

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**  
**КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ**  
**ІМЕНІ ВАДИМА ГЕТЬМАНА**  
**ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В ЕКОНОМІЦІ**

**Кафедра системного аналізу та кібербезпеки**

**ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА «КІБЕРБЕЗПЕКА»**  
**Галузь знань 12 «Інформаційні технології»**  
**Спеціальність 125 «Кібербезпека»**  
**Форма навчання: очна (денна)**

**КВАЛІФІКАЦІЙНА БАКАЛАВРСЬКА РОБОТА**

**на тему: «Дослідження соціального фактору у проблемі забезпечення**  
**інформаційної безпеки та вироблення рекомендацій щодо захисту інформації**  
**від соціотехнічних атак»**

Здобувача Козічевої Ірини Ігорівни

Науковий керівник: Професор Толюпа Сергій Васильович

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

Завідувач кафедри системного аналізу та кібербезпеки:  
д.ф.-м.н., професор Джалладова І.А.

**Київ 2024**

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

**ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В ЕКОНОМІЦІ**

**Кафедра системного аналізу та кібербезпеки**

**ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА «КІБЕРБЕЗПЕКА»**

**Галузь знань 12 «Інформаційні технології»**

**Спеціальність 125 «Кібербезпека»**

**ПОГОДЖЕНО**

Керівник проектної групи (гарант)  
освітньо-професійної програми  
«Кібербезпека»  
к. ф. — м. н. доцент Г.В. Мамонова  
\_\_\_\_\_ 2024 р.

**ЗАТВЕРДЖУЮ**

Завідувач кафедри системного аналізу  
та кібербезпеки  
д.ф.-м.н., професор Джалладова І.А.  
\_\_\_\_\_ 2024 р.

**ІНДИВІДУАЛЬНЕ ЗАВДАННЯ**

**здобувача вищої освіти Козічевої Ірини Ігорівни**

**денної форми навчання**

**на підготовку кваліфікаційної бакалаврської роботи**

**на тему «Дослідження соціального фактору у проблемі забезпечення  
інформаційної безпеки та вироблення рекомендацій щодо захисту інформації  
від соціотехнічних атак»**

**Тему затверджено наказом ректора Університету 30.04.2024 р. № 726-ст**

### План кваліфікаційної бакалаврської роботи

|                                                                                                                                                                                                                                                                                                                                         |                                                                                                                                                                                                                                                         |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Розділ 1                                                                                                                                                                                                                                                                                                                                | Розуміння соціотехнічних атак                                                                                                                                                                                                                           |
| Розділ 2                                                                                                                                                                                                                                                                                                                                | Людські фактори та довіра в інформаційній безпеці                                                                                                                                                                                                       |
| Розділ 3                                                                                                                                                                                                                                                                                                                                | Соціальні медіа та внутрішні загрози                                                                                                                                                                                                                    |
| Розділ 4                                                                                                                                                                                                                                                                                                                                | Стратегії захисту від соціотехнічних атак та тенденції майбутнього                                                                                                                                                                                      |
| Об'єкт дослідження:                                                                                                                                                                                                                                                                                                                     | Процес забезпечення інформаційної безпеки з урахуванням соціальних факторів.                                                                                                                                                                            |
| <b>Предмет дослідження:</b> методи захисту інформації від соціотехнічних атак та рекомендації щодо їх впровадження в інформаційну систему.                                                                                                                                                                                              |                                                                                                                                                                                                                                                         |
| <b>Мета кваліфікаційної бакалаврської роботи:</b> дослідження соціальних факторів у проблемі забезпечення інформаційної безпеки та розробка рекомендацій щодо захисту інформації від соціотехнічних атак.                                                                                                                               |                                                                                                                                                                                                                                                         |
| <b>Конкретні завдання, які здобувач повинен виконати для досягнення поставленої мети:</b><br>1. Проаналізувати типи та приклади соціотехнічних атак.<br>2. Дослідити вплив соціально-технічних атак на організації.<br>3. Визначити основні прийоми в соціотехнічних атаках.<br>4. Розробити стратегії захисту від соціотехнічних атак. |                                                                                                                                                                                                                                                         |
| У розділі 1                                                                                                                                                                                                                                                                                                                             | Дослідити та визначити соціотехнічні атаки. Проаналізувати їх вплив на організації. Описати загальні прийоми та психологічні тактики соціотехнічних атак. Вивчити приклади успішних атак.                                                               |
| У розділі 2                                                                                                                                                                                                                                                                                                                             | Вивчити людські помилки, що призводять до порушень безпеки. Описати програми навчання та підвищення обізнаності для співробітників. Дослідити роль організаційної культури та важливість довіри. Розглянути проблеми конфіденційності та захисту даних. |
| У розділі 3                                                                                                                                                                                                                                                                                                                             | Проаналізувати ризики використання соціальних медіа в контексті інформаційної безпеки. Дослідити внутрішні загрози та методи моніторингу працівників. Описати практики співпраці та обміну інформацією.                                                 |
| У розділі 4                                                                                                                                                                                                                                                                                                                             | Розробити рекомендації щодо захисту від соціотехнічних атак. Підготувати плани та протоколи реагування на інциденти. Дослідити технологічні рішення, використання штучного інтелекту та інтеграцію аналізу поведінки.                                   |

Завдання підготував  
науковий керівник

д.т.н., професор  
Толюпа С. В.

Завдання одержав  
здобувач

Козічева І. І.

## РЕФЕРАТ

Кваліфікаційна бакалаврська робота містить 85 сторінок, список літератури з 49 найменувань.

Перелік ключових слів: соціотехнічні атаки, соціальна інженерія, безпека інформації, двофакторна аутентифікація, внутрішні загрози, конфіденційність даних

Предмет дослідження: : методи захисту інформації від соціотехнічних атак та рекомендації щодо їх впровадження в інформаційну систему.

Об'єкт дослідження: Процес забезпечення інформаційної безпеки з урахуванням соціальних факторів.

Мета кваліфікаційної бакалаврської роботи полягає в проведенні комплексного аналізу соціальних аспектів соціотехнічних атак, визначити ключові фактори, що призводять до їх успішності, та розробити рекомендації щодо захисту інформації від таких загроз.

Завданням кваліфікаційної бакалаврської роботи є аналіз типів та прикладів соціотехнічних атак, дослідження впливу соціально-технічних атак на організації, визначення основних прийомів в соціотехнічних атаках та розробка стратегії захисту від соціотехнічних атак.

Рік виконання кваліфікаційної бакалаврської роботи 2024

Рік захисту кваліфікаційної бакалаврської роботи 2024

**ВІДГУК**  
**на кваліфікаційну бакалаврську роботу**  
**студентки Козічевої Ірини групи ІК-401**  
**на тему «Дослідження соціального фактору у проблемі**  
**забезпечення інформаційної безпеки та вироблення рекомендацій щодо**  
**захисту інформації від соціотехнічних атак»**

**Актуальність теми:** інформаційна безпека є критичною проблемою в сучасну цифрову епоху, коли зростає кількість соціально-технічних атак, націлених на окремих осіб, організації та уряди. Ці атаки використовують не лише технічні вразливості, але й соціальні фактори для отримання несанкціонованого доступу до конфіденційної інформації. Тому розуміння перетину технологій і людської поведінки має важливе значення для розробки ефективних стратегій захисту від цих загроз. Соціальні фактори, такі як людська помилка, недостатня обізнаність і тактика соціальної інженерії, відіграють значну роль в успіху соціотехнічних атак, підкреслюючи необхідність цілісного підходу до інформаційної безпеки. Досліджуючи вплив соціальних факторів на інформаційну безпеку, ми можемо виявити слабкі місця, які часто не помічаються традиційними заходами кібербезпеки.

Враховуючи перераховані фактори можна сміливо зтверджувати, що тема роботи актуальна і потребує детального дослідження.

**Повнота розкриття теми:** в даній роботі повністю виконані поставлені завдання, її обсяг та зміст відповідає задачам на бакалаврську кваліфікаційну роботу.

**Теоретичний рівень:** проведене дослідження свідчить про вміння автора опрацьовувати та аналізувати іншомовні видання, нормативні документи, технічну документацію, проводити аналіз, використовувати метод індукції та узагальнювати матеріал.

**Практичне значення роботи:** дотримуючись запропонованих рекомендацій, організації можуть значно зменшити свою вразливість до атак, які використовують як технічні, так і людські вразливості. Однією з ключових рекомендацій є впровадження багатофакторної автентифікації в усіх системах і платформах. Цей додатковий рівень безпеки може допомогти запобігти

несанкціонованому доступу до конфіденційної інформації, навіть якщо паролі зламано.

**Самостійність виконання роботи:** студентка показала здатність самостійно працювати з науково-технічною літературою, визначати вектор дослідження, знаходити та обробляти інформацію, має достатні теоретичні знання. Робота відповідає затвердженій темі, а всі етапи, затверджені календарним планом, були виконані у зазначений термін.

**Якість оформлення, загальна та спеціальна грамотність:** пояснювальна записка кваліфікаційної бакалаврської роботи написана якісно та в доступній для ознайомлення формі.

**Переваги та недоліки роботи:** завданням кваліфікаційної бакалаврської роботи є аналіз типів та прикладів соціотехнічних атак, дослідження впливу соціально-технічних атак на організації, визначення основних прийомів в соціотехнічних атаках та розробка стратегії захисту від соціотехнічних атак, що є необхідним в безпековій сфері.

У зв'язку з великою кількістю дослідницького матеріалу, студентка прагнула охопити якомога більше аспектів, що спричинило глибокий аналіз кожної частини. Однак, деякі питання могли бути розкриті більш детально.

**Загальна оцінка роботи та висновок щодо рекомендації до захисту в ЕК:** вважаю, що кваліфікаційна робота виконана на достатньо професійному рівні і студентка Козічева Ірина підтвердила свою підготовленість до самостійної роботи в галузі інформаційної безпеки, і заслуговує на оцінку «добре/82» та присвоєння йому ступеня бакалавра зі спеціальності «Кібербезпека».

Науковий керівник  
професор кафедри  
системного аналізу та  
кібербезпеки «Інститут  
інформаційних технологій в  
економіці»  
д.т.н., професор



(підпис)

Сергій ТОЛЮПА

(ініціали, прізвище)

«13» червня 2024 р.

**Рецензія на дипломну роботу Козічевої Ірини на тему  
«Дослідження соціального фактору у проблемі забезпечення  
інформаційної безпеки та вироблення рекомендацій щодо  
захисту інформації від соціотехнічних атак»**

Рецензент: *Олена Ткаченко*

Дата: 4 червня 2024 року

*1. Актуальність теми*

Тема дипломної роботи Козічевої Ірини є надзвичайно актуальною в сучасному світі, де все більше інформації зберігається та передається в електронному вигляді. Соціотехнічні атаки, які ґрунтуються на маніпулюванні людськими факторами, стають все більш поширеними та небезпечними. Дослідження соціального фактору у проблемі забезпечення інформаційної безпеки та вироблення рекомендацій щодо захисту інформації від соціотехнічних атак є необхідним для підвищення рівня кібербезпеки.

*2. Наукова новизна*

Дипломна робота Козічевої Ірини містить оригінальні дослідження соціального фактору у проблемі забезпечення інформаційної безпеки. Авторка проаналізувала різні типи соціотехнічних атак та визначила ключові фактори, які роблять людей уразливими до них. Авторка також розробила комплекс рекомендацій щодо захисту інформації від соціотехнічних атак. Ці рекомендації можуть бути корисними для організацій та окремих осіб, які прагнуть підвищити рівень кібербезпеки.

*3. Теоретична основа*

Дипломна робота Козічевої Ірини ґрунтується на сучасних наукових дослідженнях в галузі інформаційної безпеки та психології. Авторка використала широкий спектр джерел, включаючи наукові статті, книги та веб-сайти.

#### *4. Практична значимість*

Результати дослідження, представлені в дипломній роботі Козічевої Ірини, мають значну практичну цінність. Рекомендації щодо захисту інформації від соціотехнічних атак можуть бути використані для розробки та вдосконалення систем інформаційної безпеки в організаціях та на особистому рівні.

#### *5. Структура та зміст роботи*

Дипломна робота Козічевої Ірини добре структурована та легко читається. Вона складається з вступу, чотирьох розділів, висновків та списку використаних джерел. Кожен розділ присвячений окремій темі та логічно пов'язаний з іншими розділами.

#### *6. Науковий стиль*

Дипломна робота Козічевої Ірини написана науковим стилем. Авторка використовує чітку та лаконічну мову, уникає вживання сленгу та розмовних виразів.

#### *7. Зауваження та пропозиції*

Дипломна робота Козічевої Ірини виконана на високому науковому рівні. Авторка продемонструвала глибокі знання в галузі інформаційної безпеки та психології. Немає суттєвих зауважень до роботи.

#### **Висновок**

Дипломна робота Козічевої Ірини на тему «Дослідження соціального фактору у проблемі забезпечення інформаційної безпеки та вироблення рекомендацій щодо захисту інформації від соціотехнічних атак» заслуговує на оцінку «**відмінно**».



*Посемко О.В.*

## ЗМІСТ

|                                                                          |    |
|--------------------------------------------------------------------------|----|
| СПИСОК УМОВНИХ СКОРОЧЕНЬ.....                                            | 4  |
| ВСТУП .....                                                              | 5  |
| РОЗДІЛ 1. РОЗУМІННЯ СОЦІОТЕХНІЧНИХ АТАК .....                            | 7  |
| 1.1. Визначення і приклади соціотехнічних атак.....                      | 7  |
| 1.2. Вплив соціально-технічних атак на організації.....                  | 2  |
| 1.3 Загальні прийоми, що використовуються в соціотехнічних атаках .....  | 3  |
| 1.4. Огляд соціальної інженерії .....                                    | 4  |
| 1.5. Психологічні тактики в атаках соціальної інженерії .....            | 6  |
| 1.6. Дослідження успішних атак соціальної інженерії.....                 | 7  |
| 1.7. Висновки до розділу 1 .....                                         | 8  |
| РОЗДІЛ 2. ЛЮДСЬКІ ФАКТОРИ ТА ДОВІРА В ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ.....         | 10 |
| 2.1. Людські помилки, що призводять до порушень безпеки .....            | 10 |
| 2.2. Програми навчання та підвищення обізнаності для співробітників .... | 11 |
| 2.3. Роль організаційної культури в зменшенні людських помилок .....     | 13 |
| 2.4. Довіра та обман в інформаційній безпеці.....                        | 14 |
| 2.4.1. Важливість довіри до обміну інформацією.....                      | 15 |
| 2.5. Проблеми конфіденційності та захисту даних .....                    | 18 |
| 2.5.1. Регулювання конфіденційності .....                                | 20 |
| 2.5.2. Техніки шифрування та анонімізації даних .....                    | 21 |
| 2.5.3. Баланс між конфіденційністю та заходами безпеки.....              | 22 |
| 2.6. Висновки до розділу 2 .....                                         | 23 |
| РОЗДІЛ 3. СОЦІАЛЬНІ МЕДІА ТА ВНУТРІШНІ ЗАГРОЗИ .....                     | 25 |
| 3.1. Ризики соціальних медіа в інформаційній безпеці.....                | 25 |
| 3.1.1. Ризики, пов'язані з використанням соціальних мереж .....          | 26 |
| 3.1.2. Соціальна інженерія через платформи соціальних медіа .....        | 27 |
| 3.1.3. Найкращі практики безпечного використання соціальних медіа .....  | 28 |

|                                                                                                                                  |    |
|----------------------------------------------------------------------------------------------------------------------------------|----|
| 3.2. Внутрішні загрози та моніторинг працівників .....                                                                           | 29 |
| 3.2.1. Типи внутрішніх загроз.....                                                                                               | 30 |
| 3.2.2. Впровадження систем моніторингу співробітників та баланс між<br>конфіденційністю працівників та моніторингом безпеки..... | 31 |
| 3.3. Етичні міркування в ІБ та вирішення етичних дилем.....                                                                      | 34 |
| 3.4. Співпраця та обмін інформацією .....                                                                                        | 38 |
| 3.5. Висновки по розділу 3 .....                                                                                                 | 45 |
| РОЗДІЛ 4. СТРАТЕГІЇ ЗАХИСТУ ВІД СОЦІОТЕХНІЧНИХ АТАК ТА<br>ТЕНДЕНЦІЇ МАЙБУТНЬОГО .....                                            | 47 |
| 4.1. Рекомендації щодо захисту від соціально-технічних атак .....                                                                | 47 |
| 4.2. Впровадження багатофакторної автентифікації.....                                                                            | 49 |
| 4.3. Проведення регулярних тренінгів з питань безпеки та створення планів<br>і протоколів реагування на інциденти.....           | 51 |
| 4.5. Навчання та освіта з кібербезпеки .....                                                                                     | 2  |
| 4.6. Технологічні рішення для соціотехнічних атак та впровадження<br>розширених систем виявлення загроз.....                     | 5  |
| 4.7. Використання штучного інтелекту для моніторингу безпеки .....                                                               | 7  |
| 4.8. Інтеграція аналізу поведінки та реагування на інциденти .....                                                               | 2  |
| 4.9. Тренування безпеки, симуляції, постійний моніторинг та оцінка.....                                                          | 4  |
| ВИСНОВКИ.....                                                                                                                    | 10 |
| СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ.....                                                                                                  | 13 |
| ДОДАТКИ                                                                                                                          |    |
| ДОДАТОК А                                                                                                                        |    |

## СПИСОК УМОВНИХ СКОРОЧЕНЬ

ІБ – інформаційна безпека

ІС – інформаційна система

ІІІ – штучний інтелект

ССРА – каліфорнійський закон про конфіденційність споживачів (від англ. California Consumer Privacy Act)

GDPR – загальний регламент захисту даних (від англ. General Data Protection Regulation)

MFA – багатофакторна автентифікація (від англ. Multi-Factor Authentication)

VPM – віртуальні приватні мережі (від англ. Virtual Private Network)

SSL – рівень захищених сокетів (від англ. Secure Sockets Layer)

## ВСТУП

Інформаційна безпека є критичною проблемою в сучасну цифрову епоху, коли зростає кількість соціально-технічних атак, націлених на окремих осіб, організації та уряди. Ці атаки використовують не лише технічні вразливості, але й соціальні фактори для отримання несанкціонованого доступу до конфіденційної інформації. Тому розуміння перетину технологій і людської поведінки має важливе значення для розробки ефективних стратегій захисту від цих загроз. Соціальні фактори, такі як людська помилка, недостатня обізнаність і тактика соціальної інженерії, відіграють значну роль в успіху соціотехнічних атак, підкреслюючи необхідність цілісного підходу до інформаційної безпеки. Досліджуючи вплив соціальних факторів на інформаційну безпеку, ми можемо виявити слабкі місця, які часто не помічаються традиційними заходами кібербезпеки. Наприклад, добре спроектована технічна система все ще може бути скомпрометована, якщо користувачі не будуть належним чином навчені розпізнавати фішингові електронні листи чи інші типи тактик соціальної інженерії. Це підкреслює важливість включення людського фактору в розробку та впровадження протоколів безпеки. Комплексний підхід до інформаційної безпеки повинен враховувати психологічні, культурні та організаційні аспекти, які можуть впливати на поведінку людей і прийняття рішень у цифровій сфері. Для ефективного пом'якшення ризиків, пов'язаних із соціотехнічними атаками, організації повинні розробити політику безпеки, яка враховує соціальні чинники разом із технічними вразливими місцями. Це може включати впровадження навчальних програм з підвищення обізнаності, проведення регулярних перевірок безпеки та виховання культури безпеки в організації. Сприяючи кращому розумінню того, як соціальні фактори впливають на інформаційну безпеку, організації можуть краще захистити свої дані та системи від нових загроз. Співпраця з експертами з психології, соціології та поведінкових

наук може надати цінну інформацію про моделі людської поведінки, які можуть допомогти розробити надійніші стратегії безпеки.

Окрім технологічних гарантій, врахування соціальних факторів має вирішальне значення для підвищення інформаційної безпеки. Атаки соціальної інженерії, коли зловмисники використовують вразливі місця людини, щоб отримати доступ до конфіденційної інформації, стають все більш поширеними в епоху цифрових технологій. Розуміючи психологічну тактику, яку використовують зловмисники, організації можуть краще навчити своїх співробітників і зацікавлених сторін розпізнавати та припиняти такі атаки. Крім того, виховання культури безпеки всередині організації може створити колективне розуміння важливості інформаційної безпеки, що призведе до підвищеної пильності та ретельного вивчення потенційних загроз. Крім того, розгляд соціальних факторів в ІБ також передбачає визнання ролі індивідуальної поведінки та мотивації. Недбалість або навмисна неправомірна поведінка співробітників може становити серйозні ризики для безпеки організаційних даних. Запровадження політики, яка стимулює відповідальне поводження з інформацією та санкціонує безвідповідальну поведінку, може допомогти зменшити ці ризики. Крім того, сприяння почуттю власності та підзвітності серед працівників щодо захисту даних може стимулювати більш проактивний підхід до безпеки [18]. Зрештою, комплексний підхід до інформаційної безпеки має виходити за рамки технологічних заходів і звертати увагу на людський фактор. Визнаючи вплив соціальних факторів на організаційну безпеку, компанії можуть розробити ефективніші стратегії захисту своїх даних і систем. Інтеграція тренінгів із соціальної інженерії, просування орієнтованої на безпеку культури та стимулювання відповідальної поведінки є ключовими компонентами посилення захисту інформаційної безпеки. Підкреслення людського аспекту в заходах кібербезпеки є незамінним у сучасному складному та взаємопов'язаному цифровому ландшафті.

