МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ПОЛІСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет інформаційних технологій,
обліку та фінансів
Кафедра комп'ютерних технологій
і моделювання систем

Кваліфікаційна робота
на правах рукопису

Троцький Владислав Валерійович

УДК 004.056:65.011.56

КВАЛІФІКАЦІЙНА РОБОТА

Соціальна інженерія методи атак і способи захисту, аналіз впливу на організації

125-«Кібербезпека та захист інформації»

Подається на здобуття освітнього ступеня магістр

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

_____
(підпис, ініціали та прізвище здобувача вищої освіти)

Керівник роботи
Євсеєв Сергій Петрович
доктор технічних наук, професор

Житомир – 2024

Висновок кафедри _____
за результатами попереднього захисту: _____

Протокол засідання кафедри _____
№ _____ від «_____» _____ 20____ р.

Завідувач кафедри _____

_____ _____ _____
(науковий ступінь, вчене звання) (підпис) (прізвище, ім'я, по батькові)
«_____» _____ 20____ р.

Результати захисту кваліфікаційної роботи

Здобувач вищої освіти _____ захистив (ла)
(прізвище ,ім'я, по батькові)
кваліфікаційну роботу з оцінкою:

сума балів за 100-бальною шкалою _____
за шкалою ECTS _____
за національною шкалою _____

Секретар ЕК

_____ _____ _____
(науковий ступінь, вчене звання) (підпис) (прізвище, ім'я, по батькові)

АНОТАЦІЯ

Троцький В.В. Соціальна інженерія методи атак і способи захисту, аналіз впливу на організації – Кваліфікаційна робота на правах рукопису.

Кваліфікаційна робота на здобуття освітнього ступеня магістр за спеціальністю 125 - «Кібербезпека та захист інформації». – Поліський національний університет, Житомир, 2024.

У межах кваліфікаційної роботи було досліджено основні методи соціальної інженерії, та їх впливу на організації, зокрема на їх інформаційну безпеку. Статистичний аналіз показав кількість випадків атак методами соціальної інженерії на організації та впливу у розрізі сфер економічної діяльності. Запропонована структурна схема системи відтворення реалістичних сценаріїв для навчання персоналу може значно підвищити протидію атакам соціальної інженерії та створити свідомий та підготовлений колектив. Тема є актуальною у зв’язку з підвищеними вимогами до інформаційної безпеки та зростаючою кількістю кібератак, які використовують психологічний вплив на співробітників організацій.

Ключові слова: фішинг, психологічний вплив, соціальна інженерія, маніпуляція довірою**,** методи захисту,загрози, людський фактор.

Робота містить 43 сторінок, 10 рисунків, 18 літературних джерел.

SUMMARY

Trotskiy V.V. Social engineering attack methods and protection strategies: analysis of impact on organizations – Qualification Thesis (Manuscript).

Qualification thesis for the degree of Master in specialty 125-"Cybersecurity and Information Protection". – Polissya National University, Zhytomyr, 2024.

As part of the qualification work, the main methods of social engineering and their impact on organizations, in particular on their information security, were investigated. Statistical analysis showed the number of cases of attacks using social engineering methods on organizations and the impact in terms of areas of economic activity. The proposed structural scheme of the system for reproducing realistic

scenarios for personnel training can significantly increase the counteraction to social engineering attacks and create a conscious and trained team. The topic is relevant in connection with the increased requirements for information security and the growing number of cyberattacks that use psychological influence on employees of organizations.

Keywords: phishing, psychological influence, social engineering, trust manipulation, protection methods, threats, human factor.

ЗМІСТ

СКОРОЧЕННЯ ТА УМОВНІ ПОЗНАЧЕННЯ

БД	база даних
СЗ	система захисту
SIEM	Security Information and Event Management
APT	Атаки типу розширеної тривалої дії

ВСТУП

У сучасному світі питання захисту інформаційної безпеки організацій набуває все більшої важливості. Методи соціальної інженерії, які використовують психологічний вплив для отримання конфіденційних даних або доступу до інформаційних систем, є одними з найпоширеніших та найбільш небезпечних видів атак. Їхня ефективність базується на вразливості людського фактору, що робить ці методи складними для виявлення та нейтралізації.

Особливо актуальною ця тема стає в умовах постійного зростання кількості кібератак, що спрямовані на маніпуляцію співробітниками, а також у зв’язку зі збільшенням вимог до інформаційної безпеки з боку державних регуляторів і бізнесу.

Ризики, пов'язані з соціальною інженерією, не лише загрожують інформаційним ресурсам, але й ставлять під удар репутацію організацій. Тому аналіз цих загроз та розробка ефективних стратегій захисту є критично важливими для сучасних компаній.

