфографіка, електронні нагадування, які підтримують актуальність теми у

свідомості співробітників. Гейміфіковані підходи - сертифікати, внутрішні рейтинги, командні змагання - формують мотивацію і залученість, сприяючи зміцненню культури безпеки. Додатково застосовуються рольові ігри, в яких співробітники моделюють атаки один на одного або на організацію в цілому, що забезпечує найвищий рівень практичного занурення.

Важливою умовою ефективності є адаптація контенту до рівня підготовки персоналу та специфіки діяльності організації. Для нових співробітників пропонується базовий курс з орієнтацією на загальні принципи безпеки. Технічні фахівці отримують розширені блоки з аналізу журналів подій, мережевої безпеки, контролю доступу. Менеджери повинні навчатися розпізнавати психологічні загрози на рівні управління: фальшиві запити, маніпуляції, шахрайські схеми під виглядом офіційної комунікації. Для відділів із доступом до конфіденційних даних важливо надати знання про правові вимоги, стандарти захисту (наприклад, GDPR, ISO/IEC 27001), інструменти контролю за обробкою інформації. Цілеспрямований підхід до навчання дозволяє не лише заощадити ресурси, а й забезпечити точкову ефективність, де кожен співробітник отримує саме ті знання й навички, які відповідають його професійній ролі.

У підсумку, комплексна програма навчання персоналу як засіб протидії соціальній інженерії повинна розглядатися як динамічна система, що поєднує педагогічні, інформаційні та організаційні компоненти. Її реалізація не лише підвищує рівень індивідуальної цифрової обізнаності, а й формує стійку корпоративну культуру інформаційної безпеки, де кожен співробітник - це активний елемент захисту, а не потенційна вразливість.

3.3 Впровадження технічних засобів захисту

На відміну від організаційних чи психологічних заходів, технічні механізми працюють у безперервному режимі, автоматизуючи процеси моніторингу, реагування та протидії. До таких засобів належать як класичні інструменти - антивіруси, брандмауери, системи контролю доступу, - так і

сучасні рішення на базі штучного інтелекту, машинного навчання, поведінкової аналітики. Важливим аспектом є також їх інтеграція у загальну архітектуру безпеки підприємства, що передбачає взаємодію між різними рівнями захисту - від робочих станцій до хмарних середовищ.

Упровадження технічних засобів захисту в інформаційній інфраструктурі є надзвичайно складним, але необхідним процесом, що вимагає не лише технічних знань, а й стратегічного бачення, інтеграції з організаційними процесами та глибокого розуміння специфіки потенційних загроз. Для досягнення максимальної ефективності, реалізація технічного захисту повинна здійснюватися поетапно, із дотриманням чіткої послідовності дій. Така систематизація дозволяє не лише знизити ризики помилок, але й забезпечити гармонійне функціонування захисних механізмів в межах усієї корпоративної інфраструктури [11, с. 20-26].

Першим і найбільш критичним етапом є аналіз ризиків та визначення потреб безпеки. Будь-яка технічна реалізація повинна ґрунтуватися на реальних викликах і ризиках, з якими стикається організація. На цьому етапі здійснюється ідентифікація потенційних векторів атак, зокрема соціоінженерних, які часто становлять основну небезпеку через психологічний вплив на працівників. Також проводиться детальна оцінка поточного стану IT-інфраструктури: виявляються слабкі місця, відсутні ланки безпеки, недоліки в політиках доступу. Важливим завданням є визначення критичних активів - інформаційних ресурсів, систем і даних, порушення цілісності або доступності яких матиме найбільш згубні наслідки. Це дозволяє чітко сформулювати рівень необхідного захисту й визначити пріоритети для подальших дій.

Наступним етапом є планування технічної архітектури захисту, яке полягає у виборі підходу до побудови захисної системи. Залежно від потреб і структури підприємства, це може бути периметральна модель захисту, що концентрується на зовнішніх межах системи, адаптивна модель із застосуванням поведінкового аналізу або багаторівневий підхід, що комбінує різні технології на кількох рівнях (мережевому, прикладному, користувацькому тощо). На основі

цього визначаються функціональні вимоги до майбутніх технічних рішень: які саме загрози повинні бути виявлені, які дії мають блокуватися автоматично, який рівень інтеграції із наявними системами буде необхідним. Важливо, щоб захисна архітектура не конфліктувала з бізнес-процесами організації, а гармонійно доповнювала їх.