## РОЗДІЛ 1. РОЗУМІННЯ СОЦІОТЕХНІЧНИХ АТАК

### 1.1. Визначення і приклади соціотехнічних атак

Щоб повністю зрозуміти соціотехнічні атаки, важливо спочатку зрозуміти саму концепцію. Соціотехнічні атаки можна визначити як комбінацію соціальних і технічних елементів для використання вразливостей у системі. Ці атаки передбачають маніпулювання окремими особами чи організаціями за допомогою психологічних тактик, таких як соціальна інженерія, з метою отримання несанкціонованого доступу до конфіденційної інформації чи систем. Використовуючи як людську поведінку, так і технічні вразливості, зловмисники можуть ефективно обійти традиційні заходи безпеки та завдати значної шкоди цільовим об'єктам. Одним із ключових аспектів соціотехнічних атак є опора на людський фактор у виконанні атак. Зловмисники часто використовують психологічні принципи, щоб змусити людей розкрити конфіденційну інформацію або вчинити дії, що ставлять під загрозу безпеку. Ця маніпуляція людською поведінкою є ключовим компонентом соціотехнічних атак, оскільки дозволяє зловмисникам обійти технічні засоби захисту та отримати несанкціонований доступ. Розуміння психологічної тактики, яка використовується в цих атаках, має важливе значення для розробки ефективних контрзаходів для пом'якшення ризику, пов'язаного з соціотехнічними загрозами. Підсумовуючи, соціотехнічні атаки представляють величезний виклик для фахівців з інформаційної безпеки через поєднання тактик соціальної інженерії та технічних експлойтів. Для ефективного захисту від цих атак організації повинні прийняти цілісний підхід, який усуває як технічну вразливість, так і людський фактор. Впроваджуючи надійні заходи безпеки, забезпечуючи всебічне навчання співробітників і розвиваючи культуру безпеки, організації можуть значно знизити ризик стати жертвою соціотехнічних атак. Розгляд складної взаємодії між соціальними та технічними елементами має

вирішальне значення для захисту конфіденційної інформації та систем від зловмисників.

Для ефективної боротьби з соціотехнічними атаками вкрай важливо розуміти взаємопов'язану природу соціальних і технічних факторів, що сприяють цим загрозам. Тактика соціальної інженерії, як-от фішингові електронні листи або текстові повідомлення, використовує людську психологію та довіру, щоб змусити людей розголошувати конфіденційну інформацію або виконувати дії, які порушують заходи безпеки. Ці напади часто ґрунтуються на природному прагненні довіряти іншим або на страху наслідків за непідкорення явним авторитетам. Окрім методів соціальної інженерії, технічними вразливими місцями в системах також можна маніпулювати, щоб сприяти соціотехнічним атакам. Зловмисники можуть використати слабкі сторони програмного забезпечення, апаратного забезпечення чи мережевих конфігурацій, щоб отримати несанкціонований доступ або завдати шкоди критично важливим системам. Крім того, зростаюча залежність від цифрових технологій як в особистому, так і в професійному середовищі посилила потенційний вплив соціотехнічних атак. З поширенням взаємопов'язаних пристроїв і онлайн-сервісів поверхня для атаки зловмисників розширилася. Цей взаємозв'язок надає зловмисникам широкі можливості для використання вразливостей у багатьох точках соціально-технічної системи, створюючи значні проблеми для захисників. Оскільки організації прагнуть підтримувати надійні позиції безпеки, вкрай важливо визнати складну взаємодію між людською поведінкою, технологічною інфраструктурою та організаційною політикою, яка лежить в основі соціотехнічних атак. Комплексно вирішуючи ці взаємопов'язані фактори, організації можуть підвищити свою стійкість проти нових загроз. Для ефективного захисту від соціотехнічних атак організації повинні віддати перевагу всебічному підходу, який поєднує як технічні засоби захисту, так і ініціативи соціальної обізнаності. Застосування надійних заходів кібербезпеки, таких як протоколи шифрування, багатофакторна автентифікація та регулярні оцінки безпеки, може допомогти зменшити технічні вразливості, які можуть бути

використані в цих атаках. Одночасно культивування міцної культури обізнаності про безпеку серед співробітників за допомогою навчальних програм, симуляції фішингових вправ і чіткого повідомлення про політику може допомогти зміцнити механізми захисту від тактик соціальної інженерії. Підтримуючи комплексну безпеку, яка стосується як технічних, так і соціальних аспектів, організації можуть краще захистити свої активи та дані від поширеної загрози соціотехнічних атак. [19]

У сучасному взаємопов'язаному цифровому ландшафті соціотехнічні атаки стали значною загрозою для ІБ. Ці атаки використовують як соціальні, так і технічні аспекти цільової системи, щоб використовувати вразливості та зламати конфіденційні дані. Одним із поширених прикладів соціально-технічної атаки є фішинг, коли зловмисники маніпулюють людською психологією, щоб обманом змусити людей розкрити конфіденційну інформацію або вчинити зловмисні дії. Поєднуючи складні технічні навички з тактикою соціальної інженерії, кіберзлочинці можуть обійти традиційні заходи безпеки та з легкістю проникнути в організації. Іншим прикладом соціотехнічної атаки є використання соціальних мереж для збору особистої інформації для крадіжки особистих даних або цілеспрямованих кібератак. Зловмисники можуть використовувати загальнодоступну інформацію на таких платформах, як Facebook або LinkedIn, щоб створювати переконливі фішингові електронні листи, призначені для конкретних осіб в організації. Такий підхід дозволяє зловмисникам створювати дуже персоналізовані повідомлення, що підвищує ймовірність успішного проникнення. Крім того, платформи соціальних медіа також служать живильним середовищем для розповсюдження шкідливих програм, що ще більше ускладнює ландшафт кібербезпеки. Організації повинні бути пильними, повідомляючи співробітникам про ризики, пов'язані з надмірним поширенням інформації в соціальних мережах, щоб пом'якшити потенційний вплив соціотехнічних атак. Підсумовуючи, соціотехнічні атаки підкреслюють складну взаємодію між людською поведінкою та технологічними вразливими місцями у сфері кібербезпеки. Оскільки цифрові

технології продовжують розвиватися, очікується, що витонченість і частота цих атак зростатимуть. Щоб ефективно захищатися від соціально-технічних атак, організації повинні запровадити цілісний підхід, який стосується як технічних, так і соціальних аспектів кібербезпеки. Це включає інвестиції в надійні заходи безпеки, проведення регулярних тренінгів із тактики соціальної інженерії та сприяння культурі обізнаності щодо кібербезпеки серед співробітників. Приймавши проактивну та комплексну стратегію, організації можуть посилити свій захист від соціально-технічних атак і захистити свою конфіденційну інформацію від зловмисників.

У контексті подолання соціотехнічних атак в інформаційній безпеці, висновки дослідження [3] щодо інформаційної безпеки України в умовах військової агресії виявляють критичну роль культури в захисті суспільства. Розуміння факторів, що впливають на інформаційну безпеку, і наслідків збою підкреслює потребу в надійному механізмі захисту. Крім того, дослідження, проведене [4], вивчає поведінку медичних працівників у сфері інформаційної безпеки в умовах лікарні, проливаючи світло на загальні вразливості та найкращі практики. Враховуючи результати цих досліджень, рекомендації щодо захисту від соціотехнічних атак можна покращити, зосередивши увагу на покращенні поведінки користувачів, запровадженні ефективних засобів контролю безпеки та вихованні культури усвідомлення інформаційної безпеки. Крім того, враховуючи різні мотиви, що стоять за поведінкою в сфері інформаційної безпеки, висвітлену в [4], інтеграція теорії мотивації захисту і загальної теорії стримування стає вирішальною для розробки цільових рекомендацій. Керівники лікарень могли б використовувати ці теоретичні перспективи для розробки індивідуальних програм інформаційної безпеки, які резонували б із медичними працівниками, зрештою зміцнюючи загальну безпеку.

## **1.2. Вплив соціально-технічних атак на організації**

У все більш взаємопов'язаному середовищі сучасних організацій вплив соціально-технічних атак не можна недооцінювати. Ці атаки, які використовують як соціальні, так і технічні вразливості, можуть завдати суттєвої шкоди репутації організації, фінансовій стабільності та загальній діяльності. Однією з ключових проблем, пов'язаних із соціотехнічними атаками, є їх здатність обійти традиційні заходи кібербезпеки, націлившись на людський елемент в організації. Цей людський фактор створює рівень складності, який може ускладнити організаціям ефективне виявлення та пом'якшення таких атак. Крім того, соціотехнічні атаки часто включають складні тактики соціальної інженерії, які використовують довіру та психологічну вразливість людей. Маніпулюючи співробітниками, які нічого не підозрюють, змушуючи їх розголошувати конфіденційну інформацію або надавати несанкціонований доступ, зловмисники можуть проникнути в системи організації з руйнівними наслідками. Поєднання соціальної маніпуляції та технічної експлуатації робить соціотехнічні атаки особливо підступними, оскільки вони можуть обійти навіть найнадійніший технологічний захист. В результаті компанії повинні не тільки інвестувати в передові інструменти кібербезпеки, але й надавати пріоритет навчанню і програмам підвищення обізнаності співробітників, щоб зменшити ризик стати жертвою цих атак. У світлі багатогранного характеру соціотехнічних атак, організації повинні прийняти цілісний підхід до кібербезпеки, який усуває як технічну вразливість, так і тактику соціальної інженерії. Цей підхід має охоплювати комбінацію технологічних рішень, таких як мережевий моніторинг, шифрування та контроль доступу, а також суворі політики та процедури для управління та захисту конфіденційної інформації. Крім того, виховання культури обізнаності щодо кібербезпеки та пильності серед співробітників має важливе значення для ефективного захисту від соціально-технічних атак. Інтегруючи соціальні чинники в свою загальну стратегію кібербезпеки, організації можуть підвищити свою стійкість проти цього

середовища загроз, що розвивається, і захистити свої важливі активи від експлуатації та маніпуляцій.

### **1.3 Загальні прийоми, що використовуються в соціотехнічних атаках**

У сфері соціотехнічних атак існує кілька поширених методів, які загрожують акторам використовувати вразливі місця як у людській поведінці, так і в технологічних системах. Одним із таких методів є фішинг, коли зловмисники використовують тактику соціальної інженерії, щоб обманом змусити людей розкрити конфіденційну інформацію, таку як паролі чи фінансові дані. Ці фішингові електронні листи часто здаються законними та спонукають одержувачів негайно вжити заходів, граючи на таких емоціях, як страх чи цікавість, щоб змусити їх потрапити на схему. Ще одна поширена техніка – це текстинг, який передбачає формування хибного почуття довіри до цілей шляхом фабрикування сценарію чи ідентифікації, щоб отримати від них інформацію. Це може включати видавання себе за довірену особу чи установу для отримання доступу до конфіденційних даних. Крім того, байтинг — це ще одна тактика, яка часто використовується в соціотехнічних атаках, коли зловмисники пропонують щось привабливе, як-от безкоштовне завантаження чи приз, щоб спонукати жертву перейти за шкідливими посиланнями або завантажити зловмисне програмне забезпечення на їхні системи. Ця техніка полює на прагнення людей отримати миттєве задоволення, використовуючи їхню готовність спілкуватися з невідомими джерелами. Ці стратегії спрямовані на маніпулювання як людською психологією, так і функціональністю технологій, щоб порушити заходи безпеки та отримати несанкціонований доступ до конфіденційної інформації. Розуміючи ці загальні методи, окремі особи та організації можуть краще підготуватися до потенційних соціально-технічних загроз і впровадити надійні заходи безпеки для ефективного пом'якшення ризиків. У відповідь на зростаючу поширеність соціотехнічних атак окремим особам і організаціям вкрай важливо бути в курсі цих оманливих тактик.

Така обізнаність може допомогти людям розпізнавати підозрілі електронні листи, повідомлення чи запити, надаючи їм змогу проявляти обережність і скептицизм під час зустрічі з потенційними загрозами. Крім того, запровадження навчальних програм безпеки та дотримання суворих протоколів безпеки в організаціях може допомогти зменшити ризики, пов'язані з соціотехнічними атаками. Розвиваючи культуру обізнаності про кібербезпеку та заохочуючи співробітників до пильної поведінки, підприємства можуть активно захищати себе від тактик соціальної інженерії та пом'якшувати потенційний вплив цих атак. Загалом комплексний підхід, який поєднує технологічні рішення з людською пильністю, має важливе значення для захисту від соціально-технічних загроз, що розвиваються, у сучасному взаємопов'язаному світі.

#### **1.4. Огляд соціальної інженерії**

Оскільки організації продовжують інвестувати в технологічні рішення для підвищення своєї інформаційної безпеки, важливо визнати вирішальну роль, яку соціальна інженерія відіграє у використанні вразливостей. Методи соціальної інженерії маніпулюють поведінкою людей, щоб отримати несанкціонований доступ до конфіденційної інформації або систем. Зловмисники часто використовують психологічні принципи, щоб змусити людей розкрити конфіденційні облікові дані чи зловмисну діяльність. Щоб пом'якшити ризики, пов'язані з атаками соціальної інженерії, організації повинні визначити пріоритетність програм інформування та навчання працівників. Покращуючи знання персоналу щодо виявлення підозрілих дій і практикуючи безпечну поведінку, компанії можуть значно зменшити ймовірність стати жертвою тактики соціальної інженерії. Крім того, впровадження надійних заходів безпеки, таких як багатофакторна автентифікація та контроль доступу, може служити додатковим рівнем захисту від атак соціальної інженерії. Ці технічні засоби захисту можуть допомогти пом'якшити вплив людської помилки та запобігти спробам

неавторизованого доступу. Крім того, організації повинні проводити регулярні оцінки безпеки та тестування на проникнення, щоб виявити потенційні слабкі місця, які можна використати за допомогою тактики соціальної інженерії. Проактивно оцінюючи та усуваючи вразливості, компанії можуть покращити загальну безпеку та захистити від соціально-технічних атак. Оскільки ландшафт загроз продовжує розвиватися, організаціям вкрай необхідно прийняти проактивний підхід до захисту своїх інформаційних активів від загроз соціальної інженерії. Підсумовуючи, соціальна інженерія становить значну загрозу ІБ, і організації повинні прийняти багатогранний підхід для ефективної боротьби з цією загрозою. Інтегруючи засоби технічного контролю з програмами підвищення обізнаності співробітників і регулярними оцінками безпеки, компанії можуть створити надійну систему безпеки, яка зменшує ризики, пов'язані з атаками соціальної інженерії. Для організацій вкрай важливо інвестувати в постійне навчання та освіту, щоб надати співробітникам знання та навички, необхідні для виявлення потенційних загроз і ефективного реагування на них. Віддаючи пріоритет цілісному підходу до інформаційної безпеки, організації можуть підвищити свою стійкість проти соціально-технічних атак і захистити свої цінні активи від зловмисників. [20] Оскільки засоби інформаційної безпеки стають дедалі надійнішими, кіберзловмисники звернулися до тактики соціальної інженерії, щоб використовувати найслабшу ланку будь-якої системи – людський елемент. Соціальна інженерія передбачає маніпулювання особами, щоб вони розголошували конфіденційну інформацію або вчиняли дії, що ставлять під загрозу безпеку. Цього можна досягти за допомогою різних засобів, таких як фішингові електронні листи, претекстинг або навіть видавання себе за іншу особу. Зловмисники використовують психологічну тактику, щоб використовувати людські схильності, такі як довіра, авторитет або цікавість, щоб обійти засоби технічного контролю безпеки [17]. Однією з головних проблем у боротьбі з атаками соціальної інженерії є складність їх виявлення. На відміну від традиційних кіберзагроз, які залишають цифрові сліди, соціотехнічні атаки часто маскуються

під законні взаємодії, що ускладнює їх ідентифікацію. Організації повинні інвестувати в навчальні програми, щоб пояснити співробітникам небезпеку соціальної інженерії та надати їм можливості розпізнавати потенційні загрози та ефективно реагувати на них [18]. Підвищуючи обізнаність і розвиваючи культуру пильності, компанії можуть значно зменшити свою вразливість до цих підступних атак. Підсумовуючи, соціальна інженерія представляє багатогранну загрозу ІБ, яка потребує цілісного підходу до пом'якшення. У той час як технологічні рішення відіграють вирішальну роль у захисті систем, урахування людського фактору є не менш важливим. Розуміючи методи та мотиви атак соціальної інженерії та впроваджуючи надійні протоколи безпеки, організації можуть краще захистити себе від цих маніпулятивних тактик. Постійна освіта, обізнаність і проактивне мислення щодо безпеки є важливими компонентами боротьби із соціальною інженерією в сучасному цифровому середовищі, яке все більше взаємопов'язане.

### **1.5. Психологічні тактики в атаках соціальної інженерії**

У сфері інформаційної безпеки розуміння психологічних тактик, що застосовуються в атаках соціальної інженерії, має першорядне значення. Атаки технічної соціальної інженерії використовують комбінацію людської психології, довіри та вразливості для зламу систем безпеки [12]. На відміну від традиційної соціальної інженерії, ці атаки використовують технологічні засоби, щоб змусити людей розкрити конфіденційну інформацію або порушити заходи безпеки. Алгоритми машинного навчання, такі як дерева рішень і випадкові ліси, відіграють вирішальну роль у виявленні цих складних атак шляхом аналізу даних мережевих хостів для потенційних індикаторів. Це підкреслює важливість інтеграції передових технологічних рішень із розумінням тактики психологічної маніпуляції для ефективної боротьби із загрозами соціальної інженерії, що розвиваються. Крім того, підкреслює поширеність тактики соціальної інженерії як у фізичному, так і у віртуальному середовищах, наголошуючи на необхідності всебічного порівняння

стратегій і контрзаходів [13]. Вивчаючи нюанси атак соціальної інженерії в різних контекстах, дослідники можуть отримати цінну інформацію про основні психологічні принципи, які використовують зловмисники. Цей порівняльний аналіз може слугувати основою для розробки надійних заходів безпеки, спрямованих на вирішення багатогранних проблем, які створює соціальна інженерія. Очевидно, що детальне розуміння психологічної тактики, яка використовується в атаках соціальної інженерії, має важливе значення для розробки ефективних стратегій запобігання та пом'якшення наслідків, які охоплюють як технологічні рішення, так і людський фактор. Крім того, дослідження тактики соціальної інженерії проливають світло на складну взаємодію між людською поведінкою та технологіями в контексті кібербезпеки. Визнаючи маніпулятивні методи, які використовують соціальні інженери для використання довіри та когнітивних упереджень, організації можуть запровадити цільові навчальні програми та ініціативи з підвищення обізнаності, щоб зменшити ризики, пов'язані з такими атаками. Поєднання технологічного захисту та психологічної обізнаності може значно підвищити стійкість організації проти прийомів соціальної інженерії, захищаючи конфіденційну інформацію та критично важливі системи від несанкціонованого доступу. Зрештою, цілісний підхід, який поєднує психологічне розуміння з передовими технологічними рішеннями, має вирішальне значення для зміцнення захисту від загроз соціальної інженерії, що розвиваються.

### **1.6. Дослідження успішних атак соціальної інженерії**

Одне дослідження, яке є прикладом успіху атак соціальної інженерії, включало фішингову кампанію, спрямовану на велику фінансову установу. Завдяки ретельному дослідженню та створенню переконливих електронних листів хакерам вдалося обманом змусити співробітників розкрити конфіденційну інформацію, таку як облікові дані для входу та реквізити рахунку. Це порушення призвело до значних фінансових втрат і заплямованої репутації організації. Це

підкреслює ефективність тактики соціальної інженерії у використанні слабких місць людини для отримання несанкціонованого доступу до систем і даних. В іншому випадку атака соціальної інженерії на медичний заклад призвела до компрометації карт пацієнтів та медичної інформації. Видаючи себе за ІТ-техніка, зловмисник отримав фізичний доступ до серверів закладу та встановив шкідливе програмне забезпечення, яке дозволяло витягувати конфіденційні дані. Цей випадок підкреслює необхідність жорсткого контролю доступу та процедур перевірки, щоб запобігти маскуванню неавторизованих осіб під законного персоналу [21]. Ці тематичні дослідження демонструють потенційний вплив успішних атак соціальної інженерії та підкреслюють критичну важливість навчання співробітників виявленню таких загроз і реагування на них. Організації повинні запроваджувати комплексні програми підвищення обізнаності щодо безпеки, щоб навчити персонал тактиці, яку використовують зловмисники, і надати їм можливість діяти як перша лінія захисту від атак соціальної інженерії. Розвиваючи культуру пильності та сприяючи проактивному підходу до безпеки, підприємства можуть зменшити ризик стати жертвою тактики соціальної інженерії та захистити свою конфіденційну інформацію від використання.

### **1.7. Висновки до розділу 1**

Соціально-технічні атаки — це комбінація соціальних і технічних методів, спрямованих на використання вразливостей системи для отримання несанкціонованого доступу до конфіденційної інформації або систем. Ці атаки включають маніпулювання психологічною поведінкою людей за допомогою соціальної інженерії, а також використання технічних недоліків програмного та апаратного забезпечення. Одним із ключових аспектів соціотехнічних атак є покладення на людський фактор для обходу традиційних заходів безпеки.

Ефективна боротьба з цими атаками вимагає комплексного підходу, який включає як технічні засоби захисту, так і обізнаність працівників про ризики

соціальної інженерії. Організаціям слід інвестувати в такі надійні технологічні рішення, як шифрування даних і багатофакторна автентифікація, а також регулярні оцінки безпеки та навчання персоналу.