Вибір теми «Соціальна інженерія методи атак і способи захисту, аналіз впливу на організації» є надзвичайно актуальною в умовах сучасних глобальних загроз. Соціальна інженерія використовує психологічний вплив на людей для отримання доступу до конфіденційної інформації або систем, і є одним із найбільш небезпечних інструментів кібератак. Такі атаки можуть здійснюватися шляхом маніпуляцій зі співробітниками, підробки ідентичності, Phishing, Vishing та інших методів, що спрямовані на порушення безпеки організації через людський фактор.

Ця тема стає ще більш актуальною на тлі військового конфлікту Росії проти України. В умовах війни інформаційні технології та кіберзагрози стали важливими інструментами ведення війни. Зокрема, агресор активно використовує методи соціальної інженерії для проникнення в корпоративні та державні системи, отримання конфіденційної інформації або паралізації важливих інфраструктурних об'єктів. Атаки на організації з використанням

соціальної інженерії можуть мати критичні наслідки, оскільки вони дають змогу обійти навіть найсучасніші технічні засоби захисту.

Зростання кіберзагроз та ускладнення методів атак вимагають від організацій нових підходів до захисту від таких загроз. Враховуючи, що людський фактор є найбільш вразливим елементом у системах безпеки, особливо в умовах війни та підвищеної напруги, розробка і впровадження ефективних методів захисту від соціальної інженерії набуває критичного значення.

Вибір цієї теми дозволяє звернути увагу на необхідність навчання та підвищення обізнаності працівників організацій про техніки соціальної інженерії, а також розробку заходів для мінімізації ризиків, пов'язаних із кібератаками, що стають все більш частими в умовах сучасної геополітичної ситуації.

Мета: розробка способів захисту та аналізу впливу на організації, на основі структурної схеми відтворення реалістичних сценаріїв для навчання персоналу, а також розробка ефективних рекомендацій протидії.

Об’єкт: процеси здійснення атак методами соціальної інженерії.

Предмет: є технології, прийоми та інструменти, що використовуються у методах атак соціальної інженерії.

Задачі поставлені в кваліфікаційній роботі:

1.Дослідити основні методи соціальної інженерії, та їх впливу на організації, зокрема на їх інформаційну безпеку.

2.Здійснити статистичний аналіз кількості випадків атак методами соціальної інженерії на організації та впливу у розрізі сфер економічної діяльності.

3.Проектування системи навчання персоналу для протидії атакам соціальної інженерії.

РОЗДІЛ 1. СОЦІАЛЬНА ІНЖЕНЕРІЯ ЯК ЗАГРОЗА ДЛЯ СУЧАСНИХ ОРГАНІЗАЦІЙ

1.1 Аналіз та характеристики соціальної інженерії та її значення у кіберзагрозах

У сучасному світі, де комунікація, є епіцентрами ділової активності, забезпечення комплексної безпеки набуває критичного значення. Соціальна інженерія займає особливе місце, поєднуючи не тільки атаки на технічні засоби, але і використовує набір методів, спрямованих на маніпулювання людьми з метою отримання доступу до інформації, ресурсів чи систем. Вона базується на психологічних прийомах, які використовуються для введення жертви в оману, змушуючи її виконувати певні дії або надавати конфіденційні дані. Основна мета соціальної інженерії — обійти технічні засоби захисту, використовуючи людський фактор як найслабшу ланку системи безпеки.

Соціальна інженерія відрізняється від традиційних технічних атак, адже її успіх залежить не від технологій, а від здатності атакуючого маніпулювати довірою, страхом або цікавістю жертви. Цей метод став надзвичайно популярним у кіберзлочинців через його високу ефективність та відносно низьку вартість реалізації.[1]

У сучасному кіберпросторі соціальна інженерія займає особливе місце, оскільки дозволяє зловмисникам обходити технічні бар'єри захисту. У той час як брандмауери, антивіруси та системи аутентифікації стають дедалі досконалішими, людський фактор залишається вразливим. Навіть найкращі технічні засоби безпеки можуть бути неефективними, якщо люди, які їх використовують, не дотримуються правил кібергігієни.

З часом кібератаки, спрямовані на маніпуляцію людьми, еволюціонували від простих форм обману до складних стратегій, заснованих на прийомах соціальної інженерії. Раніше подібні атаки здебільшого обмежувались шахрайством через телефонні дзвінки чи листування. Однак із розвитком цифрових технологій методи атак стали значно витонченішими,

використовуючи електронну пошту, соціальні мережі та інші онлайн-ресурси для розсилки фішингових повідомлень або створення підроблених вебресурсів.