Після теоретичної розробки настає етап вибору та закупівлі технічних рішень. На цьому етапі проводиться порівняння різних засобів захисту: мережевих брандмауерів, систем виявлення та запобігання вторгненням (IDS/IPS), рішень класу EDR (Endpoint Detection and Response), SIEM-платформ для централізованого моніторингу, VPN-сервісів для шифрування трафіку тощо. Важливими критеріями є не лише функціональні можливості, а й юридичні аспекти (ліцензії), якість технічної підтримки, можливість масштабування рішень відповідно до зростання організації. За потреби проводиться пілотне впровадження обраного продукту - тестова інтеграція, що дозволяє на практиці оцінити сумісність, продуктивність і зручність використання.

Після остаточного вибору рішень здійснюється інсталяція та налаштування засобів захисту. Цей процес може включати як встановлення програмного забезпечення на робочі станції, сервери чи мережеві вузли, так і розгортання апаратних пристроїв. Не менш важливою є правильна конфігурація систем: визначення політик безпеки, правил доступу, критеріїв сповіщення про інциденти. Особливої уваги потребує інтеграція нових засобів із уже діючими системами: CRM, ERP, email-сервісами, внутрішніми базами даних. Лише за умови повної сумісності можна досягти синергії й уникнути "сліпих зон" у захисті.

Після розгортання захисних механізмів важливо провести тестування та валідацію ефективності. На цьому етапі проводяться внутрішні випробування, зокрема пентести (тестування на проникнення), які моделюють реальні атаки. Аналіз журналів подій дозволяє оцінити, як система реагує на підозрілу активність. У разі виявлення недоліків або невідповідностей проводяться

коригування конфігурацій, оновлення сигнатур, адаптація правил до реального середовища.

Жодна технічна система не буде ефективною без людського чинника, тому наступним логічним етапом є навчання персоналу та адміністраторів. Співробітники мають чітко розуміти, як працює система захисту, які їхні обов'язки у разі спрацювання системи, як взаємодіяти з техпідтримкою або службою безпеки. Адміністратори, у свою чергу, повинні вміти здійснювати моніторинг, оновлення, діагностику системи. У межах цього етапу розробляється технічна документація, визначаються відповідальні особи, створюються інструкції з дій у надзвичайних ситуаціях.

Завершальним, але постійно діючим етапом є моніторинг, аудит та оновлення систем захисту. Безперервний моніторинг дозволяє оперативно виявляти підозрілі події, вчасно реагувати на нові загрози, підтримувати актуальність конфігурацій. Аудити - як внутрішні, так і зовнішні - допомагають оцінити відповідність політик безпеки чинним стандартам (наприклад, ISO/IEC 27001), виявити недоліки у процедурі захисту, підготуватись до сертифікації. Регулярне оновлення сигнатур, виправлення вразливостей, оновлення програмного забезпечення - усе це формує гнучку, адаптивну систему кібербезпеки, здатну ефективно протидіяти постійно змінюваним викликам інформаційного середовища [34].

Таким чином, класифікація кроків впровадження технічних засобів захисту дозволяє сформувати логічно завершену, ефективну та стійку систему захисту інформації, яка охоплює не лише технологічні компоненти, а й організаційні та людські аспекти. Системний підхід до реалізації таких заходів забезпечує надійне функціонування IT-інфраструктури, зменшує ризик втрати даних, підвищує рівень довіри клієнтів та партнерів, а також сприяє зміцненню інформаційної стійкості організації в цілому.