Поширені методи атак соціальної інженерії включають фішинг, текстові повідомлення та різні методи соціальної інженерії, які використовують довіру, страх або цікавість людей. Зокрема, фішингові листи та маніпуляції через соціальні мережі є одними з найефективніших методів, які дозволяють зловмисникам отримати доступ до конфіденційної інформації.

Організації повинні розробляти та впроваджувати стратегії, які враховують як технічні аспекти безпеки, так і поведінку людини. Це включає регулярне навчання співробітників, проведення моделювання фішингових атак і впровадження чітких політик безпеки. Прийняття такого цілісного підходу зменшує ризики, пов'язані з атаками соціальної інженерії, і захищає конфіденційну інформацію від зловмисників.

## **РОЗДІЛ 2. ЛЮДСЬКІ ФАКТОРИ ТА ДОВІРА В ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ**

### **2.1. Людські помилки, що призводять до порушень безпеки**

У сфері інформаційної безпеки вплив людського фактора не можна переоцінити. Особи в організації можуть несвідомо порушити безпеку через такі дії, як обмін паролем або стати жертвою атак соціальної інженерії. Крім того, людські помилки залишаються однією з основних причин порушень безпеки, підкреслюючи критичну потребу в підвищенні обізнаності та освіти серед персоналу. Навчальні програми, які зосереджуються на найкращих практиках кібербезпеки та потенційних вразливостях, можуть надати співробітникам можливість стати активними учасниками захисту конфіденційної інформації. Культивуєючи культуру свідомості безпеки, організації можуть значно зменшити ризики, пов'язані з людським фактором для інформаційної безпеки. Окрім навчання, впровадження надійних політик і процедур може допомогти пом'якшити вплив людської помилки на інформаційну безпеку. Чіткі вказівки щодо обробки даних, контролю доступу та звітування про інциденти можуть надати співробітникам структуру для дотримання, зменшуючи ймовірність ненавмисних порушень безпеки [22]. Регулярні перевірки та оцінки безпеки також можуть допомогти виявити слабкі місця та вчасно виправити їх, перш ніж їх використають. Встановивши цілісну стратегію безпеки, яка наголошує як на технологічних рішеннях, так і на практиці, орієнтованій на людину, організації можуть покращити загальну безпеку та краще захистити від потенційних загроз. Зрештою, звернення до людського фактору в ІБ вимагає багатогранного підходу, який поєднує в собі технологічні інструменти, забезпечення виконання політики та індивідуальну підзвітність. Організації повинні усвідомлювати, що люди є водночас життєво важливим активом і потенційною вразливістю, коли йдеться про захист

конфіденційних даних. Інвестуючи в комплексні навчальні програми, впроваджуючи чітку політику та розвиваючи культуру пильності, організації можуть ефективно боротися з ризиками, пов'язаними з людським фактором для інформаційної безпеки.

У сфері інформаційної безпеки людські помилки відіграють значну роль у виникненні порушень безпеки. Ці помилки можуть проявлятися в різних формах, наприклад стати жертвою тактики соціальної інженерії, ненавмисного обміну конфіденційною інформацією або нехтування оновленням протоколів безпеки. Згідно з дослідженням Ponemon Institute, недбалість залишається основною причиною витоку даних, підкреслюючи критичну потребу для організацій урахувати людський фактор у своїх заходах безпеки. У багатьох випадках співробітники можуть бути недостатньо навчені найкращим практикам кібербезпеки, що призводить до ненавмисних помилок, які потенційно можуть скомпрометувати всю систему. Крім того, дедалі складніша технологія та динамічний характер робочого середовища сприяють людським помилкам, які можуть призвести до порушень безпеки. Співробітники можуть виявитися приголомшеними різноманітністю інструментів і технологій, які вони повинні використовувати, що призводить до помилок, якими можуть скористатися хакери. Крім того, вимога дотримуватись стислих термінів і квот може призвести до того, що люди будуть обмежуватися або нехтувати протоколами безпеки на користь ефективності, створюючи вразливі місця в системі [23]. Організаціям вкрай важливо забезпечити постійне навчання та підтримку, щоб переконатися, що співробітники готові ефективно справлятися зі змінними викликами кібербезпеки.

## **2.2. Програми навчання та підвищення обізнаності для співробітників**

Широко визнано, що людські помилки є значним фактором, що сприяє порушенням кібербезпеки в організаціях. Програми навчання та підвищення обізнаності для співробітників відіграють вирішальну роль у зниженні цих ризиків,

озброюючи персонал знаннями та навичками, необхідними для виявлення потенційних загроз безпеці та реагування на них. Проводячи для співробітників регулярні тренінги з найкращих практик кібербезпеки, організації можуть створити культуру обізнаності про безпеку, яка пронизує всю робочу силу. Це не лише допомагає запобігти інцидентам із безпекою, але й сприяє усвідомленню відповідальності серед працівників щодо захисту конфіденційної інформації та активів компанії. Крім того, включення реалістичних сценаріїв і симуляційних вправ у навчальні програми може підвищити залученість співробітників і збереження ключових концепцій безпеки. Інтерактивні семінари та імітація кібератак можуть надати співробітникам практичний досвід розпізнавання та нейтралізації потенційних загроз у контрольованому середовищі. Таке практичне навчання може значно підвищити ефективність заходів безпеки в організації, оскільки співробітники стають більш вправними у виявленні підозрілих дій і належному реагуванні на інциденти безпеки. Крім того, періодичні курси підвищення кваліфікації можуть служити нагадуванням співробітникам про важливість збереження пильності перед обличчям нових кіберзагроз [24]. На закінчення, інвестування у комплексні програми навчання та підвищення обізнаності для співробітників є стратегічним імперативом для організацій, які прагнуть зміцнити свій захист від соціотехнічних атак. Озброївши співробітників знаннями та навичками, необхідними для виявлення та пом'якшення ризиків безпеці, організації можуть значно зменшити свою вразливість до кіберзагроз. Програми навчання мають бути адаптовані до конкретних потреб і ролей співробітників, гарантуючи, що вони готові ефективно впоратися з потенційними інцидентами безпеки. Зрештою, добре навчена робоча сила, яка піклується про безпеку, є критично важливим активом для захисту цифрових активів організації та підтримки надійної системи безпеки у все більш взаємопов'язаному світі.

### 2.3. Роль організаційної культури в зменшенні людських помилок

Організаційна культура відіграє вирішальну роль у зменшенні людських помилок всередині організації. Сильний наголос на культурі відкритого спілкування та прозорості може створити середовище, в якому працівники почуватимуться комфортно, повідомляючи про помилки, не боячись покарання. Це може призвести до раннього виявлення та вирішення помилок до того, як вони переростуть у більші порушення безпеки. Крім того, культура, яка цінує навчання на помилках і заохочує постійне вдосконалення, може допомогти запобігти помилкам у майбутньому. Розвиваючи культуру, яка надає пріоритет співпраці та спільній відповідальності, організації можуть зменшити ймовірність людських помилок, що загрожують ІБ. Крім того, організаційна культура може впливати на поведінку працівників і прийняття рішень, що може вплинути на ймовірність людських помилок. Культура, яка сприяє підзвітності та дотриманню встановлених політик і процедур, може допомогти зменшити ризик помилок, спричинених недбалістю чи необережністю. Співробітники, які мають повноваження брати на себе відповідальність за свої дії, швидше за все, проявлятимуть обережність і старанність у виконанні своїх завдань, зводячи до мінімуму можливість виникнення помилок. Поєднуючи організаційні цінності із зобов'язанням дотримуватись стандартів інформаційної безпеки, організації можуть створити культуру, яка підсилює важливість запобігання помилкам і заохочує людей віддавати пріоритет безпеці у своїй повсякденній діяльності [25]. Підсумовуючи, організаційна культура є критично важливим фактором у вирішенні людських помилок і підвищенні інформаційної безпеки в організації. Плекаючи культуру, яка цінує прозорість, безперервне навчання та підзвітність, організації можуть створити середовище, яке зменшує ймовірність людських помилок, які піддають ризику конфіденційні дані. Організаціям важливо надати пріоритет розвитку сильної організаційної культури, яка відповідає цілям інформаційної безпеки та сприяє поведінці, яка зменшує ризики, пов'язані з людськими помилками.

Зрештою, культура, яка заохочує спільну відповідальність за безпеку, може значно сприяти загальній стійкості організації проти соціально-технічних атак.

#### **2.4. Довіра та обман в інформаційній безпеці**

Під час обміну конфіденційною інформацією або доступу до онлайн-ресурсів часто довіряють різним суб'єктам, таким як окремі особи, організації та технології. Однак цією довірою можна скористатися шляхом обману, що призведе до несанкціонованого доступу, витоку даних та інших інцидентів безпеки. Кіберзловмисники часто використовують оманливі методи, такі як фішингові електронні листи, тактики соціальної інженерії та шкідливе програмне забезпечення використовувати довірчі відносини та отримати доступ до цінної інформації. Це підкреслює важливість скептицизму та механізмів перевірки для пом'якшення ризиків, пов'язаних з обманом у сфері інформаційної безпеки. Для вирішення проблем, пов'язаних із шахрайськими практиками в ІБ, організації повинні надати пріоритет встановленню надійних засобів автентифікації та авторизації. Впровадження багатофакторної автентифікації, шифрування та контролю доступу може допомогти підвищити рівень безпеки та захистити від спроб несанкціонованого доступу. Крім того, навчання співробітників і користувачів щодо ризиків обману та важливості перевірки автентичності повідомлень і запитів може значною мірою допомогти запобігти успішним соціотехнічним атакам [26]. Розвиваючи культуру обізнаності про безпеку та просуваючи найкращі практики інформаційної безпеки, організації можуть краще захищатися від обману та підтримувати довіру своїх зацікавлених сторін. Підсумовуючи, довіра та обман є критичними факторами, які впливають на безпеку інформаційних систем і мереж. Оскільки цифровий ландшафт продовжує розвиватися, організаціям вкрай важливо адаптувати свої стратегії безпеки для подолання динамічної природи кіберзагроз. Інвестуючи в технології, які покращують процеси автентифікації та авторизації, а також навчаючи користувачів

про ризики обману, організації можуть посилити свій захист від соціально-технічних атак і захистити конфіденційну інформацію. Зрештою, розуміючи складний зв'язок між довірою та обманом у сфері інформаційної безпеки, організації можуть завчасно зменшувати ризики та ефективно захищати свої цифрові активи.

#### **2.4.1. Важливість довіри до обміну інформацією**

У сфері соціальних факторів, що впливають на інформаційну безпеку, важливість довіри до обміну інформацією не може бути завищеною. Роль довіри це ключовий фактор впливу на наміри на купівлю покоління Z у віртуальних спільнотах, підкреслюючи важливий зв'язок між довірою та поведінкою споживачів в онлайн-просторах [46]. Розуміння багатогранних аспектів довіри до обміну інформацією має першочергове значення для захисту від соціотехнічних атак. Розбираючись у складних факторах, що впливають на динаміку довіри, організації можуть посилити свої заходи інформаційної безпеки та пом'якшити потенційні вразливості, що виникають через брак довіри серед користувачів. Крім того, культивування довіри через сприйману цінність, автентичність і персоналізовані рекомендації може не тільки зміцнити впевненість користувачів у обміні інформацією, але й покращити загальну безпеку онлайн-платформ. Цей тонкий підхід до побудови довіри узгоджується з проактивними стратегіями, необхідними для навігації в мінливому ландшафті загроз ІБ. По суті, зв'язок між довірою та обміном інформацією є стрижнею у зміцненні стійкості цифрових екосистем проти зловмисників, які прагнуть використовувати вразливості. З огляду на наміри покоління Z на купівлю та динаміку довіри користувачів на платформах соціальних мереж, організації можуть впроваджувати цілеспрямовані стратегії, щоб зародити довіру, покращити протоколи безпеки та сприяти відповідальним методам обміну інформацією. Відчуття безпеки, сприйняття конфіденційності та обізнаності користувачів мають значний вплив на довіру користувачів до платформ

соціальних мереж. Довіра, у свою чергу, має значний вплив на кількість інформації, яка ділиться на цих платформах [15]. Оскільки цифровий ландшафт продовжує розвиватися, пріоритет довіри як основного елемента в процесах обміну інформацією стає обов'язковим для створення безпечного та надійного онлайн-середовища, яке захищає окремих осіб, компанії та спільноти від соціально-технічних ризиків. практики відіграють значну роль в обмані окремих осіб та організацій з метою отримання доступу до конфіденційної інформації. Ці практики часто використовують вразливі місця людини, такі як довіра та цікавість, щоб маніпулювати цілями, щоб розкрити конфіденційні дані або натиснути зловмисні посилання. Наприклад, кіберзлочинці можуть використовувати фішингові електронні листи, які нагадують законне листування з надійних джерел, щоб обманом змусити користувачів надати облікові дані для входу чи іншу особисту інформацію. Крім того, тактика соціальної інженерії, як-от подача приводів або переслідування, ґрунтується на маніпулюванні соціальними нормами для отримання несанкціонованого доступу до зон або систем з обмеженим доступом. Використання шахрайських методів у соціально-технічних атаках може мати руйнівні наслідки, оскільки кіберзлочинці можуть використовувати ці тактики для проникнення в мережі, викрадення конфіденційних даних або порушення роботи критично важливих служб. Без належної освіти та обізнаності особи та організації можуть стати жертвами цих схем, що призведе до фінансових втрат, шкоди репутації та юридичних наслідків. Організаціям важливо впроваджувати надійні навчальні програми, щоб ознайомити співробітників із ризиками, пов'язаними з оманливими методами, і культивувати культуру обізнаності про безпеку. Виховуючи настороженість і скептицизм, люди можуть краще захистити себе від соціотехнічних атак і пом'якшити потенційний вплив цих оманливих тактик [27]. Підсумовуючи, під час соціотехнічних атак зазвичай використовуються оманливі методи, щоб використати вразливі місця людини та маніпулювати цілями, щоб мимовільно розкрити конфіденційну інформацію. Ці тактики, як-от фішингові електронні листи та схеми соціальної інженерії, можуть мати серйозні наслідки для

окремих осіб і організацій, якщо їх не контролювати. Щоб посилити захист від цих шахрайських методів, організації повинні надати пріоритет навчанню з питань кібербезпеки та сприяти розвитку культури свідомості безпеки серед співробітників. Оснащуючи людей знаннями та навичками, щоб розпізнавати соціотехнічні атаки та реагувати на них, організації можуть ефективно пом'якшувати ризики, пов'язані з оманливою тактикою, і захищати конфіденційну інформацію від несанкціонованого доступу або зловживання. стосунки мають важливе значення для забезпечення захисту конфіденційних даних і систем. Одним із способів встановлення довіри є прозоре спілкування між зацікавленими сторонами. Організації повинні відкрито ділитися інформацією про свої заходи безпеки, методи обробки даних і протоколи реагування на інциденти, щоб запевнити користувачів і партнерів у своїй відданості захисту інформації. Крім того, участь у регулярних діалогах із зовнішніми сторонами, такими як постачальники, клієнти та регулятори, може сприяти зміцненню довіри та співпраці у впровадженні надійних заходів безпеки. Іншим важливим аспектом побудови надійних відносин у сфері інформаційної безпеки є добре продемонстрована відповідальність. Це передбачає взяття на себе відповідальності за порушення безпеки або помилки та надання своєчасних і прозорих пояснень постраждалим сторонам. Несучи відповідальність за інциденти безпеки, організації можуть підтримувати свою репутацію та довіру, демонструючи, що вони віддані справі усунення вразливостей і запобігання майбутнім порушенням. Така підзвітність може допомогти зміцнити довіру між зацікавленими сторонами та продемонструвати відданість найкращим практикам інформаційної безпеки. Окрім прозорого спілкування та підзвітності, організації також можуть будувати надійні стосунки, віддаючи пріоритет конфіденційності та дотримуючись правил захисту даних. Застосовуючи комплексні заходи захисту даних і дотримуючись відповідних законів, таких як GDPR або CCPA, організації можуть продемонструвати свою відданість захисту прав особи на дані. Пріоритет конфіденційності не тільки допомагає організаціям дотримуватися юридичних

вимог, але й створює довіру користувачів і партнерів, які цінують захист своєї особистої інформації. Зосереджуючись на конфіденційності та захисті даних, організації можуть підвищити свою репутацію надійних розпорядників конфіденційної інформації [28].

## **2.5. Проблеми конфіденційності та захисту даних**

Дотримання правил конфіденційності демонструє прихильність етичним методам обробки даних і допомагає зміцнити довіру клієнтів і зацікавлених сторін. Рухаючись вперед, організації повинні продовжувати надавати пріоритет правилам конфіденційності та інвестувати в надійну політику та методи конфіденційності, щоб захистити конфіденційну інформацію та захистити права особи на конфіденційність [29]. У сфері інформаційної безпеки, поширення зважених соціальних мереж і послуги мобільного Інтернету викликали серйозні проблеми з конфіденційністю, що вимагає надійних заходів захисту даних. Зокрема, використання алгоритмів захисту конфіденційності, таких як DCDP, пропонує багатообіцяючий підхід до захисту конфіденційної інформації в зважених соціальних мережах, зберігаючи при цьому точність даних — важливий баланс в епоху посилення атак на конфіденційність [5]. Алгоритм DCDP (Dynamic Constraint-Driven Path) призначений для пошуку оптимальних маршрутів з урахуванням змінних обмежень у реальному часі. Він аналізує такі фактори, як трафік, погодні умови або інші динамічні зміни, щоб адаптувати маршрути. Цей технологічний прогрес підкреслює важливість завчасного вирішення питань конфіденційності для підтримки конфіденційності користувачів і цілісності даних у соціальних мережах. Крім того, поява мобільного Інтернету на основі краудсенсингу створює унікальні проблеми через розкриття семантики поведінки користувачів через траєкторії розташування, що вимагає інноваційних рішень, таких як BSPri для протистояти інференційним атакам і ефективно захищати конфіденційність користувачів [6]. BSPri (Bandwidth-aware Shortest Path with

Reservation Information) — це алгоритм маршрутизації, що використовується в комп'ютерних мережах для визначення найкоротшого шляху між вузлами з урахуванням доступної пропускної здатності та інформації про зарезервовані ресурси. Основна мета BSPri — забезпечити ефективне використання мережевих ресурсів, мінімізуючи затримки та запобігаючи перевантаженню. Він враховує поточний стан мережі та дозволяє резервувати необхідну пропускну здатність для конкретних передач, що особливо важливо для додатків з високими вимогами до якості обслуговування, таких як відеоконференції або потокове відео. Постійний розвиток цифрових платформ і каналів зв'язку підкреслює критичну потребу в надійних механізмах збереження конфіденційності, особливо в умовах складних атак на конфіденційність, націлених на поведінку користувачів і конфіденційну інформацію. Інтегруючи вдосконалені алгоритми, як-от DCDP, у зважені соціальні мережі, організації та користувачі можуть покращити свої стратегії захисту даних, щоб ефективно зменшити ризики конфіденційності та вразливості. Розробка попередніх рішень для збереження конфіденційності, таких як BSPri, є активним кроком до вирішення проблем конфіденційності в послугах мобільного Інтернету, підкреслюючи важливість превентивних заходів для захисту даних користувачів і пом'якшення впливу потенційних порушень конфіденційності [6]. У контексті соціотехнічних атак та інформаційної безпеки інтеграція найсучасніших алгоритмів захисту конфіденційності та рішень для збереження конфіденційності стає фундаментальною опорою для зміцнення захисту від складних загроз, спрямованих на конфіденційність користувачів і конфіденційну інформацію. Інноваційні підходи, як-от DCDP і BSPri, не лише є прикладом поточних зусиль щодо покращення захисту даних, але й підкреслюють необхідність випереджати проблеми конфіденційності, що розвиваються в цифровому середовищі [5] [6]. Використовуючи ці досягнення та стратегії, організації та окремі особи можуть орієнтуватися в складній взаємодії між соціальними факторами та інформаційною безпекою, щоб зміцнити свій захист і захистити конфіденційність користувачів у все більш взаємопов'язаному світі.