Сучасні методи таких атак базуються на використанні психологічних маніпуляцій, які змушують жертву реагувати емоційно, а не раціонально. Злочинці часто апелюють до страху, співчуття або терміновості, щоб переконати людину виконати певну дію. Наприклад, вони можуть використовувати техніку "спуфінгу" – створення електронних листів або сайтів, які виглядають правдоподібно, але насправді є шахрайськими. Інший приклад – "бейтинг", де жертві пропонують вигідні умови або нагороди, що призводить до компрометації її даних чи пристроїв.

Навчання та підвищення обізнаності користувачів відіграють ключову роль у запобіганні таким атакам. Розуміння механізмів, які роблять ці атаки ефективними, дозволяє розробити більш дієві заходи захисту. Вивчення цієї теми відкриває можливості для вдосконалення стратегій захисту від нових форм кіберзагроз.

Згідно з даними аналітичних компаній, понад 85% успішних кібератак включають елементи соціальної інженерії. Цей метод використовується як самостійна стратегія або в поєднанні з іншими атаками, такими як фішинг, вішинг чи бейтинг. Соціальна інженерія також є важливим етапом складних атак, зокрема тих, що спрямовані на великі корпорації чи урядові установи. Щоб краще усвідомити масштаби проблеми, варто звернути увагу на графік фішингових атак за останні роки, який наочно демонструє еволюцію цього напрямку соціально-орієнтованх кібератак.

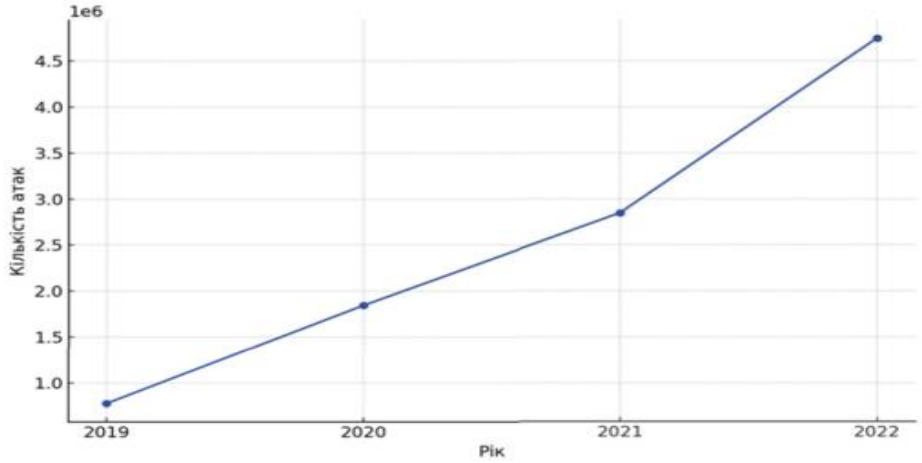


Рис. 1.1 – Кількість фішингових атак за 2019-2022 (кількість йде на трільйони) [2]

Прикладами успішних атак можуть слугувати:

- Атака на Target (2013): Кібератака на американську мережу магазинів Target є одним із найвідоміших випадків, коли соціальна інженерія стала ключовим інструментом злочинців. Зловмисники отримали доступ до системи компанії через підрядника, використовуючи фішингові листи. Це дозволило їм викрасти дані понад 40 мільйонів кредитних карток.
- Атака на Twitter (2020): У липні 2020 року було зламано акаунти багатьох відомих людей, зокрема Ілона Маска, Джеффа Безоса та Барака Обами. Зловмисники використовували соціальну інженерію, щоб обдурити співробітників компанії і отримати доступ до внутрішніх систем. У результаті вони розмістили шахрайські повідомлення, які дозволили їм зібрати значну кількість криптовалюти.
- Атака на RSA (2011): Кібератака на компанію RSA, що спеціалізується на розробці систем захисту, була здійснена через spear-phishing. Зловмисники відправили співробітникам компанії електронні листи із зараженим файлом Excel. Відкриття файлу дозволило їм отримати доступ до критично важливих даних.

Ці приклади демонструють, як соціальна інженерія дозволяє зловмисникам обходити навіть найскладніші системи захисту, використовуючи слабкості в

поведінці людей. Зрозуміти принципи роботи соціальної інженерії — перший крок до захисту від цієї загрози.

Дослідження показало, що слабкі місця систем часто виникають через низький рівень усвідомлення ризиків, технічні вади інфраструктури та людські помилки, такі як відсутність належної уваги до питань інформаційної безпеки. Враховуючи це, зменшення ризиків вимагає впровадження інтегрованого підходу, який включає не лише технічні засоби захисту, але й освітні програми, спрямовані на підвищення рівня обізнаності працівників.

Для ефективного протистояння кібератакам, орієнтованим на людський фактор, важливо не тільки вдосконалювати технічні рішення, але й приділяти значну увагу навчанню персоналу. Постійна робота над підвищенням кібергігієни та обізнаності дозволить створити стійкий бар'єр для захисту від цих багатогранних і складних загроз.