Успішна реалізація технічного захисту інформаційного середовища свідчить про високий рівень інформаційної зрілості організації. Впровадження таких рішень потребує не лише інвестицій у програмно-апаратні ресурси, але й

комплексного підходу, що базується на стратегічному плануванні, міжвідділовій координації, постійному моніторингу та адаптації до динамічних умов загрозового ландшафту. Роль технічних засобів полягає не стільки у створенні ізольованого бар'єру, скільки у вибудовуванні цілісного механізму реагування, що функціонує у режимі реального часу та взаємодіє з іншими складовими системи безпеки - організаційною політикою, людськими ресурсами, правовим забезпеченням.

З огляду на наведені вище відомості, доцільним є представлення узагальненої структури, яка відображає систематизовану класифікацію ключових аспектів, що стосуються розробки комплексної системи захисту від атак соціальної інженерії (рисунок 3.1).

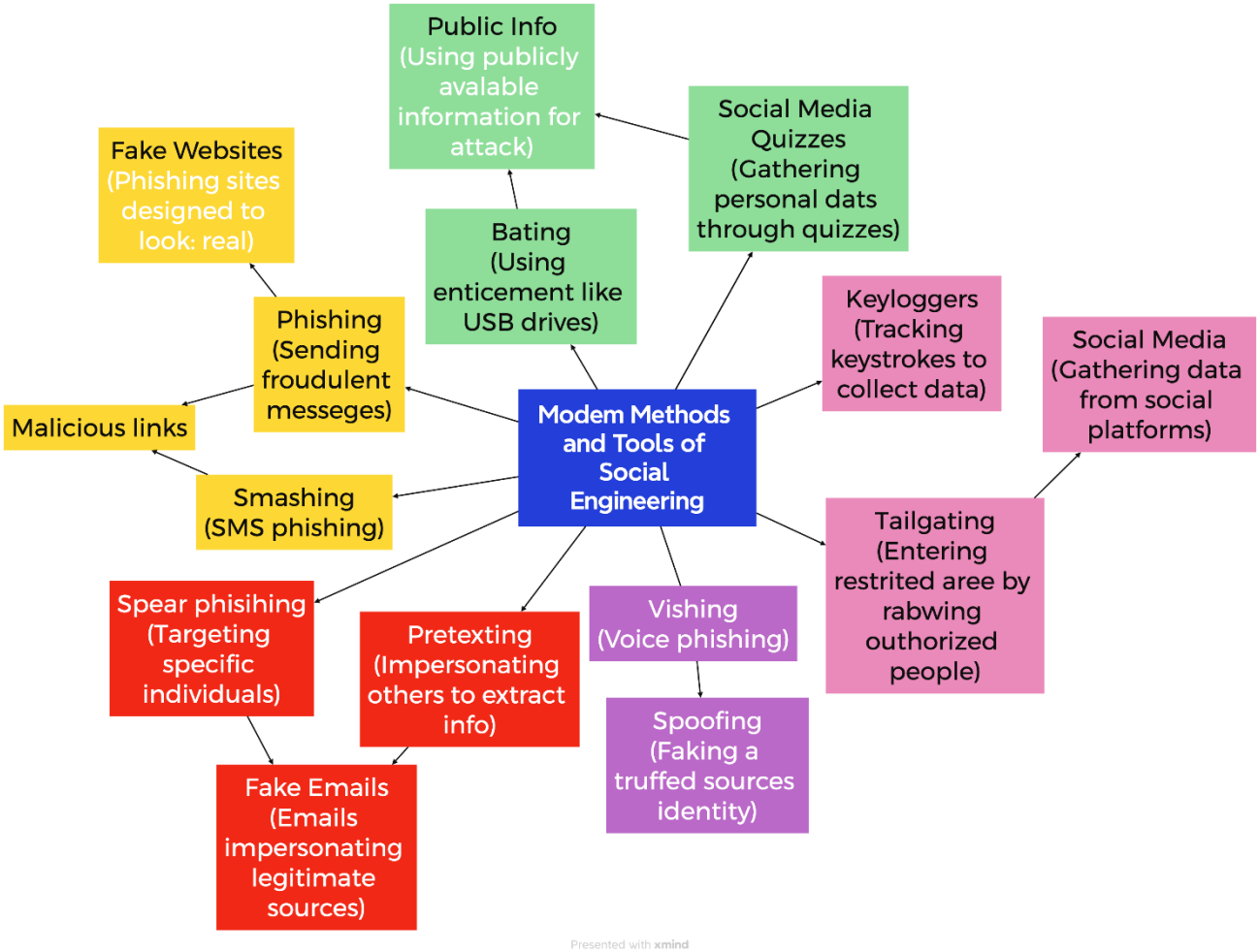

Рисунок 3.1 - Розробка комплексної системи захисту від атак соціальної інженерії

Технічні заходи мають розглядатися не як окремі продукти чи інструменти, а як складова інтегрованої архітектури захисту, де кожен компонент виконує чітко визначену функцію. Підхід, орієнтований на гнучкість, масштабованість і аналітичну обґрунтованість, дозволяє не лише відповідати на наявні виклики, а й проактивно протистояти майбутнім загрозам. Саме через грамотне впровадження технічних рішень організація отримує реальний контроль над своєю цифровою безпекою, трансформуючи потенційно вразливе середовище на стратегічно керований простір із високим рівнем захисту.

3.4 Тестування та оцінка ефективності системи

Після впровадження комплексу організаційних і технічних заходів захисту інформаційного середовища ключовим кроком у забезпеченні надійної кібербезпеки виступає тестування та подальша оцінка ефективності функціонування системи. Жодне, навіть найсучасніше технічне рішення, не може вважатися дієвим без підтвердження його результативності в реальних або змодельованих умовах. Саме тому перевірка працездатності механізмів безпеки, їх стійкості до потенційних загроз, відповідності вимогам та очікуванням - критично важливий етап, що дозволяє виявити слабкі місця, усунути недоліки й оптимізувати захисну інфраструктуру.