### 2.5.1. Регулювання конфіденційності

У сфері інформаційної безпеки правила конфіденційності відіграють вирішальну роль у захисті персональних даних фізичних осіб від несанкціонованого доступу та зловживання. Організації повинні дотримуватися цих правил, щоб гарантувати, що конфіденційна інформація обробляється відповідально та безпечно. Відповідність цим нормам не тільки допомагає зміцнити довіру клієнтів і зацікавлених сторін, але й зменшує потенційні ризики, пов'язані з витоком даних і кібератаками. Впроваджуючи надійну політику та методи конфіденційності, організації можуть захистити свої активи даних і захистити права на конфіденційність окремих осіб. Крім того, дотримання правил конфіденційності має важливе значення для розвитку культури прозорості та підзвітності в організаціях. Дотримуючись суворих інструкцій щодо захисту даних, організації демонструють свою відданість повазі прав особи на конфіденційність і дотриманню етичних стандартів у поводженні з даними. Відповідність також допомагає організаціям зберігати конкурентну перевагу в світі, де все більше керується даними, де довіра та лояльність споживачів тісно пов'язані із захистом особистої інформації. Таким чином, інтеграція правил конфіденційності в організаційну політику та процедури має вирішальне значення для підтримки міцної репутації та захисту від потенційних правових наслідків. Підсумовуючи, положення про конфіденційність і відповідність є невід'ємними компонентами ефективної стратегії інформаційної безпеки. Віддаючи пріоритет захисту конфіденційності та дотримуючись нормативних вимог, організації можуть покращити свою кібербезпеку та зменшити ризик витоку даних. Крім того, дотримання положень щодо конфіденційності демонструє прихильність етичному використанню даних і допомагає зміцнити довіру клієнтів і зацікавлених сторін. Рухаючись вперед, організації повинні продовжувати надавати пріоритет нормам конфіденційності та інвестувати в надійну політику та методи конфіденційності,

щоб захистити конфіденційну інформацію та захистити права особи на конфіденційність. [26]

### **2.5.2. Техніки шифрування та анонімізації даних**

Завдяки кодуванню даних у спосіб, який можуть розшифрувати лише авторизовані сторони, шифрування гарантує, що навіть у разі перехоплення даних їхній вміст залишається захищеним. Кожна з різних технік шифрування, як-от симетричне й асиметричне шифрування, має унікальні переваги у захисті даних як у стані спокою, так і під час передачі. Однак одного лише шифрування не завжди достатньо в світі, де продовжують розвиватися складні кіберзагрози. Методи анонімізації відіграють додаткову роль у підвищенні конфіденційності даних шляхом видалення ідентифікаційної інформації з наборів даних, тим самим зменшуючи ризик повторної ідентифікації. Поєднання методів шифрування та анонімізації забезпечує багаторівневий підхід до захисту даних, зменшуючи ризики, пов'язані з витоком даних і несанкціонованим доступом. Шифрування захищає вміст самих даних, тоді як анонімізація зосереджується на приховуванні ідентифікаційних атрибутів, які можуть зв'язати дані з особами. Шляхом реалізації обидва методи разом, організації можуть значно підвищити конфіденційність і конфіденційність своїх даних, узгоджуючи їх з нормативними вимогами та найкращими практиками інформаційної безпеки. Більше того, синергетичний ефект шифрування та анонімізації дозволяє організаціям підтримувати цілісність даних, мінімізуючи потенційну можливість викриття в разі інциденту безпеки. У контексті соціотехнічних атак, коли тактика соціальної інженерії часто використовується для використання вразливостей людини та обходу технічного захисту, використання шифрування та анонімізації стає вирішальним. Ці методи не тільки запобігають несанкціонованому доступу з боку зовнішніх загроз, але також відіграють роль у захисті даних від внутрішніх загроз, коли особи з законним доступом можуть зловживати або неправильно поводитися з конфіденційною

інформацією. Завдяки застосуванню надійного шифрування та анонімізації у свої протоколи безпеки даних організації можуть краще захистити себе від складної взаємодії соціальних і технічних факторів, які визначають соціотехнічні атаки. Зрештою, інтеграція методів шифрування та анонімізації представляє проактивний підхід до захисту від нових загроз у все більш взаємопов'язаному цифровому середовищі.

### **2.5.3. Баланс між конфіденційністю та заходами безпеки**

У сфері інформаційної безпеки існує тонкий баланс між захистом конфіденційності окремих осіб та впровадженням необхідної безпеки заходи щодо захисту конфіденційних даних. Конфіденційність є основним правом людини, яке необхідно поважати та підтримувати, але в сучасну епоху цифрових технологій потреба в суворих протоколах безпеки стає все більш важливою. Встановлення правильного балансу між цими двома принципами є непростим завданням, оскільки питання конфіденційності часто суперечать вимогам надійної інфраструктури безпеки. Одним із потенційних рішень цієї головоломки є впровадження технологій шифрування для забезпечення безпечних каналів зв'язку, зберігаючи конфіденційність користувачів. Шифрування дозволяє безпечно передавати та зберігати дані, захищаючи їх від потенційних порушень або несанкціонованого доступу. Впроваджуючи шифрування в різні ІС, організації можуть підтримувати свої протоколи безпеки, не порушуючи прав особи на конфіденційність. Крім того, використання шифрування може допомогти зменшити ризики, пов'язані з кібератаками та витоком даних, тим самим покращуючи загальні заходи безпеки інформації. Організації повинні надавати пріоритет прозорості та чіткій комунікації з користувачами щодо збору та використання їхніх персональних даних. Будучи прозорими щодо даних, які збираються, як вони використовуватимуться та хто матиме до них доступ, організації можуть створити довіру своїх користувачів і продемонструвати

зобов'язання поважати конфіденційність людей. Завдяки чіткій політиці конфіденційності та механізмам отримання згоди організації можуть надати людям можливість робити обґрунтований вибір щодо своїх даних і забезпечити вирішення питань щодо конфіденційності. Активно вирішуючи ці проблеми, організації можуть розвивати культуру конфіденційності та безпеки, яка приносить користь як окремим особам, так і організації в цілому.

## **2.6. Висновки до розділу 2**

Людські помилки відіграють значну роль у порушеннях безпеки, підкреслюючи важливість підвищення обізнаності та освіти персоналу. Незважаючи на технологічні вдосконалення, людський фактор залишається критичним у забезпеченні інформаційної безпеки. Програми навчання та підвищення обізнаності можуть значно зменшити ризик людських помилок, навчаючи співробітників найкращим практикам кібербезпеки та допомагаючи їм виявляти потенційні загрози.

Крім того, організаційна культура відіграє важливу роль у зменшенні людських помилок. Культура відкритого спілкування, навчання на помилках та підзвітності може створити середовище, де працівники відчують себе комфортно, повідомляючи про помилки, що сприяє ранньому виявленню та усуненню вразливостей.

Довіра та обман також є критичними аспектами інформаційної безпеки. Кіберзловмисники часто використовують довіру, маніпулюючи користувачами через фішингові атаки та соціальну інженерію. Впровадження надійних засобів автентифікації та навчання користувачів можуть значно зменшити ризики, пов'язані з обманом.

Організаціям важливо інвестувати в навчання та створення культури безпеки, що включає прозорість, відповідальність та пріоритетність

конфіденційності даних. Це сприятиме зміцненню довіри між зацікавленими сторонами та покращенню загальної стійкості до соціотехнічних атак.

## **РОЗДІЛ 3. СОЦІАЛЬНІ МЕДІА ТА ВНУТРІШНІ ЗАГРОЗИ**

### **3.1. Ризики соціальних медіа в інформаційній безпеці**

Взаємопов'язаний характер платформ соціальних медіа дає змогу окремим особам і організаціям миттєво обмінюватися інформацією, ведучи підвищення продуктивності та співпраці. Однак таке ж підключення створює значні ризики для інформаційної безпеки, оскільки зловмисники можуть використовувати вразливості на сайтах соціальних мереж, щоб отримати доступ до конфіденційних даних. Атаки соціальної інженерії, такі як фішинг і фальшиві профілі, які використовуються для обману користувачів, щоб вони розкрили конфіденційну інформацію або завантажили зловмисне програмне забезпечення. Ці ризики підкреслюють необхідність посилення обізнаності та заходів безпеки в організаціях, щоб пом'якшити потенційний вплив соціальних мереж на інформаційну безпеку. Окрім зовнішніх загроз, внутрішні ризики в організаціях також можуть посилюватися через використання соціальних мереж. Співробітники можуть випадково злити конфіденційну інформацію або порушити протоколи безпеки, обмінюючись конфіденційними даними на публічних платформах. Крім того, соціальні медіа надають хакерам зручну платформу для проведення розвідки та збору інформації про потенційні цілі для майбутніх атак [27]. Це підкреслює важливість впровадження суворої політики та навчальних програм для навчання працівників ризикам, пов'язаним із соціальними медіа, і просування найкращих практик щодо захисту конфіденційної інформації. Незважаючи на ці проблеми, соціальні медіа також можна використовувати як інструмент для підвищення інформаційної безпеки за допомогою проактивного моніторингу та стратегій реагування. Активно відстежуючи канали соціальних мереж на наявність потенційних загроз і взаємодіючи з користувачами для вирішення проблем безпеки, організації можуть ефективно виявляти та зменшувати ризики до їх

ескалації. Використання соціальних медіа як платформи для підвищення обізнаності про найкращі практики кібербезпеки може надати людям можливість приймати обґрунтовані рішення та захистити себе від онлайн-загроз. Зрештою, комплексний підхід, який поєднує технологічні рішення з освітою та обізнаністю користувачів, має важливе значення для забезпечення інформаційної безпеки у все більш взаємопов'язаному цифровому середовищі.

### **3.1.1. Ризики, пов'язані з використанням соціальних мереж**

Незаперечно, що платформи соціальних мереж стали невід'ємною частиною нашого повсякденного життя, полегшуючи спілкування. Обмін інформацією та створення мереж у глобальному масштабі. Однак, поряд із перевагами, існують значні ризики, пов'язані з повсюдним використанням цих платформ. Однією з головних проблем є загроза конфіденційності користувачів і безпеці даних. Платформи соціальних медіа часто збирають величезні обсяги особистої інформації, яка може бути використана зловмисниками для різних цілей, включаючи крадіжку особистих даних, кіберзалякування та цільову рекламу. Без належних заходів безпеки користувачі ризикують отримати конфіденційні дані. Крім того, дуже взаємопов'язаний характер мереж соціальних медіа також може призвести до швидкого поширення дезінформації та фейкових новин, сприяючи ерозії довіри до інформації, що поширюється в Інтернеті. Користувачі можуть несвідомо наражатися на маніпульований вміст, пропаганду або шкідливі кампанії з дезінформації, що ще більше ускладнює і без того складне завдання відрізнити правду від брехні. Це явище не тільки підриває довіру до інформації в соціальних мережах, але й створює значні ризики для суспільства, потенційно формуючи громадську думку та впливаючи на процеси прийняття рішень. Окрім проблем конфіденційності та дезінформації, платформи соціальних мереж також можуть служити розсадником кібератак і онлайн-шахрайства. Спроби фішингу, розповсюдження зловмисного програмного забезпечення та тактика соціальної

інженерії зазвичай використовуються кіберзлочинцями, щоб скористатися вразливими місцями нічого не підозрюючих користувачів на цих платформах. Використовуючи методи соціальної інженерії, зловмисники можуть маніпулювати користувачами, змушуючи їх розкривати конфіденційну інформацію або завантажувати шкідливе програмне забезпечення, скомпрометувавши як окремих користувачів, так і цілі організації. Це підкреслює нагальну потребу у покращенні обізнаності щодо кібербезпеки проактивні заходи для пом'якшення ризиків, пов'язаних із використанням соціальних медіа.

### **3.1.2. Соціальна інженерія через платформи соціальних медіа**

Оскільки платформи соціальних медіа продовжують розвиватися, вони створюють як можливості, так і проблеми для тактики соціальної інженерії. Ці платформи стали живильним середовищем для зловмисників, щоб маніпулювати поведінкою людей, використовувати довіру та збирати конфіденційну інформацію за допомогою шахрайства. Використовуючи взаємопов'язану природу соціальних медіа, зловмисники можуть легко створити правдоподібних персонажів, щоб встановити довіру до нічого не підозрюючих користувачів. Ця довіра потім використовується для отримання особистої інформації або поширення шкідливого вмісту. Крім того, із зростанням цільової реклами та персоналізованого контенту, платформи соціальних медіа мають велику кількість даних, які можуть використовуватися зловмисниками, щоб адаптувати свої атаки соціальної інженерії для максимальної ефективності. Щоб протистояти загрозі соціальної інженерії через платформи соціальних медіа, організації повинні впроваджувати надійні заходи кібербезпеки та забезпечувати комплексне навчання співробітників і користувачів. Це включає в себе навчання окремих осіб різноманітним тактикам, які використовують зловмисники, наприклад схеми фішингу та використання приводів, а також сприяння культурі скептицизму та пильності під час взаємодії з невідомими особами в Інтернеті. Крім того, організації повинні інвестувати в

передові технології, такі як ШІ і машинне навчання, щоб виявляти та запобігати атакам соціальної інженерії в режимі реального часу. Поєднуючи ці технічні рішення з ефективними політиками та процедурами кібербезпеки, компанії можуть пом'якшити ризики, пов'язані із соціальною інженерією через платформи соціальних мереж [23]. Підсумовуючи, соціальна інженерія через платформи соціальних мереж становить значну загрозу як для організацій, так і для окремих осіб. Оскільки зловмисники продовжують використовувати вразливі місця людської поведінки, вкрай важливо вживати профілактичних заходів для захисту від таких атак. Розвиваючи культуру обізнаності, забезпечуючи комплексне навчання та використовуючи передові технології, підприємства можуть підвищити свою стійкість до тактик соціальної інженерії на платформах соціальних мереж. Зрештою, ключ до захисту полягає в багатогранному підході, який поєднує освіту, технології та правозастосовну політику для захисту від соціально-технічних атак, що постійно змінюються [23].

### **3.1.3. Найкращі практики безпечного використання соціальних медіа**

Оскільки соціальні медіа продовжують відігравати невід'ємну роль як в особистому, так і в професійному спілкуванні, вкрай важливо застосувати найкращі практики для захисту інформації, яка поширюється на цих платформах. Однією з ключових стратегій є регулярний перегляд і оновлення налаштувань конфіденційності, щоб лише схвалені контакти мали доступ до конфіденційної інформації. Обмеживши аудиторію публікацій і деталей профілю, люди можуть мінімізувати ризик несанкціонованого доступу до персональних даних. Крім того, рекомендується використовувати надійні унікальні паролі для кожного облікового запису соціальних мереж, щоб запобігти несанкціонованому доступу в разі зламу одного облікового запису. Використання двофакторної автентифікації додає додатковий рівень безпеки, вимагаючи код підтвердження на додаток до пароля для входу. Крім того, користувачам слід бути обережними під час взаємодії з

незнайомими або підозрілими профілями, оскільки вони можуть бути потенційними джерелами кіберзагроз, таких як фішинг або розповсюдження шкідливого програмного забезпечення. Перевірка автентичності запитів на особисту інформацію та уникнення натискання підозрілих посилань можуть захистити вас від того, щоб стати жертвою соціальної інженерії тактика. Бажано навчатися та бути в курсі останніх загроз безпеці та шахрайства, поширених на платформах соціальних мереж. Зберігаючи пильність і розумно розуміючи, люди можуть зменшити ризики, пов'язані з обміном особистою інформацією в Інтернеті. У світлі еволюції кіберзагроз важливо регулярно оновлювати програми соціальних мереж, щоб виправляти вразливості та захищати від нових ризиків безпеки. Оновлення програмного забезпечення часто включають виправлення відомих проблем безпеки, якими можуть скористатися зловмисники. Крім того, люди повинні бути уважними до інформації, якою вони діляться в соціальних мережах, утримуючись від публікації конфіденційних особистих даних, таких як адреси, номери телефонів або фінансова інформація. Обережний підхід до обміну інформацією може допомогти запобігти крадіжці особистих даних і несанкціонованому доступу до особистих даних. Застосовуючи ці найкращі практики для безпечного використання соціальних мереж, люди можуть зменшити ризики стати жертвами кіберзагроз і захистити свою конфіденційність в Інтернеті [30].

### **3.2. Внутрішні загрози та моніторинг працівників**

Внутрішні загрози становлять значний ризик для організацій. Ці загрози можуть надходити від співробітників, які навмисно чи ненавмисно порушують безпеку конфіденційних даних. Одним із підходів, який організації можуть використати для пом'якшення внутрішніх загроз, є впровадження механізмів моніторингу співробітників. Відстежуючи діяльність співробітників, організації можуть виявляти підозрілу поведінку та вживати профілактичних заходів для

запобігання потенційним порушенням безпеки. Однак впровадження моніторингу працівників викликає етичні міркування щодо конфіденційності та довіри на робочому місці. Моніторинг співробітників повинен знайти баланс між захистом конфіденційної інформації та повагою до конфіденційності співробітників. Організації повинні гарантувати, що методи моніторингу є прозорими та проводяться чесно та етично. Прозорість є ключем до збереження довіри між працівниками та роботодавцями, оскільки працівники повинні знати про заходи моніторингу, які застосовуються, і причини, що їх обумовлюють. Крім того, організації повинні встановити чітку політику щодо контролю за працівниками, щоб забезпечити його проведення в законний та етичний спосіб. [31] Загалом, контроль за працівниками може бути цінним інструментом запобігання Внутрішні загрози, організації повинні орієнтуватися в етичних складнощах, пов'язаних із конфіденційністю та довірою на робочому місці. Запроваджуючи прозорі та етичні методи моніторингу, організації можуть ефективно захищати конфіденційні дані, зберігаючи при цьому позитивне робоче середовище. Для організацій вкрай важливо ретельно розглянути наслідки моніторингу співробітників і переконатися, що воно відповідає правовим і етичним стандартам.

### **3.2.1. Типи внутрішніх загроз**

У сфері внутрішніх загроз різні типи становлять значні ризики для організацій. Зловмисні інсайдери викликають, мабуть, найбільше занепокоєння, оскільки вони навмисно використовують свій доступ для особистої вигоди або для шкоди організації. Ці люди можуть бути незадоволеними співробітниками, які прагнуть помститися, або зовнішніми акторами, які проникли в організацію. Іншим поширеним типом внутрішньої загрози є недбалий інсайдер, який може несвідомо порушити безпеку через необережні дії, такі як піддатися фішингу або використання слабких паролів. Ці особи не мають злих намірів, але їхні дії все одно можуть мати серйозні наслідки для безпеки даних. Крім того, існують також

внутрішні загрози від сторонніх постачальників або підрядників, які мають доступ доконфіденційні системи та дані. Ці люди можуть не мати такого ж рівня лояльності чи інвестицій в організацію, як штатні працівники, що робить їх потенційними цілями для зовнішніх гравців, які прагнуть використати їхній доступ. Крім того, ненавмисні інсайдерські загрози також можуть виникати від співробітників із добрими намірами, які ненавмисно порушують протоколи безпеки, намагаючись підвищити ефективність чи продуктивність. Ці особи можуть не усвідомлювати потенційних ризиків своїх дій, що підкреслює важливість комплексного навчання безпеки та програм підвищення обізнаності [31]. Щоб ефективно пом'якшити ризики, пов'язані з інсайдерськими загрозами, організації повинні застосувати багатогранний підхід, який включає технічний контроль, моніторинг співробітників і аналіз поведінки. Відстежуючи поведінку співробітників і моделі доступу, організації можуть виявляти аномалії або підозрілі дії, які можуть вказувати на загрози з боку внутрішньої сторони. Також важливо встановити чітку політику та процедури для надання та скасування доступу до конфіденційних даних, а також регулярно переглядати та оновлювати дозволи, щоб забезпечити доступ лише уповноваженому персоналу. Зрештою, поєднання проактивних заходів і реактивних заходів має важливе значення для захисту від різноманітних типів внутрішніх загроз, з якими організації можуть зіткнутися в епоху цифрових технологій.

### **3.2.2. Впровадження систем моніторингу співробітників та баланс між конфіденційністю працівників та моніторингом безпеки**

Оскільки організації орієнтуються в складному ландшафті інформаційної безпеки, впровадження постійного моніторингу безпеки стає важливою стратегією для зменшення ризиків і виявлення потенційних загроз у режимі реального часу. Безперервний моніторинг виходить за рамки традиційних періодичних оцінок, забезпечуючи постійний потік даних, що дозволяє швидко реагувати та вживати

заходів з усунення несправностей. Цей проактивний підхід дозволяє організаціям не тільки зміцнити свої механізми захисту, але й адаптуватися до нових загроз у динамічному середовищі. Застосовуючи інструменти та технології, які автоматизують процес моніторингу, організації можуть покращити рівень безпеки та випередити кіберзлочинців. Крім того, постійний моніторинг безпеки узгоджується з концепцією поглибленого захисту, багаторівневої стратегії безпеки, яка наголошує на кількох захисних заходах для захисту від різноманітних загроз. Інтегруючи постійний моніторинг у існуючі системи безпеки, організації можуть створити надійну лінію захисту, яка доповнює інші засоби контролю безпеки, такі як брандмауери, антивірусне програмне забезпечення та системи виявлення вторгнень. Цей багаторівневий підхід підвищує ймовірність виявлення та блокування потенційних порушень на різних етапах життєвого циклу атаки, мінімізуючи вплив інцидентів безпеки на критичні активи та дані. Підсумовуючи, впровадження безперервного моніторингу безпеки є проактивним і стратегічним вкладенням у захист організаційних активів і конфіденційної інформації. Інтегрувавши цю практику у свої протоколи безпеки, організації можуть підвищити свою стійкість проти кіберзагроз і забезпечити своєчасне реагування на потенційні інциденти безпеки. Оскільки цифровий ландшафт продовжує розвиватися, впровадження безперервного моніторингу безпеки буде важливим для підтримки міцної позиції безпеки та захисту від зростаючої складності кіберзагроз [14].

У контексті інформаційної безпеки впровадження систем моніторингу співробітників може бути цінним інструментом для організації для захисту своїх конфіденційних даних. Відстежуючи цифрову діяльність співробітників, компанії можуть виявляти та запобігати потенційним внутрішнім загрозам, несанкціонованому доступу або витоку даних. Цей проактивний підхід до моніторингу може служити стримуючим фактором для співробітників, які можуть задуматися про участь у зловмисних діях, таким чином сприяючи культурі підзвітності та відповідності в організації. Крім того, системи моніторингу

співробітників можуть надати цінну інформацію про моделі поведінки співробітників і допомогти визначити потреби в навчанні або області для вдосконалення процесів для підвищення загальної безпеки. Однак до впровадження систем моніторингу працівників слід підходити обережно, щоб уникнути порушення прав працівників на конфіденційність. Організації повинні чітко повідомляти співробітникам про мету та обсяг діяльності з моніторингу, забезпечуючи прозорість і за необхідності отримуючи їхню згоду. Крім того, важливо встановити чітку політику та процедури щодо використання даних моніторингу, окреслюючи дозволені види використання та обмеження для запобігання неправильному використанню або зловживанню системою. Встановлюючи баланс між потребами безпеки та турботами про конфіденційність співробітників, організації можуть ефективно використовувати системи моніторингу для зміцнення свого захисту від соціально-технічних атак. Підсумовуючи, ефективне впровадження систем моніторингу співробітників може значно сприяти підвищенню інформаційної безпеки в організаціях. Використовуючи ці системи для відстеження та аналізу цифрової діяльності співробітників, компанії можуть проактивно виявляти та пом'якшувати ризики безпеки, сприяючи культурі обізнаності про безпеку та відповідності вимогам. Однак для організацій вкрай важливо підходити до моніторингу стратегічно, забезпечуючи повагу до прав співробітників на конфіденційність і підтримуючи прозорість у їхній діяльності. Запроваджуючи чітку політику та процедури та сприяючи відкритому спілкуванню зі співробітниками, організації можуть використовувати переваги систем моніторингу, дотримуючись при цьому етичних і правових стандартів у своїх стратегіях безпеки. [32]

У сфері інформаційної безпеки питання балансу між конфіденційністю співробітників і моніторингом безпеки є складним і делікатним. З одного боку, організації несуть відповідальність за захист своїх конфіденційних даних і захист від потенційних порушень. Це часто вимагає впровадження систем моніторингу для виявлення та запобігання загрозам безпеки. Однак такий моніторинг

потенційно може порушувати права працівників на конфіденційність. Організації повинні ретельно впоратися з цією напругою, щоб забезпечити належну підтримку як безпеки, так і конфіденційності. Щоб досягти цього балансу, організації повинні встановити чітку політику та вказівки щодо практик моніторингу безпеки. Ці політики мають окреслювати конкретні обставини, за яких здійснюватиметься моніторинг, типи даних, які збиратимуться, а також те, як ці дані використовуватимуться та зберігатимуться. Забезпечуючи прозорість і чітку комунікацію, організації можуть допомогти зменшити занепокоєння співробітників щодо порушень конфіденційності [33]. Крім того, організаціям слід розглянути можливість впровадження технологій, які надають пріоритет захисту даних, таких як методи шифрування та анонімізації, щоб мінімізувати ризик порушення конфіденційності. Зрештою, пошук правильного балансу між конфіденційністю співробітників і моніторингом безпеки вимагає багатогранного підходу. Організації повинні надавати пріоритет як захисту конфіденційної інформації, так і повазі прав співробітників на конфіденційність. Встановлюючи чітку політику, забезпечуючи прозорість і впроваджуючи безпечні технології, організації можуть досягти гармонійного співіснування заходів безпеки та захисту конфіденційності. Цей збалансований підхід не тільки підвищує інформаційну безпеку, але й сприяє розвитку культури довіри та поваги в організації.

### **3.3. Етичні міркування в ІБ та вирішення етичних дилем**

Розглядаючи етичні міркування в ІБ, важливо розглянути такі питання, як конфіденційність, доступність і цілісність даних. Окремі особи та організації повинні дотримуватися етичних принципів поваги до конфіденційності, захищаючи особисту інформацію від несанкціонованого доступу чи неправомірного використання. Крім того, дотримання конфіденційності гарантує, що конфіденційні дані будуть доступні лише авторизованим особам, захищаючи їх від потенційних порушень або витоків. Цілісність даних також має вирішальне

значення, оскільки будь-яке втручання або маніпулювання інформацією може мати серйозні наслідки як для окремих осіб, так і для компаній. У контексті інформаційної безпеки етичні міркування відіграють важливу роль у формуванні політики та практики, які регулюють використання технологій та даних. Етичні принципи забезпечують керівні принципи для процесів прийняття рішень, допомагаючи забезпечити відповідальне та прозоре управління інформацією. Дотримуючись етичних принципів, організації можуть побудувати довіру зі своїми зацікавленими сторонами та продемонструвати відданість захисту конфіденційної інформації. Неврахування етичних міркувань інформаційної безпеки може мати згубні наслідки як для репутації, так і для юридичної відповідальності. Загалом, етичні аспекти інформаційної безпеки є важливими для сприяння довірі, підзвітності та відповідальності в цифровому середовищі. Дотримуючись таких етичних принципів, як повага до приватного життя, конфіденційності та цілісності даних, окремі особи та організації можуть створити безпечне та надійне середовище для зберігання та обміну інформацією. Вкрай важливо, щоб зацікавлені сторони визначали пріоритетність етичних міркувань і інтегрували їх у свої стратегії інформаційної безпеки, щоб зменшити ризики та захистити від потенційних загроз [42].

обробляючи конфіденційні дані, організації повинні надавати пріоритет захисту приватного життя та конфіденційності. Це вимагає встановлення чітких політик і процедур для збору, зберігання та обміну даними, щоб забезпечити відповідність таким нормам, як GDPR. Впроваджуючи суворий контроль доступу та протоколи шифрування, організації можуть зменшити ризик несанкціонованого доступу та витоку даних, тим самим захищаючи конфіденційну інформацію від зловмисників. Крім того, культивування культури етики даних в організації має важливе значення для сприяння підзвітності та прозорості в роботі з конфіденційними даними. Це включає в себе проведення програм навчання та підвищення обізнаності для співробітників, щоб зрозуміти важливість етичних методів обробки даних і потенційні наслідки недотримання. Етичні міркування також поширюються на використання новітніх технологій, таких як ШІ і машинне

навчання, для обробки конфіденційних даних. Організації повинні гарантувати, що ці технології використовуються відповідально та етично, беручи до уваги такі фактори, як упередженість та дискримінація в алгоритмічному прийнятті рішень. Проводячи регулярні аудити та оцінки систем штучного інтелекту, організації можуть виявити та виправити будь-які етичні проблеми, які можуть виникнути під час обробки конфіденційних даних [43]. Крім того, включення етичних принципів у проектування та розробку програм ІІІ, таких як справедливість, підзвітність і прозорість, може допомогти зменшити етичні ризики та сприяти довірі між користувачами та зацікавленими сторонами [43]. Підсумовуючи, етичні принципи поводження з конфіденційними даними мають вирішальне значення для підтримки довіри та впевненості людей у методах обробки даних організації. Віддаючи пріоритет конфіденційності та конфіденційності, впроваджуючи надійні заходи безпеки та розвиваючи культуру етики даних, організації можуть захистити конфіденційну інформацію від несанкціонованого доступу та зловживання. Крім того, відповідальне використання нових технологій і дотримання етичних принципів при обробці даних є важливими для пом'якшення етичних ризиків і забезпечення дотримання нормативних актів. Зрештою, дотримуючись етичних стандартів у поводженні з конфіденційними даними, організації можуть підтримувати свою репутацію, зміцнювати довіру клієнтів і робити внесок у безпечне та етичне цифрове середовище.

Для організацій надзвичайно важливо вирішувати етичні дилеми впрактики безпеки для підтримки цілісності та довіри в цифровій екосистемі. Одним із ключових міркувань є дилема між заходами безпеки та індивідуальними правами на конфіденційність. Хоча надійні протоколи безпеки необхідні для захисту конфіденційних даних, вони не повинні без потреби порушувати конфіденційність людей. Організації повинні підтримувати цей делікатний баланс, впроваджуючи прозорі заходи безпеки, які надають пріоритет як безпеці, так і конфіденційності. Таким чином вони можуть продемонструвати відданість етичним практикам, зберігаючи при цьому безпечне середовище для своїх зацікавлених сторін. Іншою

етичною дилемою в практиці безпеки є використання технологій спостереження для моніторингу співробітників або користувачів. Хоча стеження може бути необхідним з метою безпеки, воно викликає занепокоєння щодо вторгнення в конфіденційність і підриву довіри. Організації повинні ретельно оцінювати необхідність і пропорційність заходів нагляду, забезпечуючи їх виправданість і етичність. Це передбачає встановлення чіткої політики та вказівок щодо практики стеження, а також отримання чіткої згоди від осіб, де це можливо. Враховуючи ці етичні міркування, організації можуть пом'якшити потенційні ризики та сприяти розвитку культури прозорості та підзвітності у своїй практиці безпеки [44]. Підсумовуючи, вирішення етичних дилем у практиці безпеки має важливе значення для підвищення стійкості кібербезпеки та дотримання етичних стандартів у цифрову епоху. Організації повинні завчасно виявляти та вирішувати етичні проблеми в практиці безпеки, такі як збалансування проблем безпеки та конфіденційності та відповідальне впровадження заходів стеження. Віддаючи пріоритет етичним міркуванням у своїх стратегіях безпеки, організації можуть побудувати довіру зі своїми зацікавленими сторонами та сприяти культурі чесності та підзвітності. Організаціям необхідно інтегрувати етичні принципи у свою практику безпеки, щоб захистити дані та дотримуватися етичних стандартів у все більш взаємопов'язаному та керованому даними світі.

Одним із ефективних способів сприяння етичній поведінці серед працівників є встановлення чітких очікувань і вказівок всередині організації. Викладаючи конкретні етичні стандарти та кодекси поведінки, співробітники, швидше за все, розумітимуть, що від них очікується, і діятимуть відповідно до цих принципів. Це може допомогти створити культуру чесності та підзвітності на робочому місці. Крім того, регулярне навчання та освіта з питань прийняття етичних рішень може ще більше зміцнити ці цінності та допомогти співробітникам долати складні етичні дилеми. Ще один важливий аспект сприяння етичній поведінці серед працівників – це показувати приклад. Керівники організацій відіграють вирішальну роль у встановленні тону етичної поведінки в компанії.

Коли лідери демонструють відданість етичним принципам у своїх діях і прийнятті рішень, це надсилає потужне повідомлення співробітникам про важливість чесності та етики в організації. Керівники повинні дотримуватися тих самих високих стандартів, яких вони очікують від своїх співробітників, слугуючи взірцем етичної поведінки [45]. Крім того, створення системи винагород і визнання етичної поведінки може стимулювати співробітників діяти відповідно до етичних принципів. Визнаючи та винагороджуючи етичну поведінку, співробітники, швидше за все, будуть мотивовані підтримувати ці цінності у своїй щоденній роботі. Це може допомогти зміцнити культуру етики та чесності в організації, заохочувати співробітників приймати етичні рішення, навіть коли вони стикаються зі складними ситуаціями. Поєднуючи чіткі очікування, лідерство власним прикладом і систему винагород, організації можуть ефективно заохочувати етичну поведінку серед співробітників і створювати позитивний етичний клімат на робочому місці.

### **3.4. Співпраця та обмін інформацією**

У сфері кібербезпеки зростаюча взаємозв'язаність цифрового світу підкреслює необхідність надійної міжнародної співпраці для ефективної боротьби з кіберзагрозами. Порівняльний аналіз кіберправа та політики безпеки в таких країнах, як Пакистан, США, Канада та Австралія, показує важливість розуміння геополітичного та соціально-економічного контексту кожної нації для формування їх стратегії кіберзахисту [1]. Це дослідження підкреслює необхідність комплексної правової бази та наголошує на ключовій ролі міжнародного співробітництва у зміцненні глобальної кіберстійкості проти нових небезпек. Використовуючи передові статистичні методи та комплексні набори даних, що охоплюють різні регіони, це дослідження підкреслює важливість виявлення кореляцій, регіональних відмінностей і тенденцій, що розвиваються, для інформування політиків і спеціалістів із безпеки [2]. Ефективне міжнародне співробітництво має важливе

значення для розвитку стійкої глобальної цифрової екосистеми, здатної протистояти мінливому ландшафту кіберзагроз. Крім того, спільні зусилля, описані в цитованих дослідженнях, підкреслюють необхідність колективного підходу до кібербезпеки, який виходить за межі національних кордонів. Аналізуючи відомі індекси кібербезпеки та глобальні системи безпеки, дослідники прагнуть надати політикам і зацікавленим сторонам корисну інформацію для посилення захисту від кіберзагроз. Дослідження заглиблюється в найкращі практики та прогалини в стратегіях кіберзахисту, наголошуючи на важливості вивчення підходів інших країн для зміцнення власних заходів кібербезпеки [1]. Цей спільний обмін знаннями та практиками сприяє більш комплексному та адаптивному підходу до кібербезпеки, необхідного для захисту цифрових інфраструктур у всьому світі. Головною метою є розвиток культури обміну інформацією та транскордонного співробітництва для зміцнення глобальної цифрової фортеці та пом'якшення ризиків, пов'язаних із кіберзагрозами.

Працюючи разом, організації можуть використовувати колективні знання та ресурси, щоб ефективніше виявляти загрози та реагувати на них. Обмін інформацією про кіберзагрози та вразливості дозволяє отримати більш повне розуміння ландшафту загроз, що розвивається, дозволяючи вживати профілактичні заходи для зменшення ризиків. Крім того, співпраця може допомогти в розробці найкращих практик і стандартів, які можна прийняти в усій галузі для підвищення загальної безпеки. У світі, де кіберзагрози постійно розвиваються та стають все більш витонченими, обмін інформацією має важливе значення для того, щоб випередити зловмисників. Організації, які співпрацюють і обмінюються розвідувальними даними про загрози, можуть отримати вигоду з ширшого спектру точок зору та розуміння, що веде до більш надійних механізмів захисту. Об'єднуючи ресурси та досвід, організації можуть посилити свою безпеку та краще захистити себе від нових загроз. Крім того, співпраця сприяє розвитку культури прозорості та підзвітності, які є важливими компонентами проактивної стратегії безпеки. Однак, незважаючи на переваги співпраці та обміну інформацією для

підвищення інформаційної безпеки, існують проблеми, які необхідно вирішити. Однією з першочергових проблем є питання довіри та конфіденційності. Організації можуть неохоче ділитися конфіденційною інформацією через занепокоєння щодо можливого порушення даних або невігідної конкуренції. Встановлення чітких інструкцій і протоколів для обміну інформацією, а також зміцнення довіри між учасниками є важливими кроками для подолання цих перешкод. Крім того, правові та нормативні обмеження можуть обмежувати обсяг, до якого організації можуть вільно обмінюватися інформацією. Знаходження балансу між проблемами конфіденційності та необхідністю заходів колективної безпеки має вирішальне значення для сприяння ефективній співпраці в боротьбі з соціотехнічними атаками.

Співпраця стає ключовою стратегією пом'якшення складних проблем, що виникають. соціотехнічними атаками. Як підкреслюється в літературі, професіонали в різних секторах, включаючи послуги охорони здоров'я та освіти, отримують значну вигоду від спільних зусиль під час захисту конфіденційних даних і систем [16] [17]. Обмін досвідом і ресурсами між міждисциплінарними командами покращує здатність оцінювати ризики, приймати обґрунтовані рішення та розробляти надійні заходи безпеки. Цей спільний підхід не тільки покращує загальну ефективність протоколів інформаційної безпеки, але й культивує культуру спільної відповідальності та підзвітності серед зацікавлених сторін. Крім того, синергія, досягнута завдяки співпраці, сприяє більш повному розумінню загроз ІБ та вразливостей у певному контексті. Визнаючи взаємозалежність між різними департаментами та агентствами, організації можуть створити єдиний фронт проти потенційних кіберризиків і зломів. Ця спільна обізнаність дозволяє впроваджувати проактивні заходи, такі як розробка чіткої політики, вибір безпечних технологій і проведення постійного моніторингу, як це пропонується в літературі [17]. У результаті екосистема спільної роботи стає фундаментальною опорою для зміцнення стійкості та адаптивності структур інформаційної безпеки перед обличчям загроз, що розвиваються. Крім того, ефективна співпраця в галузі

інформаційної безпеки не тільки підвищує ефективність роботи, але й зміцнює цілісність навчального середовища. Коли професіонали в різних галузях об'єднуються для вирішення проблем безпеки, вони приносять безліч точок зору та ідеї, які збагачують процес прийняття рішень і сприяють інноваційним рішенням. Розвиваючи культуру відкритого спілкування та обміну знаннями, організації можуть використовувати колективний досвід міждисциплінарних команд для вирішення складних проблем безпеки, як видно з обговорення факторів, що впливають на судження, прийняття рішень і міждисциплінарну співпрацю в захисті вразливих груп населення [16]. Зрештою, переваги співпраці в ІБ виходять за межі простого зменшення ризиків і охоплюють цілісний підхід, який забезпечує конфіденційність, цілісність і доступність критично важливих інформаційних активів.

Організації повинні впроваджувати надійні заходи безпеки для захисту конфіденційної інформації, забезпечуючи при цьому співпрацю та спілкування між авторизованими користувачами. Однією з ефективних стратегій покращення практики безпечного обміну інформацією є впровадження технологій шифрування. За допомогою шифрування даних як під час передачі, так і в спокої організації можуть гарантувати, що лише авторизовані особи зможуть отримати доступ до конфіденційної інформації та розшифрувати її, зменшуючи ризик несанкціонованого доступу та витоку даних. Крім того, використання безпечних каналів зв'язку, таких як VPN і безпечні протоколи передачі файлів, може покращити захист спільної інформації шляхом створення зашифрованих тунелів для передачі даних. Крім того, створення чіткої та всебічної політики обміну інформацією має важливе значення для регулювання обміну конфіденційними даними всередині організації. Ця політика має окреслювати вказівки щодо ідентифікації та класифікації різних типів інформації на основі їхнього рівня конфіденційності, а також вказувати авторизованих користувачів, які можуть отримувати доступ до кожної категорії даних і ділитися ними. Визначаючи ролі та обов'язки, пов'язані з обміном інформацією, організації можуть запобігти витоку

даних і мінімізувати ризик внутрішніх загроз. Регулярні тренінги та програми підвищення обізнаності для співробітників щодо методів безпечного обміну інформацією також можуть посилити важливість захисту даних і культивувати культуру обізнаності про кібербезпеку в організації [48]. Підсумовуючи, захищені практики обміну інформацією мають першочергове значення для зменшення ризиків, пов'язаних із соціотехнічними атаками, і забезпечення конфіденційності, цілісності та доступності конфіденційних даних. Організації повинні визначити пріоритети впровадження технологій шифрування, безпечних каналів зв'язку та надійної політики обміну інформацією, щоб створити надійну систему безпеки. Застосовуючи проактивний підхід до інформаційної безпеки та розвиваючи культуру пильності та відповідальності серед співробітників, організації можуть ефективно захистити свої цінні активи від загроз, що постійно змінюються. Застосування методів безпечного обміну інформацією є не лише вимогою відповідності, але й стратегічним імперативом для організацій, які прагнуть захистити свої активи даних і зберегти свою репутацію у все більш взаємопов'язаному світі [48].

У сфері безпеки Співпраця, використання інструментів і технологій відіграє ключову роль у забезпеченні захисту конфіденційної інформації та даних. Наприклад, програмне забезпечення для шифрування має важливе значення для захисту каналів зв'язку та запобігання несанкціонованому доступу до спільних документів або повідомлень. Впроваджуючи наскрізне шифрування, організації можуть захистити свої конфіденційні дані від потенційних порушень або перехоплення зловмисниками. Крім того, безпечні платформи для співпраці пропонують такі функції, як контроль доступу, журнали аудиту та шифрування даних у стані спокою, що ще більше підвищує рівень безпеки спільної роботи. Крім того, інтеграція MFA в інструменти для співпраці додає додатковий рівень безпеки, вимагаючи від користувачів надавати кілька форм перевірки перед доступом до спільних ресурсів. Це не тільки допомагає перевірити особу осіб, які беруть участь у спільній роботі, але й мінімізує ризик несанкціонованого доступу у разі

скомпрометованих облікових даних. Крім того, впровадження безпечних технологій обміну файлами, які використовують протоколи шифрування та засоби контролю доступу, гарантує безпечну передачу конфіденційних документів між співавторами, зменшуючи ризик витоку даних [26]. Загалом, використання передових інструментів і технологій у сфері безпечної співпраці є обов'язковим для сучасних організацій, які прагнуть захистити свою інтелектуальну власність і конфіденційну інформацію. Використовуючи зашифровані канали зв'язку, надійні засоби контролю доступу та механізми автентифікації, компанії можуть створити безпечне середовище для спільної роботи без шкоди для безпеки даних. Оскільки кіберзагрози продовжують розвиватися, організації повинні залишатися проактивними у впровадженні інноваційних рішень для захисту їхніх спільних зусиль та збереження цілісності їхніх цифрових активів.

Глобальне співробітництво в кіберзахисті має вирішальне значення для вирішення проблем, що розвиваються загроз і вразливостей у сучасному взаємопов'язаному світі. Управління ІТ-додатками для європейських фондів і модернізація ІТ-інфраструктури вимагають розширеного кіберзахисту та можливостей оборони, що підкреслює необхідність міжнародної співпраці у зміцненні кіберзахисту [10]. У контексті гібридних операцій, націлених на вразливі місця, як обговорювалося в [11], розуміння стратегій, які використовують державні та недержавні суб'єкти для використання слабких місць, зокрема через платформи соціальних мереж, вимагає єдиного фронту для протидії таким загрозам. Визнаючи взаємопов'язаний характер кіберризиків і спільну відповідальність за захист критично важливої інформації та систем, глобальна співпраця стає наріжним каменем у зміцненні загальних можливостей кіберзахисту. Крім того, взаємозалежність націй у цифровій сфері, як зазначено в [10], підкреслює важливість колективних зусиль у залученні ресурсів і досвіду для ефективної боротьби з кіберзагрозами. Залежність від цифрових технологій для стимулювання інновацій, економічного зростання та надання державних послуг посилює необхідність скоординованих глобальних стратегій безпеки кіберпростору. У світлі

геополітичних і стратегічних міркувань, розглянутих у [11], потреба у взаємній підтримці та обміні інформацією між націями стає все більш очевидною для пом'якшення багатогранних викликів, створених гібридними загрозами. Міжнародне співробітництво не тільки підвищує стійкість окремих держав, але й сприяє досягненню ширшої мети підтримки регіональної та глобальної безпеки перед обличчям кіберзбоїв. Підсумовуючи, заклик до глобальної співпраці у сфері кіберзахисту є не просто проактивним заходом, а необхідністю для захисту національних інтересів і підтримки цілісності цифрової екосистеми. Завдяки об'єднанню ресурсів, досвіду та обміну розвідданими через кордони, держави можуть ефективно зміцнити свої механізми кіберзахисту та адаптуватися до динамічного ландшафту загроз. Рекомендації, викладені в [10] і [11], підкреслюють критичну роль міжнародного співробітництва в усуненні вразливостей, протидії гібридним загрозам і просуванню безпечного та стійкого кіберсередовища в глобальному масштабі. Застосування колективного підходу до кібербезпеки має важливе значення для подолання складних викликів, пов'язаних із соціотехнічними атаками, і просування до більш безпечного цифрового майбутнього для всіх.