Тестування дає змогу перевірити не лише технічну надійність окремих компонентів системи, але й здатність персоналу реагувати на інциденти, узгодженість дій різних служб, а також динамічну адаптацію до змін у зовнішньому середовищі. Крім того, системна оцінка ефективності дозволяє зберігати відповідність стандартам галузі, регламентам внутрішнього аудиту та вимогам зовнішніх сертифікацій. У межах цього пункту буде розглянуто підходи до побудови тестового середовища, типи перевірок, інструменти оцінювання, а також критерії результативності, що дозволяють об’єктивно визначити рівень зрілості системи інформаційної безпеки.

У системі побудови інформаційної безпеки тестування та оцінка ефективності захисних рішень не лише мають завершальний характер у процесі впровадження, а й відіграють роль постійного елемента зворотного зв’язку. Це ключовий механізм, що дозволяє відмовитися від статичного підходу до безпеки на користь динамічної, самовідновлюваної та адаптивної моделі захисту. У сучасному середовищі, де загрози змінюються не щомісяця, а щодня, відсутність регулярного тестування перетворює навіть найкращі технічні рішення на неефективні інструменти. Лише через ретельне моделювання реальних атак, оцінку поведінкових реакцій, аналіз логів та стрес-тестування систем можна говорити про фактичну, а не декларативну готовність організації протистояти зовнішнім і внутрішнім загрозам.

Початковим рівнем перевірки є функціональне тестування технічних компонентів, що дозволяє переконатися у правильності інсталяції та конфігурації систем захисту. Цей тип перевірки проводиться на кожному етапі впровадження нових інструментів - від міжмережевих екранів до VPN-серверів, від систем багатофакторної аутентифікації до внутрішніх систем шифрування. Наприклад, під час тестування фаєрволу інженери перевіряють, чи блокуються порти з обмеженим доступом, чи працюють правила NAT, чи не пропускається трафік із заборонених джерел. У разі SIEM-платформи (наприклад, Splunk або IBM QRadar) перевіряється повнота збору логів, їх правильна кореляція та формування звітів відповідно до встановлених правил. Такий тип тестування дозволяє підтвердити коректну роботу інструментів у звичайному, щоденному режимі.