У сфері інформаційної безпеки обмін інформацією про загрози через кордони представляє як виклики, так і можливості. Однією з головних переваг обміну даними про загрози на міжнародному рівні є можливість ефективніше виявляти нові кіберзагрози та реагувати на них. Співпрацюючи з іншими країнами, організації можуть отримати цінну інформацію про різні типи атак і посилити власні заходи кібербезпеки. Цей колективний підхід може призвести до більш надійного глобального захисту від кіберзагроз, що принесе користь усім залученим сторонам. Однак існують перешкоди для обміну інформацією про загрози через кордони, зокрема культурні відмінності, правові обмеження та занепокоєння щодо конфіденційності даних. Ці виклики необхідно вирішувати шляхом посилення співпраці та розробки взаємоузгоджених структур для обміну конфіденційною інформацією [40]. Крім того, обмін інформацією про загрози через кордони також може призвести до підвищення довіри та співпраці між країнами у сфері

кібербезпеки. Працюючи разом у боротьбі зі спільними загрозами, країни можуть будувати міцніші відносини та розвивати почуття солідарності перед обличчям кібератак. Ця співпраця також може допомогти усунути прогалини в знаннях і ресурсах, дозволяючи країнам з різним рівнем розвитку кібербезпеки вчитися одна в одній та спільно зміцнювати свій захист. Завдяки обміну розвідувальними даними про загрози країни можуть зробити свій внесок у створення більш безпечного глобального кіберпростору та пом'якшити ризики, створені досвідченими кіберсупротивниками [40]. Підсумовуючи, обмін даними про загрози через кордони має важливе значення для підвищення стійкості глобальної кібербезпеки та боротьби з дедалі складнішими кіберзагрозами. Хоча існують проблеми, які необхідно подолати, наприклад правові та культурні бар'єри, переваги міжнародної співпраці значно переважають ризики. Встановлюючи чіткі рамки для обміну розвідувальною інформацією про загрози та сприяючи культурі співпраці, країни можуть колективно зміцнювати свій захист і краще захищати критичну інфраструктуру та дані від зловмисників. Вкрай важливо, щоб організації та уряди надавали пріоритет обміну інформацією як ключовому компоненту своєї стратегії кібербезпеки, щоб ефективно протистояти ландшафту загроз, що розвивається.

### **3.5. Висновки по розділу 3**

На завершення, вирішення багатогранної проблеми соціотехнічних атак вимагає комплексного підходу, який враховує складну взаємодію між соціальними і технічними факторами. Усвідомлюючи вплив соціальної динаміки на інформаційну безпеку, організації можуть розробляти ефективніші стратегії захисту від таких типів атак. Це включає впровадження навчальних програм безпеки, які навчають користувачів про ризики, пов'язані з тактикою соціальної інженерії, і просування культури безпеки в організації. Крім того, організації можуть отримати вигоду від проведення регулярних оцінок безпеки для виявлення вразливостей, якими можуть скористатися зловмисники. Крім того, співпраця між

різними зацікавленими сторонами, включаючи спеціалістів із безпеки, відділи кадрів і керівництво, є важливою для пом'якшення ризиків, пов'язаних із соціотехнічними атаками. Сприяючи відкритому спілкуванню та співпраці між цими групами, організації можуть підвищити загальну безпеку та краще захистити від тактики соціальної інженерії. Крім того, розробка політик і процедур, які стосуються соціальних факторів інформаційної безпеки, може допомогти організаціям встановити чіткі вказівки щодо реагування на потенційні загрози та інциденти. Такий проактивний підхід може значно знизити ймовірність успішних соціотехнічних атак і мінімізувати їх вплив на організацію. Зрештою, рекомендації, викладені в цьому есе, є дорожньою картою для організацій щодо посилення захисту від соціально-технічних атак і захисту конфіденційної інформації. Інтегруючи соціальні фактори у свої стратегії безпеки та розвиваючи культуру пильності серед співробітників, організації можуть ефективно пом'якшувати ризики, пов'язані з тактикою соціальної інженерії. Завдяки постійному навчанню, співпраці та профілактичним заходам безпеки організації можуть краще захистити свої інформаційні активи та мінімізувати вплив соціально-технічних атак. Організаціям вкрай важливо надати пріоритет інтеграції соціальних факторів у свої системи безпеки, щоб випереджати загрози, що розвиваються в цифровому ландшафті. [23]

## РОЗДІЛ 4. СТРАТЕГІЇ ЗАХИСТУ ВІД СОЦІОТЕХНІЧНИХ АТАК ТА ТЕНДЕНЦІЇ МАЙБУТНЬОГО

### 4.1. Рекомендації щодо захисту від соціально-технічних атак

Захист від соціально-технічних атак потребує багатогранного підходу, який об'єднує як технічні, так і орієнтовані на людину стратегії. Важливе впровадження надійних протоколів шифрування для пом'якшення вразливостей у хмарних системах. Усунення соціотехнічних вразливостей вимагає всебічного розуміння різноманітних впливів, які формують ландшафт безпеки. Щоб зміцнити захист від соціотехнічних атак, організації повинні визначити пріоритетність заходів, які зміцнюють як технологічну стійкість, так і обізнаність людей. Впровадження суворого контролю доступу та механізмів шифрування може зміцнити безпеку цифрових активів. Крім того, міркування політичної та економічної нестабільності підкреслюють потребу в контекстуальних оцінках ризиків, які враховують соціально-політичну динаміку [9]. Розвиваючи культуру обізнаності про кібербезпеку та інтегруючи соціально-економічні знання в стратегії зменшення ризиків, організації можуть активно боротися з багатогранною природою соціально-технічних загроз. Підсумовуючи, конвергенція технологічної вразливості та соціально-політичних факторів підкреслює необхідність узгоджених стратегій для захисту від соціально-технічних атак. Криптографія та геополітичні міркування відіграють невід'ємну роль у підвищенні стійкості безпеки [9]. Використовуючи знання з різних областей і сприяючи цілісному підходу до інформаційної безпеки, організації можуть проактивно захищатися від багатогранних загроз, створених соціотехнічними атаками.

Одним з найважливіших аспектів підтримки ефективної інформаційної безпеки в організаціях є дотримання нормативних вимог і управління. У сучасному складному цифровому ландшафті компанії повинні дотримуватися різноманітних

правил і стандартів, щоб захистити конфіденційні дані та пом'якшити кіберзагрози. Відповідність нормативним вимогам гарантує, що організації дотримуються встановлених інструкцій, законів і найкращих галузевих практик для захисту своїх інформаційних активів. Впроваджуючи сильні структури управління, компанії можуть оптимізувати свої зусилля з дотримання вимог і забезпечити послідовне застосування заходів безпеки в усій організації. Приклад важливості дотримання нормативних вимог і управління можна побачити в галузі охорони здоров'я, де організації повинні дотримуватися нормативних актів, таких як НІРАА закон про перенесення та підзвітність медичної інформації, щоб захистити інформацію про пацієнтів. Недотримання цих правил не лише створює ризик для конфіденційних даних, але також може призвести до серйозних фінансових санкцій і шкоди репутації організації. Належні системи управління допомагають компаніям охорони здоров'я встановити чітку політику, процедури та засоби контролю для досягнення та підтримки відповідності, тим самим зменшуючи ризик витоку даних і порушень нормативних документів. Підсумовуючи, дотримання нормативних вимог і управління відіграють вирішальну роль у забезпеченні інформаційної безпеки в організаціях. Дотримуючись нормативних вимог і впроваджуючи надійні структури управління, компанії можуть ефективно захистити свої активи даних і зменшити ризик кіберзагроз. Організаціям важливо постійно контролювати та оновлювати свої програми відповідності, щоб усунути нові ризики безпеки та нормативні зміни. За допомогою проактивного підходу до дотримання нормативних вимог і управління компанії можуть покращити загальну безпеку та зміцнити довіру зі своїми зацікавленими сторонами. [40]

Для ефективного захисту від соціально-технічних атак організаціям вкрай важливо мати повне розуміння правових вимог щодо захисту даних. Дотримання таких законів, як GDPR у Європейському Союзі та CCPA у Сполучених Штатах є важливим для захисту конфіденційної інформації. Ці положення окреслюють права осіб щодо їхніх персональних даних, а також зобов'язання компаній, які обробляють ці дані. Забезпечуючи відповідність вимогам законодавства,

організації можуть зменшити ризики дорогих штрафів і репутаційної шкоди, які можуть виникнути внаслідок витоку даних або невідповідності. Крім того, розуміння законодавчих вимог щодо захисту даних також допомагає організаціям будувати довіру з клієнтами. Демонструючи відданість захисту особистої інформації та дотримуючись відповідних законів, компанії можуть підвищити свою репутацію та довіру в очах споживачів. Це може призвести до підвищення лояльності та задоволеності клієнтів, оскільки люди частіше довірятимуть організаціям, які надають пріоритет конфіденційності та безпеці даних. У сучасну цифрову епоху, коли витоки даних стають все більш поширеними, розвиток такого рівня довіри є важливим для підтримки лояльної клієнтської бази. Підсумовуючи, чітке розуміння законодавчих вимог щодо захисту даних має вирішальне значення для організацій, які прагнуть захистити конфіденційну інформацію та захистити від соціально-технічних атак. Дотримуючись таких нормативних актів, як GDPR і ССРА, компанії можуть уникнути юридичних наслідків, зміцнити довіру клієнтів і підвищити загальну кібербезпеку. Організаціям важливо бути в курсі законів про захист даних, що розвиваються, і гарантувати, що їх політика та практика відповідають цим вимогам, щоб ефективно пом'якшити ризики, пов'язані з витоком даних і невідповідністю.

#### **4.2. Впровадження багатфакторної автентифікації**

У сфері інформаційної безпеки впровадження MFA стало важливою стратегією для посилення захисту від соціотехнічних атак. MFA вимагає від користувачів надати дві або більше форм ідентифікації перед отриманням доступу до конфіденційних даних, таких як пароль і унікальний код, надісланий на їхній мобільний пристрій. Цей додатковий рівень безпеки значно знижує ймовірність несанкціонованого доступу та витоку даних. Дослідження показали, що MFA може знизити ризик компрометації облікового запису до 99,9%, що робить його ключовим компонентом комплексної системи безпеки. Крім того, прийняття MFA

демонструє проактивний підхід до захисту критично важливих інформаційних активів. Інтегруючи кілька факторів автентифікації, організації можуть мінімізувати ймовірність стати жертвою кіберзагроз, таких як фішинг або викрадення облікових даних. Інвестиції в технологію MFA не тільки захищають конфіденційні дані, але й допомагають зміцнити довіру клієнтів, які покладаються на безпечні транзакції та комунікації. Оскільки кібератаки продовжують вдосконалюватися, впровадження MFA стає важливим для випередження зловмисників і забезпечення цілісності цифрових операцій [34]. Підсумовуючи, розгортання багатофакторної автентифікації є необхідним заходом для зміцнення захисту інформаційної безпеки від соціально-технічних атак. У той час як традиційні методи автентифікації, такі як паролі, схильні до використання, MFA додає додатковий рівень перевірки, який значно зменшує вразливості. Вимагаючи кількох форм ідентифікації, організації можуть створити надійну систему безпеки, яка зменшить ризики, пов'язані з несанкціонованим доступом і витоком даних. Оскільки технологічний прогрес і загрози стають все більш поширеними, інтеграція MFA служить проактивним рішенням для захисту критично важливих активів і підтримки довіри в світі, що стає все більш цифровим.

Під час переддипломної практики в консалтинговій компанії, що спеціалізується на управлінні ризиками, кібербезпекою та аналітикою, я мала можливість детально ознайомитися з процесом впровадження MFA у реальних умовах. Моя робота включала аналіз існуючих методів автентифікації в компаніях-клієнтах та розробку рекомендацій щодо їх удосконалення шляхом впровадження MFA. Також я брала участь у проведенні оцінки ризиків, пов'язаних із потенційними кіберзагрозами, та виявленні вразливостей у системах ІБ клієнтів. Завдяки практичному досвіду я набула цінних знань щодо ефективних стратегій захисту ІС та значення багатофакторної автентифікації як одного з ключових компонентів кібербезпеки."

#### **4.3. Проведення регулярних тренінгів з питань безпеки та створення планів і протоколів реагування на інциденти**

У сфері інформаційної безпеки, особливо під час інцидентів безпеки, створення надійних протоколів зв'язку має першочергове значення для зменшення ризиків і підтримки цілісності конфіденційних даних. Поява пристроїв IoT у ненадійних мережах підкреслює важливість збереження анонімності та безпеки в каналах зв'язку [7]. Завдяки адаптації цибулевої маршрутизації до середовищ Інтернету речей можна значно зменшити ймовірність несанкціонованого доступу та витоку даних. Ця адаптація не тільки покращує конфіденційність, але й посилює наскрізну безпеку для пристроїв Інтернету речей, узгоджуючи надзвичайну потребу в безпечних протоколах зв'язку. Крім того, [8] підкреслює необхідність інноваційних заходів кібербезпеки, особливо перед обличчям нових загроз, таких як кібервійна. Представлення MicroToken Exchange™ (MTE) представляє новий підхід до безпечних архітектур керування даними, пропонуючи додатковий рівень захисту від кібератак. Заплутуючи потоки даних і роблячи конфіденційні дані команд невидимими для хакерів, MTE усуває вразливості під час передачі даних, підвищуючи стійкість протоколів зв'язку. Ця зміна парадигми безпеки даних не тільки покращує захист інформації, але й сприяє загальному стану кібербезпеки в складних технологічних екосистемах. У контексті інцидентів безпеки інтеграція передових технологій, таких як MTE та адаптована цибулева маршрутизація, може революціонізувати підхід до протоколів зв'язку. Ці інновації пропонують багатогранне рішення, забезпечуючи безпечну передачу даних, гарантуючи, що лише авторизовані сторони можуть отримати доступ до конфіденційної інформації та інтерпретувати її. Використовуючи висновки [7] і [8], організації можуть проактивно встановлювати комунікаційні протоколи, які не тільки запобігають порушенням і неавторизованому доступу, але й зміцнюють загальну стійкість їхніх структур інформаційної безпеки проти соціально-технічних атак.

Для ефективної боротьби з соціотехнічними атаками організації повинні надавати пріоритет регулярним впровадженням тренінги з питань безпеки для своїх співробітників. Такі навчальні програми відіграють ключову роль у забезпеченні персоналу знаннями та навичками, необхідними для виявлення потенційних загроз безпеці та реагування на них. Розвиваючи у працівників культуру свідомості безпеки, організації можуть значно зменшити ймовірність стати жертвою тактики соціальної інженерії чи інших форм кіберексплуатації. У цифровому середовищі, що швидко розвивається, де людська помилка залишається загальною вразливістю, інвестиції в безперервне навчання мають першочергове значення для зміцнення захисних механізмів організації. Крім того, проведення регулярних тренінгів з питань безпеки є профілактичним заходом для зменшення ризиків і захисту конфіденційної інформації від несанкціонованого доступу. Завдяки цим навчальним ініціативам співробітники краще розуміють важливість захисту даних і отримують можливість застосовувати безпечні методи у своїй повсякденній роботі [24]. Підвищуючи важливість конфіденційності, цілісності та доступності інформаційних активів, організації можуть виховувати робочу силу, яка дбає про безпеку, яка виступає в якості передового захисту від потенційних загроз. Оскільки поширеність внутрішніх загроз продовжує становити значний ризик для безпеки організації, надання співробітникам необхідних інструментів і знань, щоб розпізнавати підозрілу діяльність і повідомляти про неї, має вирішальне значення для підтримки надійної безпеки. Підсумовуючи, впровадження регулярних тренінгів з питань безпеки є важливим компонентом цілісного підходу до інформаційної безпеки. Навчаючи співробітників передовим практикам, новим загрозам і протоколам безпеки, організації можуть зміцнити свої механізми захисту від соціально-технічних атак і підвищити загальну стійкість кібербезпеки. Оскільки технології продовжують розвиватися, а суб'єкти загрози стають все більш витонченими у своїй тактиці, організації повинні залишатися пильними у забезпеченні своєї робочої сили навичками та обізнаністю, необхідними для захисту від потенційних ризиків [24]. Зрештою, інвестиції у комплексне навчання

безпеки не тільки захищають цінні активи організації, але й прищеплюють культуру свідомості безпеки, яка пронизує всі рівні організації.

Одним з найважливіших аспектів інформаційної безпеки в організаціях є створення системи реагування на інциденти. плани і протоколи. Ці плани служать дорожньою картою того, як ефективно та результативно реагувати на випадки порушення безпеки чи інциденту. Маючи ці плани, організації можуть мінімізувати вплив інциденту та швидко пом'якшити будь-яку потенційну шкоду своїй системіс і дані. Плани реагування на інциденти повинні окреслювати процедури виявлення, реагування на інциденти безпеки та відновлення після них, а також розподіл ролей і обов'язків для ключового персоналу в організації. Розробляючи плани реагування на інциденти, організації повинні враховувати такі фактори, як тип і ступінь серйозності потенційних загроз, конкретні потреби організації в безпеці та нормативні вимоги, які можуть застосовуватися. Важливо пристосувати плани реагування на інциденти до унікальних характеристик і вразливостей кожної організації, щоб забезпечити їх ефективність у вирішенні потенційних ризиків. Крім того, організації повинні регулярно тестувати та оновлювати свої плани реагування на інциденти, щоб враховувати нові загрози, зміни в технології та уроки, отримані з минулих інцидентів [35]. Загалом, створення надійних планів реагування на інциденти та протоколів є критично важливим компонентом загальної стратегії безпеки організації. Вкладаючи час і ресурси в розробку комплексних і ефективних планів, організації можуть краще захистити свої системи, дані та репутацію від зростаючої загрози кібератак. За допомогою чітко визначених протоколів організації можуть швидко й рішуче реагувати на інциденти безпеки, мінімізуючи потенційну шкоду та зберігаючи довіру клієнтів і партнерів. Підсумовуючи, плани реагування на інциденти слід розглядати як основоположний елемент цілісного підходу до інформаційної безпеки в організаціях.

#### 4.5. Навчання та освіта з кібербезпеки

Щоб ефективно боротися зі зростаючою загрозою кібератак, організаціям важливо віддавати пріоритет навчанню та освіті своїх співробітників з кібербезпеки. Завдяки комплексним навчальним програмам співробітники можуть краще усвідомити потенційні ризики безпеці та навчитися найкращим практикам захисту конфіденційної інформації. Крім того, постійне навчання може допомогти співробітникам бути в курсі останніх загроз кібербезпеці та методів запобігання, що зрештою зменшує ймовірність успішної кібератаки. Інвестуючи в навчання та освіту з кібербезпеки, організації можуть створити більш обізнану та пильну робочу силу, яка краще підготовлена для виявлення потенційних порушень безпеки та реагування на них. Крім того, навчання з кібербезпеки може сприяти розвитку культури обізнаності про безпеку в організації. Коли співробітники розуміють важливість кібербезпеки та свою роль у захисті конфіденційної інформації, вони, швидше за все, вживатимуть профілактичних заходів для захисту від потенційних загроз. Цей культурний зсув може призвести до покращення загальної безпеки та зниження ризику успішних атак [36]. Розвиваючи культуру обізнаності про безпеку, організації можуть створити більш стійкий захист від дедалі витонченіших тактик, які застосовують кіберзлочинці. Підсумовуючи, навчання та освіта з кібербезпеки є важливими компонентами комплексної стратегії безпеки. Інвестуючи в програми навчання та сприяючи культурі обізнаності про безпеку, організації можуть надати своїм співробітникам можливість стати активними учасниками захисту від кіберзагроз. Зрештою, добре навчена робоча сила є критично важливим захистом від кібератак, що розвиваються, і має важливе значення для збереження конфіденційності, цілісності та доступності конфіденційної інформації.

Для ефективної боротьби з соціотехнічними атаками в організаціях важливо поточні навчальні програми неможливо переоцінити. Ці програми відіграють вирішальну роль у інформуванні працівників про останні загрози кібербезпеці та

найкращі методи запобігання. Проводячи регулярні тренінги, співробітники можуть залишатися в курсі інформаційної безпеки, що постійно розвивається, гарантуючи, що вони готові розпізнавати потенційні атаки та ефективно реагувати на них. Без постійного навчання співробітники можуть стати самовдоволеними або не знати про ризики, залишаючи організацію вразливою до кіберзагроз. Крім того, поточні навчальні програми допомагають розвивати культуру безпеки в організації. Коли співробітникам регулярно нагадують про важливість інформаційної безпеки та надають їм знання та навички щодо захисту конфіденційних даних, вони, швидше за все, віддадуть пріоритет кібербезпеці у своїх щоденних завданнях. Така колективна пильність може створити міцну лінію захисту від соціотехнічних атак, оскільки співробітники стають активними учасниками захисту цифрових активів організації. Крім того, постійне навчання також може допомогти прищепити почуття відповідальності серед працівників, заохочуючи їх взяти на себе відповідальність за практику кібербезпеки [24]. Підсумовуючи, постійні навчальні програми є наріжним каменем ефективної практики інформаційної безпеки в організаціях. Інвестуючи в постійну освіту та розвиток співробітників, організації можуть створити обізнану та пильну робочу силу, яка краще підготовлена для виявлення та пом'якшення соціально-технічних атак. Ці програми не тільки надають співробітникам необхідні навички для захисту від кіберзагроз, але й сприяють розвитку культури обізнаності про безпеку, яка є важливою в сучасну цифрову епоху. Вкрай важливо, щоб організації віддавали пріоритет постійному навчанню як ключовому елементу своєї стратегії кібербезпеки, щоб випереджати потенційні загрози та захищати конфіденційну інформацію.

Враховуючи складний характер загроз ІБ, який постійно розвивається, це має вирішальне значення для організацій включити реальні сценарії у свої навчальні програми. Імітуючи реалістичні соціотехнічні атаки, співробітники можуть розвинути навички критичного мислення, необхідні для виявлення потенційних порушень безпеки та ефективного реагування на них. Дослідження

показали, що практичні навчальні вправи є більш захоплюючими та запам'ятовуються учасникам, що призводить до вищих показників утримання та кращої готовності до реальних загроз. Крім того, піддаючи співробітникам різноманітні сценарії, вони можуть допомогти їм зрозуміти різні мотиви та тактики, які використовують зловмисники, дозволяючи їм ефективніше передбачати та зменшувати ризики. Крім того, включення реальних сценаріїв у навчання може допомогти подолати розрив між теоретичними знаннями та практичним застосуванням. Співробітники швидше розуміють важливість протоколів безпеки, коли бачать, як ці заходи безпосередньо впливають на їх повсякденну роботу. Цей практичний підхід не тільки покращує їхнє розуміння найкращих практик кібербезпеки, але й заохочує культуру пильності в організації [24]. Роблячи тренінги більш релевантними та пов'язаними з посадовими ролями співробітників, організації можуть гарантувати, що кібербезпека залишається головним пріоритетом на всіх рівнях робочої сили. Загалом, інтеграція реальних сценаріїв у навчальні програми має важливе значення для підготовки працівників до протистояння дедалі складнішим соціотехнічним атакам, які загрожують ІБ. Занурюючи учасників у реалістичне моделювання, організації можуть розвивати проактивне мислення щодо кібербезпеки та розширювати можливості їхній персонал повинен діяти рішуче у разі порушення. Зважаючи на швидкий технологічний прогрес і зростаючу поширеність гібридних загроз, вкрай важливо, щоб організації інвестували в комплексні та динамічні навчальні ініціативи, які відображають складність сучасного цифрового ландшафту.

Залучаючи професіоналів, які володіють передовими знаннями та практичними навичками з кібербезпеки, співробітники можуть отримати вигоду від актуальної інформації та передового досвіду. Ця співпраця може надати цінну інформацію про останні загрози безпеці та тенденції, озброївши співробітників необхідними інструментами для захисту конфіденційних даних і зменшення ризиків. Крім того, експерти галузі можуть запропонувати вказівки щодо впровадження надійних заходів безпеки, адаптованих до конкретних потреб

організації, забезпечуючи комплексну та ефективну стратегію безпеки. Крім того, партнерство з галузевими експертами під час тренінгів може сприяти розвитку культури постійного навчання та вдосконалення в організації. Завдяки залученню зовнішніх експертів співробітники отримують доступ до різноманітних точок зору та інноваційних підходів до інформаційної безпеки. Ця інформація може надихнути на творчість і критичне мислення, заохочуючи співробітників бути в курсі розвитку кібербезпеки. Крім того, співпраця з галузевими експертами може допомогти побудувати міцніші мережі та партнерства в рамках спільноти кібербезпеки, відкриваючи двері для потенційної співпраці та можливостей обміну знаннями, які можуть ще більше підвищити рівень безпеки організації. Підсумовуючи, залучення досвіду професіоналів галузі для навчальних сесій є стратегічним вкладенням у зміцнення можливостей інформаційної безпеки організації. Використовуючи зовнішні ресурси знань, співробітники можуть отримати безцінні навички та знання, які можуть допомогти зміцнити захист організації від соціотехнічних атак. Завдяки безперервній співпраці з галузевими експертами організації можуть культивувати націленість на безпеку, надавати співробітникам можливість активно вирішувати проблеми безпеки та, зрештою, захистити критично важливі активи від потенційних загроз. Цей спільний підхід не тільки підвищує стійкість організації до безпеки, але й сприяє культурі інновацій і постійному вдосконаленню методів інформаційної безпеки. [37]

#### **4.6. Технологічні рішення для соціотехнічних атак та впровадження розширених систем виявлення загроз**

Щоб протистояти зростаючій загрозі соціотехнічних атак, організації повинні впроваджувати передові технологічні рішення, які виходять за рамки традиційних заходів кібербезпеки. Одним із таких рішень є використання ШІ і алгоритмів машинного навчання для виявлення підозрілих моделей і аномалій у поведінці користувачів. Використовуючи ці технології, організації можуть

завчасно виявляти й пом'якшувати потенційні загрози, перш ніж вони переростуть у повномасштабні атаки. Крім того, інструменти на основі штучного інтелекту можуть безперервно контролювати системи та мережі, забезпечуючи в режимі реального часу інформацію про будь-які відхилення від нормальної діяльності, таким чином підвищуючи загальну безпеку. Крім того, впровадження надійних протоколів шифрування може значно підвищити захист від соціально-технічних атак. Використання наскрізного шифрування гарантує, що конфіденційні дані залишаються в безпеці як під час передачі, так і в стані спокою, що ускладнює зловмисникам перехоплення чи підробку інформації. Організації також повинні враховувати двикористання захищених каналів зв'язку, таких як VPN і сертифікати SSL, для встановлення безпечного з'єднання між користувачами та системами. Ці заходи шифрування не тільки захищають цілісність даних, але й підвищують загальну стійкість проти тактик соціальної інженерії, які застосовуються в соціотехнічних атаках. Крім того, використання розширеної аналітики та платформ аналізу загроз може надати організаціям цінну інформацію про нові вектори атак і тактики, які використовують кіберзлочинці. Використовуючи можливості аналітики великих даних, організації можуть завчасно виявляти потенційні вразливості у своїх системах і розробляти цільові стратегії для зменшення ризиків, пов'язаних із соціотехнічними атаками. Крім того, платформи аналізу загроз можуть агрегувати та аналізувати дані з різних джерел, щоб надавати дієву інформацію про потенційні загрози, дозволяючи організаціям бути на крок попереду кіберсупротивників. Зрештою, шляхом інтеграції цих технологічних рішень у свою систему кібербезпеки організації можуть посилити свої механізми захисту від соціально-технічних атак і краще захистити свої цифрові активи.

У світлі дедалі складнішого кіберзагроз організації повинні вживати профілактичних заходів для захисту своїх конфіденційна інформація. Впровадження передових систем виявлення загроз має вирішальне значення для захисту як від відомих, так і від нових загроз у цифровому середовищі. Ці системи використовують передові технології, такі як алгоритми машинного навчання та

аналіз поведінки, щоб виявляти аномалії та потенційні порушення безпеки в режимі реального часу. Завдяки безперервному моніторингу мережевого трафіку та поведінки користувачів ці рішення можуть значно підвищити здатність організації виявляти й реагувати на потенційні загрози до їх ескалації. Крім того, передові системи виявлення загроз можуть надати організаціям цінну інформацію про загальну безпеку. Аналізуючи моделі та тенденції кібератак, ці системи можуть допомогти виявити вразливі місця в існуючих заходах безпеки та визначити пріоритети для покращення. Такий проактивний підхід до кібербезпеки зрештою може допомогти організаціям краще захистити свої активи та зменшити потенційні ризики для їх діяльності. Більше того, дані, зібрані цими системами, можуть допомогти у створенні більш надійних політик і процедур безпеки, адаптованих до конкретних потреб організації [38]. Підсумовуючи, впровадження передових систем виявлення загроз є важливим у сучасному складному ландшафті загроз. Інвестуючи в ці передові технології, організації можуть посилити захист кібербезпеки та бути на крок попереду зловмисників. Крім того, інформація, яку надають ці системи, може інформувати про прийняття стратегічних рішень і допомагати організаціям постійно покращувати рівень безпеки. Оскільки кіберзагрози продовжують розвиватися, організації повинні використовувати інноваційні рішення для захисту своїх критично важливих активів і забезпечення безперервності бізнесу.

#### **4.7. Використання штучного інтелекту для моніторингу безпеки**

Використання штучного інтелекту (ШІ) для моніторингу безпеки з'явилося як перспективний підхід до підвищення можливостей виявлення загроз і реагування. Системи на основі штучного інтелекту можуть аналізувати величезні обсяги даних у режимі реального часу, дозволяючи організаціям виявляти підозрілу діяльність і потенційні вразливості точніше й ефективніше, ніж традиційні методи. Використовуючи алгоритм машинного навчання Таким чином,

ці системи можуть постійно адаптуватися та вчитися на нових загрозах, підвищуючи свою ефективність з часом. Цей проактивний підхід може допомогти організаціям випередити зловмисників, які постійно вдосконалюють свою тактику, щоб обійти традиційні заходи безпеки. Крім того, ШІ може відігравати вирішальну роль в автоматизації повторюваних завдань, таких як аналіз журналів і моніторинг, звільняючи персонал безпеки, щоб зосередитися на більш стратегічних ініціативах. Це може призвести до підвищення ефективності роботи та скорочення часу реагування на інциденти безпеки. Крім того, системи моніторингу безпеки на основі штучного інтелекту можуть надати організаціям цінну інформацію про їх мережеву інфраструктуру та моделі поведінки користувачів, дозволяючи їм визначати потенційні ризики та вживати проактивних заходів для їх пом'якшення [39]. Використовуючи технології штучного інтелекту, організації можуть посилити свої існуючі заходи безпеки та посилити загальний захист від складних кіберзагроз. Хоча переваги використання ШІ для моніторингу безпеки очевидні, організаціям важливо усвідомлювати обмеження та потенційні ризики, пов'язані з цими технологіями. Системи штучного інтелекту не захищені від упередженості та помилок, які можуть призвести до помилкових спрацьовувань або негативів під час виявлення загроз. Організаціям вкрай необхідно впроваджувати ретельні процеси тестування та перевірки, щоб забезпечити точність і надійність рішень безпеки на основі ШІ. Крім того, етичні наслідки штучного інтелекту в моніторингу безпеки, такі як питання конфіденційності та захисту даних, повинні бути ретельно розглянуті та розглянуті, щоб зберегти довіру та прозорість із зацікавленими сторонами. Оскільки організації продовжують використовувати ШІ для моніторингу безпеки, цілісний підхід, який поєднує людський досвід із можливостями штучного інтелекту, буде необхідним для ефективного зниження ризиків і захисту критичних активів від нових кіберзагроз.

#### **4.8. Інтеграція аналізу поведінки та реагування на інциденти**

Для підвищення рівня безпеки щоб організації могли протистояти новим кіберзагрозам, вкрай важливо інтегрувати аналітику поведінки в існуючі інструменти безпеки. Використовуючи аналітику поведінки, організації можуть досягти проактивного підходу до виявлення аномалій і підозрілих дій у своїй мережевій інфраструктурі. Традиційні інструменти безпеки часто покладаються на методи, засновані на сигнатурах, які можуть бути неефективними проти прогресивних і нових загроз. Поведінкова аналітика, з іншого боку, може допомогти виявити відхилення від нормальних моделей поведінки користувачів, дозволяючи завчасно виявити потенційні порушення безпеки. Цей перехід до більш динамічної та адаптивної стратегії безпеки є важливим у сучасному складному ландшафті загроз. Крім того, інтеграція поведінкової аналітики в інструменти безпеки може надати організаціям цінну інформацію про дії користувачів і взаємодію з критично важливими системами та даними. Аналізуючи моделі поведінки користувачів, служби безпеки можуть краще зрозуміти наміри та мотивацію певних дій, що дозволить їм приймати більш обґрунтовані рішення під час реагування на інциденти безпеки. Це не тільки підвищує здатність організації виявляти внутрішні загрози, але й покращує загальну ефективність роботи за рахунок зменшення помилкових спрацьовувань і втоми від сповіщень. Оскільки організації продовжують стикатися зі складними кібератаками, потреба в передових технологіях безпеки, таких як поведінкова аналітика, стає все більш важливою. Крім того, впровадження поведінкової аналітики також може допомогти організаціям відповідати нормативним вимогам і галузевим стандартам, надаючи детальні журнали аудиту та докази належної обачності у захисті конфіденційної інформації. Демонструючи проактивний підхід до моніторингу безпеки та виявлення загроз, організації можуть зменшити ризик недотримання вимог і потенційних штрафів. Крім того, деталізована аналітика поведінки може

допомогти організаціям провести ретельні розслідування після інциденту, дозволяючи їм визначити першопричини та вжити заходів для запобігання майбутнім порушенням безпеки. Загалом, інтеграція поведінкової аналітики в інструменти безпеки має вирішальне значення не лише для посилення захисту кібербезпеки, але й для забезпечення дотримання нормативних вимог і захисту активів конфіденційних даних.

Розглядаючи розробку планів реагування на інциденти в контексті інформаційної безпеки, це Важливо розставити пріоритети для встановлення чітких ролей і обов'язків в організації. Це включає призначення групи реагування, визначення їхніх обов'язків та забезпечення ефективної координації та комунікації. Чітко визначивши, хто несе відповідальність за які дії у випадку інциденту безпеки, організації можуть оптимізувати свої зусилля з реагування та зменшити потенційну плутанину чи затримки. За словами , наявність чітко визначеної групи реагування на інциденти може значно підвищити здатність організації виявляти, реагувати на порушення безпеки та відновлювати їх. ВКрім чіткого визначення ролей і обов'язків, плани реагування на інциденти також повинні включати детальні процедури виявлення та аналізу інцидентів безпеки. Це передбачає налаштування систем моніторингу, впровадження механізмів оповіщення та проведення регулярних оцінок безпеки для проактивного виявлення вразливостей. Встановивши надійний процес виявлення та аналізу, організації можуть покращити свою здатність своєчасно виявляти інциденти безпеки та оцінювати ступінь збитку. Раннє виявлення має вирішальне значення для мінімізації впливу порушень безпеки та запобігання подальшому злому конфіденційної інформації [35]. Крім того, плани реагування на інциденти повинні включати стратегії стримування, викорінення та відновлення для ефективного управління інцидентами безпеки та мінімізації їх впливу на організаційні операції. Це включає ізоляцію уражених систем, видалення шкідливих компонентів, відновлення даних із резервних копій і впровадження заходів для запобігання майбутнім інцидентам. Окреслюючи чіткі та систематичні процедури стримування, викорінення та відновлення, організації

можуть прискорити свої зусилля з реагування та зменшити загальну шкоду, спричинену інцидентами безпеки. Добре структурований план реагування на інциденти необхідний організаціям для ефективної навігації та своєчасного й ефективного відновлення після порушень безпеки [35].

#### **4.9. Тренування безпеки, симуляції, постійний моніторинг та оцінка**

Для ефективного захисту від соціотехнічних атак організаціям вкрай важливо проводити регулярні тренування з безпеки та симуляції. Ці навчання допомагають перевірити готовність співробітників і систем до різних загроз безпеки. Імітуючи реальні сценарії в контрольованому середовищі, організації можуть виявити вразливі місця та прогалини у своїх заходах безпеки, дозволяючи їм вносити необхідні покращення до того, як станеться фактичне порушення. Такий проактивний підхід до безпеки може значно знизити ризик успішних атак і звести до мінімуму потенційну шкоду для репутації та фінансів організації. Крім того, тренування з безпеки та моделювання є цінними можливостями для навчання для співробітників на всіх рівнях організації. Завдяки участі в цих навчаннях люди можуть набути практичного досвіду реагування на інциденти з безпекою та ознайомитися з найкращими методами пом'якшення ризиків. Це не тільки допомагає покращити загальну культуру безпеки в організації, але й сприяє розвитку почуття відповідальності та пильності серед співробітників, коли йдеться про захист конфіденційної інформації. Таким чином, тренування з безпеки відіграють ключову роль у формуванні міцного мислення щодо безпеки серед співробітників, що робить їх важливим компонентом комплексної стратегії безпеки. На додаток до підвищення готовності та розвитку культури, орієнтованої на безпеку, регулярні тренування та симуляції безпеки також можуть допомогти організаціям відповідати вимогам відповідності та галузевим стандартам. Багато нормативно-правових актів і сертифікатів, як-от ISO 27001 і PCI DSS, вимагають впровадження тестування безпеки та навчальних програм для забезпечення

безпеки конфіденційних даних та інформаційних систем. Проводячи ці навчання на регулярній основі, організації можуть продемонструвати свою відданість дотриманню вимог безпеки та показати зацікавленим сторонам, що вони вживають активних заходів для захисту від потенційних загроз. Загалом, переваги проведення регулярних тренувань і симуляцій безпеки очевидні, що робить їх критичним елементом будь-якої надійної стратегії безпеки.

Для посилення заходів безпеки інформації та щоб зменшити ризики, пов'язані з соціотехнічними атаками, організаціям слід розглянути можливість проведення аудитів та оцінок відповідності. Проводячи регулярні аудити, компанії можуть оцінити свої поточні протоколи безпеки, виявити потенційні вразливості та переконатися, що вони відповідають відповідним нормам і стандартам. Аудити відповідності можуть надати цінну інформацію про ефективність існуючих заходів безпеки та допомогти організаціям завчасно усунути будь-які прогалини або слабкі місця в їхній системі безпеки. Крім того, оцінки відповідності можуть допомогти організаціям оцінити свій рівень дотримання нормативних вимог, галузевих стандартів і передового досвіду. Завдяки всебічній оцінці компанії можуть виявити області, де вони можуть не відповідати нормам, і вжити заходів для покращення безпеки. Регулярно проводячи оцінку відповідності, організації можуть продемонструвати свою відданість захисту конфіденційних даних і захисту від соціально-технічних атак, зрештою зміцнюючи довіру клієнтів, партнерів та інших зацікавлених сторін. Загалом, впровадження аудитів відповідності ай оцінки можуть відігравати вирішальну роль у зміцненні захисту інформаційної безпеки та мінімізації ймовірності соціотехнічних атак. Регулярно оцінюючи свої методи безпеки та забезпечуючи відповідність відповідним нормам, організації можуть краще захистити свої активи та конфіденційну інформацію від зловмисників. Підприємствам важливо постійно оцінювати та вдосконалювати свої заходи безпеки, щоб адаптуватися до нових загроз і підтримувати надійний захист від соціально-технічних атак [41]. еволюціонуючий характер соціально-технічних атак, для організацій вкрай важливо розвивати культуру підзвітності та

відповідальності серед своїх співробітників. Це передбачає встановлення чітких очікувань щодо протоколів і процедур інформаційної безпеки, а також притягнення осіб до відповідальності за їхні дії. Створюючи культуру, в якій співробітники розуміють важливість захисту конфіденційних даних і потенційні наслідки їх невиконання, організації можуть значно знизити ризики порушень безпеки. Крім того, призначення відповідальності за моніторинг і застосування заходів безпеки може допомогти гарантувати, що працівники дотримуються високих стандартів, коли йдеться про захист конфіденційної інформації. Крім того, виховання культури підзвітності та відповідальності також може сприяти активній участі в ініціативах безпеки. Коли співробітники відчують себе уповноваженими взяти на себе відповідальність за інформаційну безпеку в своїй організації, вони, швидше за все, братимуть активну участь у виявленні вразливостей і впровадженні необхідних заходів безпеки. Такий рівень взаємодії може призвести до більш надійної безпеки, оскільки люди в організації працюють разом, щоб зміцнити захист від потенційних загроз. Крім того, наголошуючи на індивідуальній відповідальності за практику безпеки, організації можуть створити міцну основу для колективної культури пильності та спільного зобов'язання щодо захисту цінних активів даних. Підсумовуючи, створення культури підзвітності та відповідальності має важливе значення для підвищення інформаційної безпеки в організаціях. Встановлюючи чіткі очікування, запроваджуючи наслідки за невиконання вимог і дозволяючи працівникам взяти на себе відповідальність за методи безпеки, організації можуть посилити свій захист від соціально-технічних атак. Цей проактивний підхід не тільки знижує ризик порушення безпеки, але й сприяє розвитку культури пильності та співпраці, коли люди працюють разом, щоб захистити цінні активи даних. Завдяки цим зусиллям організації можуть краще захистити свої ІС та адаптуватися до постійно мінливого ландшафту загроз кібербезпеці. [40]

Для ефективного захисту від соціально-технічних атак необхідний постійний моніторинг і оцінка заходів безпеки мають вирішальне значення. Завдяки постійному моніторингу мереж, систем і поведінки користувачів організації

можуть завчасно виявляти будь-які підозрілі дії або вразливості, якими можуть скористатися зловмисники. Моніторинг у режимі реального часу дозволяє негайно реагувати на потенційні загрози та пом'якшувати їх, перш ніж вони переростуть у повномасштабні порушення безпеки. Цей проактивний підхід є необхідним у сучасному динамічному цифровому середовищі, де кіберзагрози постійно розвиваються та стають все більш витонченими. Крім того, безперервна оцінка протоколів і практик безпеки дозволяє організаціям адаптувати та посилювати захист у відповідь на нові загрози. Регулярні оцінки безпеки, тестування на проникнення та сканування вразливостей допомагають виявити слабкі місця в системі безпеки та надати розуміння тих областей, які потребують покращення. Проводячи регулярні оцінки, організації можуть випереджати потенційні ризики та впроваджувати необхідні зміни для посилення загальної безпеки. Цей ітеративний процес моніторингу та оцінки є важливим для підтримки надійного та стійкого захисту від соціотехнічних атак. Підсумовуючи, постійний моніторинг і оцінка є важливими компонентами комплексної стратегії інформаційної безпеки. Постійно оцінюючи заходи безпеки, відстежуючи потенційні загрози та оцінюючи ефективність заходів безпеки, організації можуть ефективно захищатися від соціально-технічних атак. Цей проактивний підхід не тільки допомагає зменшити ризики безпеки, але й гарантує, що організації зможуть адаптуватися та своєчасно реагувати на нові загрози. Зробивши постійний моніторинг і оцінку пріоритетом, організації можуть бути на крок попереду кіберзагроз і ефективно захищати свої конфіденційні дані та активи. [24]

Оскільки організації орієнтуються в складному ландшафті інформаційної безпеки, впровадження постійного моніторингу безпеки стає важливою стратегією для зменшення ризиків і виявлення потенційних загроз у режимі реального часу. Безперервний моніторинг виходить за рамки традиційних періодичних оцінок, забезпечуючи постійний потік даних, що дозволяє швидко реагувати та вживати заходів з усунення несправностей. Цей проактивний підхід дозволяє організаціям не тільки зміцнити свої механізми захисту, але й адаптуватися до нових загроз у

динамічному середовищі. Застосовуючи інструменти та технології, які автоматизують процес моніторингу, організації можуть покращити рівень безпеки та випередити кіберзлочинців. Крім того, постійний моніторинг безпеки узгоджується з концепцією поглибленого захисту, багаторівневої стратегії безпеки, яка наголошує на кількох захисних заходах для захисту від різноманітних загроз. Інтегруючи постійний моніторинг у існуючі системи безпеки, організації можуть створити надійну лінію захисту, яка доповнює інші засоби контролю безпеки, такі як брандмауери, антивірусне програмне забезпечення та системи виявлення вторгнень. Цей багаторівневий підхід підвищує ймовірність виявлення та блокування потенційних порушень на різних етапах життєвого циклу атаки, мінімізуючи вплив безпекиінциденти щодо критичних активів і даних. Підсумовуючи, впровадження безперервного моніторингу безпеки є проактивним і стратегічним вкладенням у захист організаційних активів і конфіденційної інформації. Інтегрувавши цю практику у свої протоколи безпеки, організації можуть підвищити свою стійкість проти кіберзагроз і забезпечити своєчасне реагування на потенційні інциденти безпеки. Оскільки цифровий ландшафт продовжує розвиватися, впровадження безперервного моніторингу безпеки буде необхідним для підтримки надійної безпеки та захисту від зростаючої складності кіберзагроз [46].