Однак лише функціональної перевірки недостатньо для реального аналізу стійкості системи. Саме тому проводиться тестування на проникнення, яке імітує дії зловмисника. У сучасній практиці використовуються як внутрішні пентести, так і зовнішні аудити із залученням спеціалізованих компаній. Мета - визначити, яким чином система може бути скомпрометована, починаючи від сканування мережі до отримання доступу до критичних даних. Наприклад, у процесі зовнішнього пентесту тестувальники можуть використати поширені уразливості

у веб-додатку (SQL-ін’єкції, XSS, CSRF), спробувати обійти автентифікацію через підбір паролів (брутфорс) або скористатися незахищеними API. Важливо, що тестування на проникнення включає також соціоінженерні сценарії: розсилка фішингових листів, підроблені повідомлення в месенджерах, дзвінки від імені "технічної підтримки". Це дає змогу оцінити не лише технічну захищеність, а й людський фактор - один із найвразливіших елементів безпеки.

Невід’ємною частиною комплексного підходу є аналіз журналів подій. У сучасних умовах кількість логів, які генерує система, сягає мільйонів записів на добу, особливо в середовищах з великою кількістю користувачів або інтенсивною взаємодією сервісів. Саме тому застосування SIEM-систем є критично важливим. Їхнє завдання - не лише збирати інформацію з різних джерел (сервери, маршрутизатори, бази даних, системи аутентифікації), але й виявляти в ній шаблони загроз. Наприклад, повторювані спроби входу до системи з різних IP-адрес можуть вказувати на атаку брутфорсом, тоді як аномальна активність вночі - на потенційний витік інформації або інсайдерську загрозу. Системи аналітики дозволяють автоматизувати ці процеси та скорочувати час реакції до хвилин або навіть секунд.

Окремий вимір - тестування процедур реагування на інциденти. Цей тип перевірок особливо важливий у великих організаціях або критичних галузях (банки, телеком, держсектор). Його мета - не перевірка програмного забезпечення, а оцінка взаємодії між підрозділами, комунікації в кризовій ситуації, дотримання протоколів реагування. Наприклад, симуляція DoS-атаки, яка "покладає" сервер електронної пошти, дозволяє перевірити, як швидко буде ідентифіковано проблему, чи вчасно буде сповіщено відповідальних осіб, наскільки швидко будуть активовані резервні рішення. Важливими метриками є час виявлення (MTTD - Mean Time to Detect), час реагування (MTTR - Mean Time to Respond), відсоток повідомлених користувачів, які діяли згідно з інструкцією [35].

Щоб результати тестування мали практичну цінність, їх необхідно формалізувати через систему оцінювання ефективності. До таких показників належать:

- Рівень виявлення загроз - відсоток успішно розпізнаних атак.
- Час до реагування - середній час між інцидентом та реакцією системи/персоналу.
- Кількість помилкових спрацювань - показник точності системи (False Positive Rate).
- Індекс проникнення - оцінка ефективності пентесту (рівень глибини доступу).
- Сумісність із галузевими стандартами - ISO/IEC 27001, NIST, OWASP тощо.

Ці критерії дозволяють не лише оцінити поточну ефективність, але й формувати тренди покращення або деградації безпеки в динаміці. Наприклад, зниження MTTR із 8 годин до 2 впродовж трьох місяців є показником зрілості системи реагування.

Після завершення тестування надзвичайно важливим є етап формування звіту. Він має містити не лише технічний опис виявлених вразливостей, але й аналітичні висновки, оцінку ризиків, пріоритезацію проблем та конкретні рекомендації. Для керівництва підприємства звіт дозволяє ухвалити рішення щодо інвестицій у безпеку, оновлення політик або запуск нових ініціатив. Для технічного персоналу - це дороговказ на найбільш критичні зони, що потребують уваги [36].

Отже, тестування та оцінка ефективності системи інформаційної безпеки - це не додаткова функція, а невід’ємна складова захисної архітектури. Вона формує культуру постійного вдосконалення, виявляє реальні слабкі місця, забезпечує зворотний зв’язок та дозволяє діяти проактивно, а не реактивно.