Організаціям вкрай важливо визначати пріоритетність регулярних оцінок і аудитів безпеки, щоб захиститися від нових загроз кібербезпеці. Ці оцінки служать профілактичними заходами для виявлення вразливостей в існуючій інфраструктурі безпеки, що дозволяє компаніям усунути ці недоліки до того, як ними скористаються зловмисники. Проводячи ретельні аудити, організації можуть отримати всебічне розуміння свого поточного стану безпеки, що дозволить їм приймати обґрунтовані рішення щодо інвестицій у безпеку та вдосконалення. Цей проактивний підхід не тільки підвищує стійкість організації до порушень безпеки, але й демонструє прагнення підтримувати цілісність даних і захистити конфіденційну інформацію. Крім того, безперервні оцінки та аудити безпеки

сприяють підвищенню загальної обізнаності про безпеку в організації. Завдяки регулярній оцінці протоколів і методів безпеки співробітники краще усвідомлюють потенційні ризики та важливість дотримання встановлених інструкцій з безпеки. Така підвищена обізнаність сприяє розвитку культури безпеки, коли люди на всіх рівнях організації активно сприяють захисту конфіденційних даних. Крім того, регулярні аудити дають можливість посилити навчання та освіту з безпеки, гарантуючи, що співробітники мають знання та навички, необхідні для ефективного пом'якшення загроз безпеці [47]. Крім того, проведення регулярних оцінок безпеки та аудитів не тільки зміцнює механізми захисту організації, але й демонструє відповідність нормативним вимогам і галузевим стандартам. Багато регулюючих органів і галузевих структур вимагають регулярних оцінок безпеки, щоб оцінити дотримання організацією конкретних інструкцій і протоколів безпеки. Забезпечуючи дотримання цих вимог, організації можуть уникнути дорогих штрафів і репутаційної шкоди внаслідок їх невиконання. Завдяки впровадженню регулярних перевірок безпеки організації можуть активно демонструвати свою прихильність підтримці безпечного середовища для обробки та обробки даних, зміцнюючи довіру як із зацікавленими сторонами, так і з клієнтами. Цей стратегічний підхід не тільки зменшує ризики, але й позиціонує організацію як відповідального зберігача конфіденційної інформації у все більш взаємопов'язаному цифровому ландшафті.

## ВИСНОВКИ

Узагальнюючи ключові моменти, розглянуті в цьому аналізі соціальних факторів інформаційної безпеки, стає очевидним, що людський фактор відіграє вирішальну роль як у вразливості, так і в захисті проти соціотехнічних атак. По-перше, особи в організаціях можуть несвідомо сприяти порушенням безпеки через такі дії, як натискання шкідливих посилань або обмін конфіденційною інформацією. Це підкреслює потребу в комплексних програмах навчання безпеки, щоб навчити співробітників передовим практикам і потенційним ризикам. Крім того, організаційна культура та структура можуть як підтримувати, так і перешкоджати зусиллям щодо захисту інформації. Культура, яка надає пріоритет безпеці та сприяє відкритому спілкуванню щодо потенційних загроз, може допомогти пом'якшити вплив соціально-технічних атак. Крім того, взаємозв'язок між технологією та поведінкою людини є ключовим фактором у розумінні та запобіганні соціотехнічним атакам. Оскільки технології продовжують розвиватися, розвиваються також і методи, які використовують кіберзлочинці для використання вразливостей людини. Для організацій вкрай важливо постійно адаптувати свої заходи безпеки для протидії цим мінливим загрозам. Крім того, зростаючий взаємозв'язок сучасного суспільства означає, що люди більше піддаються потенційним ризикам безпеки як у своєму особистому, так і в професійному житті. Це підкреслює важливість впровадження надійних протоколів безпеки, які захищають конфіденційну інформацію на різних платформах і пристроях. Підсумовуючи, рекомендації щодо посилення захисту від соціально-технічних атак передбачають багатогранний підхід, який стосується як технологічних, так і людських факторів. Віддаючи пріоритет тренінгам з питань безпеки, розвиваючи організаційну культуру, що піклується про безпеку, і залишаючись в курсі нових загроз, організації можуть краще захистити свої дані та системи від зловмисників. Зрештою, всебічне розуміння соціальної динаміки в ІБ має важливе значення для

розробки ефективних стратегій боротьби з соціально-технічними атаками та пом'якшення їхнього потенційного впливу.

Розуміння складного взаємозв'язку між соціальними факторами та інформаційною безпекою є має першочергове значення для захисту від кіберзагроз, що розвиваються. Хоча технічні заходи є основоположними для захисту даних, нехтування людським фактором робить організації вразливими для соціально-технічних атак. Дослідження показали, що значна кількість порушень безпеки є результатом людських помилок або маніпуляцій, що підкреслює критичну важливість урахування соціальних факторів у протоколах безпеки. Приоритезуючи такі аспекти, як навчання з питань кібербезпеки, створення культури підзвітності та впровадження суворого контролю доступу, організації можуть зменшити ризики, пов'язані з тактикою соціальної інженерії та внутрішніми загрозами. Крім того, суспільні норми та поведінка відіграють ключову роль у формуванні ефективності стратегій інформаційної безпеки. Людська психологія, упередження та моделі поведінки впливають на сприйнятливість людей до фішингу, атак соціальної інженерії та інших форм маніпуляцій з боку зловмисників [49]. Визнання та усунення цих соціальних факторів може підвищити загальну стійкість заходів безпеки, гарантуючи, що персонал не тільки оснащений технічними знаннями для захисту даних, але й усвідомлює, що дозволяє розпізнавати потенційні ризики безпеці та ефективно реагувати на них. Підсумовуючи, неможливо переоцінити важливість звернення до соціальних факторів в ІБ. Для ефективного захисту від соціотехнічних атак організації повинні прийняти цілісний підхід, який поєднує технічні рішення з соціальною обізнаністю та поведінковими розуміннями. Визнаючи людський фактор у кібербезпеці та впроваджуючи заходи для навчання, залучення та розширення можливостей персоналу, бізнес. Вони можуть зміцнити свій захист і зменшити ймовірність стати жертвою складних тактик соціальної інженерії. Зрештою, комплексна стратегія безпеки, яка враховує соціальні фактори разом із технічними засобами контролю,

має важливе значення для пом'якшення загроз, що постійно розвиваються в цифровій сфері.

Щоб ефективно боротися зі зростаючою загрозою соціально-технічних атак, це Вкрай важливо, щоб організації вжили негайних заходів для реалізації рекомендацій, висунутих експертами в галузі інформаційної безпеки. Ці рекомендації є результатом обширних досліджень і аналізу минулих атак, а також сучасних тенденцій у кіберзлочинності. Дотримуючись цих рекомендацій, організації можуть значно зменшити свою вразливість до атак, які використовують як технічні, так і людські вразливості. Однією з ключових рекомендацій є впровадження багатофакторної автентифікації в усіх системах і платформах. Цей додатковий рівень безпеки може допомогти запобігти несанкціонованому доступу до конфіденційної інформації, навіть якщо паролі зламано. Крім того, організації повинні надавати пріоритет навчанням і програмам підвищення обізнаності співробітників, щоб навчити персонал останнім тактикам, які використовують кіберзлочинці. Розвиваючи в організації культуру свідомості безпеки, співробітники можуть стати передовою лінією захисту від соціально-технічних атак. Підсумовуючи, заклик до дії для впровадження рекомендацій щодо захисту від соціотехнічних атак неможливо недооцінити. Наслідки успішної атаки можуть бути руйнівними як у фінансовому плані, так і в репутації. Організації зобов'язані визначити пріоритетність заходів кібербезпеки та інвестувати в необхідні ресурси для зміцнення свого захисту. Вживаючи проактивних заходів зараз, організації можуть краще захистити свої системи та дані від тактики зловмисників у цифровій сфері, що постійно розвивається.

## СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Omer Mahmood Watto, Muhammad Islam, Syed Arshad Hussain, Muhammad Shahab (2024), *"Cyber Law and Cyber Security Policies in Pakistan: A Comparative Study with USA, Canada and Australia"*
2. Yijie Weng, Jianhao Wu (2024), *"Fortifying the Global Data Fortress: A Multidimensional Examination of Cyber Security Indexes and Data Protection Measures across 193 Nations"*
3. Sopilko, Lesya Rapatska (2023), *"Social-legal foundations of information security of the state, society and individual in Ukraine"*
4. Puspita Kencana Sari, Putu Wuri Handayani, Achmad Nizar Hidayanto, Pribadi Wiranda Busro (2023), *"How Information Security Management Systems Influence the Healthcare Professionals' Security Behavior in a Public Hospital in Indonesia"*
5. Lei Zhang, Lina Ge (2024), *"A clustering-based differential privacy protection algorithm for weighted social networks."*, pp. 3755-3773
6. Guoying Qiu, Guoming Tang, Chuandong Li, Deke Guo, Yulong Shen, Yan Gan (2024), *"Behavioral-Semantic Privacy Protection for Continual Social Mobility in Mobile-Internet Services"*, pp. 462-477
7. Jens Hiller, J. Pennekamp, Markus Dahlmanns, Martin Henze, A. Panchenko, Klaus Wehrle (2019), *"Tailoring Onion Routing to the Internet of Things: Security and Privacy in Untrusted Environments"*, pp. 1-12
8. Dariusz G. Mikulski, Steven R. Russo (2018), *"MICROTOKEN EXCHANGE (MTE) FOR SECURING DIGITAL DATA FROM CYBER WARFARE ATTACKS"*
9. Capt. Nana Raymond Lawrence Ofosu-Boateng, Z. Jiping (2020), *"A Pestle Analysis of Maritime Piracy and Maritime Security in the Gulf of Guinea"*, pp. 472-482
10. Marius Stefan (2024), *"Agile transformation and performing management of IT and cyber security projects, at the government level"*

11. Georgiana-Daniela Lupulescu (2024), *"Revealing Hybrid Threats: Vulnerability Exploitation in Romania's Social Media Landscape"*
12. S. Lysenko, Volodymyr Vorobiov, Oleksandr Bokhonko, Piotr Gaj, O. Savenko, Jacek Wołoszyn (2023), *"Social Engineering Attacks Detection Approach"*, pp. 1-7
13. Md Abdus Shobur, Kazi Nazrul Islam, Md. Humayun Kabir, Anwar Hossain (2023), *"A CONTRADISTINCTION STUDY OF PHYSICAL VS. CYBERSPACE SOCIAL ENGINEERING ATTACKS AND DEFENSE."*
14. Pan Lv, Xiaodong Zhu, Hongli Tian (2024), *"The Impact of Social Sharing Based on Virtual Community on the Purchase Intention of Gen Z"*
15. Issam Alhadid, Evon M. O. Abu-Taieh, Mohammad Al Rawajbeh, Rami Suleiman Alkhawaldeh, Sufian M Khwaldeh, Suha Afaneh, Ala'aldin Alrowwad, Dima Farhan Alrwashdeh (2023), *"Evaluating the influence of security considerations on information dissemination via social networks"*
16. L. ey, C. V. Bennett, Harriet Dorothy Quinn-Scoggins, D. Nuttall, David Wilkins, Alison Mary Kemp (2024), *"Factors Influencing Clinicians', Health Visitors' and Social Workers' Professional Judgements, Decision-Making and Multidisciplinary Collaboration When Safeguarding Children with Burn Injuries: A Qualitative Study"*
17. Ahmad Jauhari Hamid Ripki (2023), *"Educational Management Strategies to Address Information Security Challenges in the Use of Social Media in Learning Environments"*
18. Mohamed, Norshidah (2015-10-19), *"Critical Socio-Technical Issues Surrounding Mobile Computing"*, IGI Global
19. Myriam Dunn Cavelty, Andreas Wenger (2022-02-15), *"Cyber Security Politics"*, Routledge
20. Nathan Clarke, Steven Furnell (2015), *"Proceedings of the Ninth International Symposium on Human Aspects of Information Security & Assurance (HAISA 2015)"*, Lulu.com

21. Dennis Hansen (2017-01-02), "*Project SAVE*", Royal Danish Defence College
22. Stephen J Zaccaro, Reeshad S. Dalal, Lois E. Tetrick, Julie A. Steinke (2016-09-19), "*Psychosocial Dynamics of Cyber Security*", Routledge
23. Narasimha Rao Vajjhala, Kenneth David Strang (2023-07-20), "*Cybersecurity for Decision Makers*", CRC Press
24. Bill Gardner, Valerie Thomas (2014-08-12), "*Building an Information Security Awareness Program*", Elsevier
25. Onwubiko, Cyril (2012-01-31), "*Situational Awareness in Computer Network Defense: Principles, Methods and Applications*", IGI Global
26. Thomas Groß, Luca Viganò (2021-06-21), "*Socio-Technical Aspects in Security and Trust*", Springer Nature
27. Vania Gatseva Dimitrova, Panagiotis Germanakos, Styliani Kleanthous (2021-01-11), "*Article Collection on Human Aspects in Adaptive and Personalized Interactive Environments (HAAPIE)*", Frontiers Media SA
28. Antonios Andreatos, Christos Douligieris (2023-06-22), "*ECCWS 2023 22nd European Conference on Cyber Warfare and Security*", Academic Conferences and publishing limited
29. Thomas Groß, Theo Tryfonas (2021-05-10), "*Socio-Technical Aspects in Security and Trust*", Springer Nature
30. Brij B. Gupta, Somya Ranjan Sahoo (2021-02-26), "*Online Social Networks Security*", CRC Press
31. Salvatore J. Stolfo, Steven M. Bellovin, Shlomo Hershkop, Angelos D. Keromytis, Sara Sinclair, Sean W. Smith (2008-08-29), "*Insider Attack and Cyber Security*", Springer Science & Business Media
32. Paolo Mori, Steven Furnell, Olivier Camp (2018-06-11), "*Information Systems Security and Privacy*", Springer
33. Jeffrey M. Stanton, Kathryn R. Stam (2006), "*The Visible Employee*", Information Today, Inc.

34. Marco Fanti (2023-06-28), *"Implementing Multifactor Authentication"*, Packt Publishing Ltd

35. Akashdeep Bhardwaj, Varun Sapra (2021-07-07), *"Security Incidents & Response Against Cyber Attacks"*, Springer Nature

36. Jannie Zaiman, Louise Leenan (2015-02-24), *"Iccws 2015 - The Proceedings of the 10th International Conference on Cyber Warfare and Security"*, Academic Conferences Limited

37. Hossein Bidgoli (2006-03-10), *"Handbook of Information Security, Information Warfare, Social, Legal, and International Issues and Security Foundations"*, John Wiley & Sons

38. National Academies of Sciences, Engineering, and Medicine, Division of Behavioral and Social Sciences and Education, Board on Behavioral, Cognitive, and Sensory Sciences, Committee on a Decadal Survey of Social and Behavioral Sciences for Applications to National Security (2019-07-26), *"A Decadal Survey of the Social and Behavioral Sciences"*, National Academies Press

39. Jean-Christophe Le Coze, *"Safety in the Digital Age"*, Springer Nature

40. Matt Aiello, Philipp Amann, Mark Anderson, Brad Arkin, Kal Bittanda, Gary A. Bolles, Michal Boni, Robert Boyce, Mario Chiock, Gavin Colman, Alice Cooper, Tom Farley, George Finney, Ryan Gillis, Marc Goodman, Mark Gosling, Antanas Guoga, William Houston, Salim Ismail, Paul Jackson, Siân John, Ann Johnson, John Kindervag, Heather King, Mischel Kwon, Selena Loh LaCroix, Gerd Leonhard, Pablo Emilio Tamez López, Gary McAlum, Diane McCracken, Mark McLaughlin, Danny McPherson, Stephen Moore, Robert Parisi, Sherri Ramsay, Max Randria, Mark Rasch, Yorck O. A. Reuber, Andreas Rohr, John Scimone, James Shira, Justin Somaini, Lisa J. Sotto, Jennifer Steffens, Megan Stifel, Ed Stroz, Ria Thomas, James C. Trainor, Rama Vedashree, Patric J. M. Versteeg, Nir Zuk, Naveen Zutshi (2018-10-05), *"Navigating the Digital Age"*

41. S.H. Solms, Rossouw Solms (2008-12-16), *"Information Security Governance"*, Springer Science & Business Media

42. Theo Tryfonas, Ioannis Askoxylakis (2014-06-07), "*Human Aspects of Information Security, Privacy, and Trust*", Springer
43. Xinru Page, Bart P. Knijnenburg, Pamela Wisniewski, Heather Richter Lipford, Nicholas Proferes, Jennifer Romano (2022), "*Modern Socio-Technical Perspectives on Privacy*", Springer Nature
44. Dark, Melissa Jane (2010-08-31), "*Information Assurance and Security Ethics in Complex Systems: Interdisciplinary Perspectives*", IGI Global
45. Reza Montasari, Hamid Jahankhani, Haider Al-Khateeb (2021-11-26), "*Challenges in the IoT and Smart Environments*", Springer Nature
46. Zhigeng Pan, Adrian David Cheok, Wolfgang Müller, Mingmin Zhang, Abdenmour El Rhalibi, Kashif Kifayat (2019-04-26), "*Transactions on Edutainment XV*", Springer
47. Elisa Bertino (2012-06-01), "*Data Protection from Insider Threats*", Morgan & Claypool Publishers
48. Wayne Jansen (2010-02), "*Directions in Security Metrics Research*", DIANE Publishing
49. Vajjhala, Narasimha Rao, Strang, Kenneth David (2022-06-24), "*Global Risk and Contingency Management Research in Times of Crisis*", IGI Global

|                                                                          |                                             |
|--------------------------------------------------------------------------|---------------------------------------------|
| Ім'я користувача:<br>Комп'ютерної математики та інформаційної безпеки... | ID перевірки:<br>1016369481                 |
| Дата перевірки:<br>17.06.2024 20:44:02 EEST                              | Тип перевірки:<br>Doc vs Internet + Library |
| Дата звіту:<br>17.06.2024 20:50:35 EEST                                  | ID користувача:<br>100005746                |

Назва документа: Диплом\_КОЗІЧЕВА І. І

Кількість сторінок: 76 Кількість слів: 18311 Кількість символів: 149895 Розмір файлу: 412.11 KB ID файлу: 1016176351

## 1.65% Схожість

Найбільша схожість: 0.2% з джерелом з Бібліотеки (ID файлу: 1015079810)

|                            |     |             |
|----------------------------|-----|-------------|
| 0.53% Джерела з Інтернету  | 56  | Сторінка 78 |
| 1.45% Джерела з Бібліотеки | 101 | Сторінка 78 |

## 0% Цитат

Вилучення цитат вимкнене

Вилучення списку бібліографічних посилань вимкнене

## 0% Вилучень

Немає вилучених джерел

## Модифікації

Виявлено модифікації тексту. Детальна інформація доступна в онлайн-звіті.

|                  |    |
|------------------|----|
| Замінені символи | 13 |
|------------------|----|