ВИСНОВКИ

У ході виконання цієї дипломної роботи я ґрунтовно дослідив природу соціоінженерних атак, механізми їх реалізації та засоби протидії. Моєю метою було не просто описати існуючі загрози, а розробити практичну, адаптивну й ефективну систему захисту, яка може бути впроваджена в реальному корпоративному середовищі. У результаті роботи мені вдалося комплексно охопити як теоретичні засади, так і практичні аспекти організації захисту від соціальної інженерії.

У першому розділі я визначив поняття соціальної інженерії, дослідив її природу як способу маніпулятивного впливу, що базується не на технічних вразливостях, а на психології людини. Проведена мною класифікація дозволила систематизувати основні типи атак та оцінити їхню потенційну небезпеку. Я також детально проаналізував сучасні методи та інструменти соціальних інженерів, включно з технічними рішеннями OSINT-розвідки, використанням соціальних мереж та спеціалізованого ПЗ.

У другому розділі я зосередився на захисній стороні. Мною були окреслені ключові підходи: організаційні, технічні й психологічні. У процесі аналізу я дійшов висновку, що жоден із цих напрямів не може бути ефективним сам по собі - лише їх синергія створює надійний захист. Я довів важливість нормативного регулювання, підвищення обізнаності працівників, запровадження політик інформаційної безпеки, а також розвитку цифрової емоційної грамотності.

У третьому розділі я запропонував власну модель комплексної системи захисту. Вона включає архітектурну побудову багаторівневої системи, створення адаптивної програми навчання персоналу, впровадження сучасних технічних засобів захисту, а також механізми оцінювання ефективності. Мною були розроблені сценарії тестування, описано приклади застосування SIEM-платформ, проведено моделювання інцидентів. Це дозволило перевірити

працездатність системи в динамічному середовищі та виявити потенційні зони вдосконалення.

Разом із тим, я усвідомлюю, що навіть найбільш досконала система потребує постійного розвитку. Тому я пропоную такі напрями покращення захисту від соціальної інженерії:

1. Впровадження систем поведінкової аналітики з використанням штучного інтелекту (UEBA), що дозволить виявляти відхилення у звичках користувача.
2. Розширення гейміфікованих освітніх платформ для підвищення мотивації персоналу.
3. Інтеграція адаптивного навчального контенту, який генерується автоматично на основі актуальних кіберзагроз.
4. Розгортання внутрішніх Red Team/Blue Team середовищ для моделювання реальних атак.
5. Співпраця з національними кіберцентрами задля отримання інформації про актуальні фішингові кампанії.

Загалом, я переконаний, що розроблена мною система є гнучкою, масштабованою та придатною до реального застосування. Вона поєднує технічні інструменти, управлінські практики та людський фактор в єдину інтегровану модель безпеки. Моя робота закладає підґрунтя для подальших досліджень і впроваджень у сфері кіберзахисту, формуючи базу для створення надійного, освіченого та критично мислячого цифрового середовища.

ПЕРЕЛІК ПОСИЛАНЬ

1. Савчук, Т. "Соціальна інженерія: як шахраї використовують людську психологію в інтернеті." Радіо Свобода. Суспільство (2018). URL: https://www.radiosvoboda.org/a/socialna-inzhenerija shaxrajstvo/29460139.html
2. Boyko, V., & Vasilenko, M. (2020). CYBERSECURITY OF "SMART CITIES": SOCIAL ASPECTS, RISKS OF DEANONYMIZATION AND DOXING: Array. Municipal Economy of Cities (Technical Science), 6(159), 186–195. Retrieved from https://khgts.kname.edu.ua/index.php/khgts/article/view/5694
3. Wang Z., Sun L., Zhu H. Defining social engineering in cybersecurity //IEEE Access. – 2020. – Т. 8. – С. 85094–85115. URL: https://ieeexplore.ieee.org/abstract/document/9087851
4. Biju J. M., Gopal N., Prakash A. J. Cyber attacks and its different types //International Research Journal of Engineering and Technology. – 2019. – Т. 6. – №. 3. – С. 4849–4852. URL: https://surl.lu/yxbyig
5. Wang Z., Zhu H., Sun L. Social engineering in cybersecurity: Effect mechanisms, human vulnerabilities and attack methods //IEEE Access. – 2021. – Т. 9. – С. 11895–11910. URL: https://ieeexplore.ieee.org/abstract/document/9323026
6. Sawa Y., Bhakta R., Harris I. G., Hadnagy C. Detection of social engineering attacks through natural language processing of conversations //2016 IEEE Tenth International Conference on Semantic Computing. – IEEE, 2016. – С. 262–265. URL: https://ieeexplore.ieee.org/abstract/document/7439345
7. Mouton, F., Nottingham, A., Leenen, L., Venter, H. S. Finite state machine for the social engineering attack detection model: SEADM //SAIEE Africa Research Journal. – 2018. – Т. 109, № 2. – С. 133–148. URL: https://ieeexplore.ieee.org/abstract/document/8531953
8. Луговець Д.В., Петренко А.Б. "СТРУКТУРА ВИЯВЛЕННЯ ФІШИНГОВИХ АТАК СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ." The 6th International scientific and practical conference... Cognum Publishing House, 2021. URL:

file:///C:/Users/Admin/Downloads/INTERNATIONAL-SCIENTIFIC-INNOVATIONS-IN-HUMAN-LIFE-15-17.12.2021%20(1).pdf

9. Halevi T., Memon N., Nov O. Spear-phishing in the wild: A real-world study of personality, phishing self-efficacy and vulnerability to spear-phishing attacks. – 2015. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2544742
10. Choi K., Lee J., Chun Y. Voice phishing fraud and its modus operandi //Security Journal. – 2017. – Т. 30. – С. 454–466. URL: https://link.springer.com/article/10.1057/sj.2014.49
11. Sokolov S. S. et al. Modern social engineering voice cloning technologies //2020 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus). – IEEE, 2020. – С. 513–516. URL: https://ieeexplore.ieee.org/abstract/document/9038954
12. Ulfath R. E. et al. Detecting smishing attacks using feature extraction and classification techniques //Proceedings of the International Conference on Big Data, IoT, and Machine Learning: BIM 2021. – Springer Singapore, 2022. – С. 677–689. URL: https://link.springer.com/chapter/10.1007/978-981-16-6636-0_51
13. Iuga C., Nurse J. R. C., Erola A. Baiting the hook: factors impacting susceptibility to phishing attacks //Human-centric Computing and Information Sciences. – 2016. – Т. 6. – С. 1–20. URL: https://link.springer.com/article/10.1186/s13673-016-0065-2
14. Bada M., Nurse J. R. C. The social and psychological impact of cyberattacks //Emerging cyber threats and cognitive vulnerabilities. – Academic Press, 2020. – С. 73–92. URL: https://www.sciencedirect.com/science/article/pii/B9780128162033000046
15. Велика мовна модель. Wikipedia. URL: https://uk.wikipedia.org/wiki/Велика_мовна_модель .
16. Schmitt, Marc, and Ivan Flechais. "Digital deception: Generative artificial intelligence in social engineering and phishing." Artificial Intelligence Review 57.12 (2024). p 3. URL: https://link.springer.com/article/10.1007/s10462-024-10973-2

17. Schmitt, Marc, and Ivan Flechais. "Digital deception: Generative artificial intelligence in social engineering and phishing." Artificial Intelligence Review 57.12 (2024). p 2. URL: https://link.springer.com/article/10.1007/s10462-024-10973-2
18. Koyun A., Al Janabi E. Social engineering attacks //Journal of Multidisciplinary Engineering Science and Technology (JMEST). – 2017. – Т. 4. – №. 6. – С. 7533–7538. URL: https://www.jmest.org/wp-content/uploads/JMESTN42352270.pdf
19. Saleem J., Hammoudeh M. Defense methods against social engineering attacks //Computer and network security essentials. – 2018. – С. 603–618. URL: https://link.springer.com/chapter/10.1007/978-3-319-58424-9_35
20. Ghafir I. et al. Social engineering attack strategies and defence approaches //2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud). – IEEE, 2016. – С. 145–149. URL: https://ieeexplore.ieee.org/abstract/document/7575856
21. Бойко В., Горбаченко С. Тестування на проникнення як ефективний інструмент менеджменту кібербезпеки // Інформаційні технології та суспільство. 2023. № 3 (9). Р. 23–29. URL: http://journals.maup.com.ua/index.php/it/article/view/2791
22. Mouton F., Leenen L., Venter H. S. Social engineering attack examples, templates and scenarios //Computers & Security. – 2016. – Т. 59. – С. 186–209. URL: https://www.sciencedirect.com/science/article/abs/pii/S0167404816300268
23. Greamo C., Ghosh A. Sandboxing and virtualization: Modern tools for combating malware //IEEE Security & Privacy. – 2011. – Т. 9. – №. 2. – С. 79–82. URL: https://ieeexplore.ieee.org/abstract/document/5739643
24. Хрипкова А. ДВОФАКТОРНА АУТЕНТИФІКАЦІЯ //ББК 32.971. 353я. – 2018. – С. 130. URL: https://surl.li/fsenla
25. Білан Л. О. Методи двофакторної автентифікації користувачів в мобільних пристроях. – 2021. URL: https://openarchive.nure.ua/server/api/core/bitstreams/7f481c42-5430-42bb-bfef-baa48c0cfaf8/content

26. Cybersecurity K. E. The Protection Technologies of Kaspersky Endpoint Security. URL: https://mediacircle.de/pdf/Protection_Technologies_Whitepaper.pdf
27. Шуліка К., Балагура Д., Смірнов А., Непокритов Д., Литвин А. Метод використання сучасних систем захисту кінцевих точок (EDR)... Innovative technologies and scientific solutions for industries. – 2024. URL:
28. Kiru M. U., Muhammad S. I. A situation analysis on cybercrime and its economic impact in Nigeria //International Journal of Computer Applications. – 2017. – Т. 975. – С. 8887. URL: https://itssi-journal.com/index.php/ittsi/article/view/495
29. Юдін О. К., Матвійчук-Юдіна О. В., Супрун О. М. "ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНА ВІЙНА ТА ТЕХНОЛОГІЇ СОЦІАЛЬНОГО ІНЖИНІРИНГУ." Science-Based Technologies 50.2 (2021). URL: https://surl.li/wqsycw
30. Цуркан О. В., Герасмов Р. П., Крук О. М. Методи протидії використанню соціальної інженерії. – 2019. URL: https://ela.kpi.ua/items/58e63fd4-62b9-4adb-8980-80a93f7a702e
31. Бойко В., Василенко М., Слатвінська В. Моделювання живучості та відновлення інформаційно-комунікаційних мереж в умовах дії кіберзагроз // Інформаційні технології та суспільство. 2024. № 1 (12). P. 13–19. URL: https://journals.maup.com.ua/index.php/it/article/view/3143
32. Половенко, Л. П., Мерінова С. В. "Виявлення ознак соціальної інженерії та технологія протидії соціальним хакерам на підприємстві." Підприємництво та інновації 10 (2019): 183–187. URL: file:///C:/Users/Admin/Downloads/255-Текст%20статті-365-2-10-20200422.pdf
33. Франчук, В. М. "Захист даних. Соціальна інженерія." Науковий часопис НПУ імені М. П. Драгоманова. Серія 2: Комп'ютерно-орієнтовані системи навчання 17 (2015): 20–26. URL: file:///C:/Users/Admin/Downloads/Nchnpu_2_2015_17_5.pdf
34. Тімченко, А. В. "Методика аудиту інформаційної безпеки на стійкість до атак соціальної інженерії." (2022). URL: https://essuir.sumdu.edu.ua/handle/123456789/89796

35. Ракович, Дарина Олександрівна. "Рефлексивний аналіз сценаріїв атак соціальної інженерії." (2021). URL: https://ela.kpi.ua/items/c56d32f3-c9ea-4fb3-bddf-0e97b8b16e79

36. Легомінова, С. В., та ін. "Тестування захищеності сучасних інформаційних систем: вибір ефективних методів та сценаріїв для різних об'єктів тестування." Сучасний захист інформації 4 (2023): 84–90. URL: https://journals.duikt.edu.ua/index.php/dataprotect/article/view/2835