1.2 Основні методи, які використовують для атак соціальної інженерії

У цьому розділі зусередемо увагу на детальному аналізі методів спрямованих на маніпуляцію людьми для отримання доступу до конфіденційної інформації або ресурсів організації. Одним із найпоширеніших методів є фішинг Ця атака полягає в обмані жертви через електронні листи, які імітують офіційні повідомлення. Зловмисники створюють підроблені сайти, що виглядають як реальні (банки, поштові сервіси), або надсилають заражені файли. Сучасні варіації фішингу включають spear phishing, спрямований на конкретних осіб, і whale phishing, орієнтований на високопосадовців. [3] Ці техніки дозволяють зловмисникам отримати паролі, фінансову інформацію чи доступ до систем, див. рисунок 1.1.

Іншим поширеним методом є вішинг, який використовує телефонні дзвінки для введення жертви в оману. Зловмисники представляються працівниками банку або технічної підтримки, просять надати особисті дані або встановити шкідливе програмне забезпечення. Підроблені номери телефонів і

переконливий тон голосу часто викликають довіру, а додавання терміновості ("ваш рахунок заблоковано") знижує настороженість жертви.

Бейтинг використовує людську цікавість. Зловмисники залишають заражені носії інформації (наприклад, флешки) у доступних місцях. Жертва, знайшовши пристрій із поміткою "Конфіденційно" чи "Важливі дані", підключає його до свого комп'ютера, активуючи шкідливий код, який дозволяє атакуючим отримати доступ до системи.

Метод tailgating полягає у фізичному проникненні на територію організації. Зловмисники використовують довірливість співробітників, проходячи разом із ними через контрольні точки доступу, іноді з виглядом "забув перепустку". Потрапивши всередину, вони можуть отримати доступ до техніки чи документів.

Pretexting (маніпуляція довірою) передбачає створення правдоподібного сценарію для обману жертви. Зловмисник може видавати себе за представника служби безпеки чи технічної підтримки і просити надати доступ до облікового запису під приводом "перевірки". Ключовими елементами є переконливий сценарій, авторитетність та використання терміновості.

Атаки типу розширеної тривалої дії (APT) належать до одних із найскладніших і найбільш цілеспрямованих кіберзагроз, спрямованих на конкретні організації або інфраструктурні об’єкти. Вони суттєво відрізняються від звичайних кібератак своєю довготривалістю, складністю та ретельним плануванням, яке дозволяє зловмисникам тривалий час залишатися непоміченими для досягнення своїх цілей, таких як викрадення конфіденційних даних або підрив стабільності організаційних систем. Основною особливістю APT є їхня чітка спрямованість. Атакуючі ретельно планують кожен етап дій, використовуючи широкий спектр методів, таких як соціальна інженерія, експлуатація вразливостей у програмному забезпеченні, впровадження шкідливого коду та використання складних технік для приховування своєї діяльності. Після успішного проникнення в систему зловмисники прагнуть

залишатися непоміченими якомога довше, що дозволяє їм здійснювати збирання інформації, моніторинг мережевого трафіку або підготовку до подальших дій. У процесі вони використовують спеціалізовані інструменти для управління скомпрометованими системами та збору цінних даних.

Дослідження APT потребує детального аналізу використовуваних технік, які дають змогу зловмисникам уникати виявлення, обходити заходи безпеки та зберігати доступ до систем. Це включає вивчення механізмів приховування присутності в мережі, збору даних і виконання шкідливих операцій. Ефективний захист від APT вимагає комплексного підходу до кібербезпеки. Необхідно використовувати сучасні технології моніторингу та виявлення загроз, проводити регулярні аудити інформаційної безпеки та впроваджувати навчальні програми для підвищення рівня обізнаності співробітників. Важливим компонентом захисту є не тільки впровадження технічних інструментів, але й створення культури безпеки, що дозволяє адаптуватися до нових викликів у сфері кіберзагроз. Кібершпигунство та кібервійни є невід'ємною частиною сучасного цифрового ландшафту загроз. Вони реалізуються як державними, так і приватними структурами та мають потенційно глобальні наслідки. [4]

Кібершпигунство зазвичай включає нелегальне проникнення в мережі урядових установ, корпорацій або науково-дослідницьких центрів для збору конфіденційної інформації. Методи включають фішинг, впровадження шкідливого програмного забезпечення та використання вразливостей систем.
Кібервійна, на відміну від шпигунства, є більш агресивною формою впливу, що спрямована на критично важливу інфраструктуру, наприклад, енергетичні мережі, системи водопостачання чи фінансові установи. Такі дії можуть спричинити серйозні наслідки, включаючи економічну дестабілізацію, соціальні заворушення або загрозу життю населення.

.

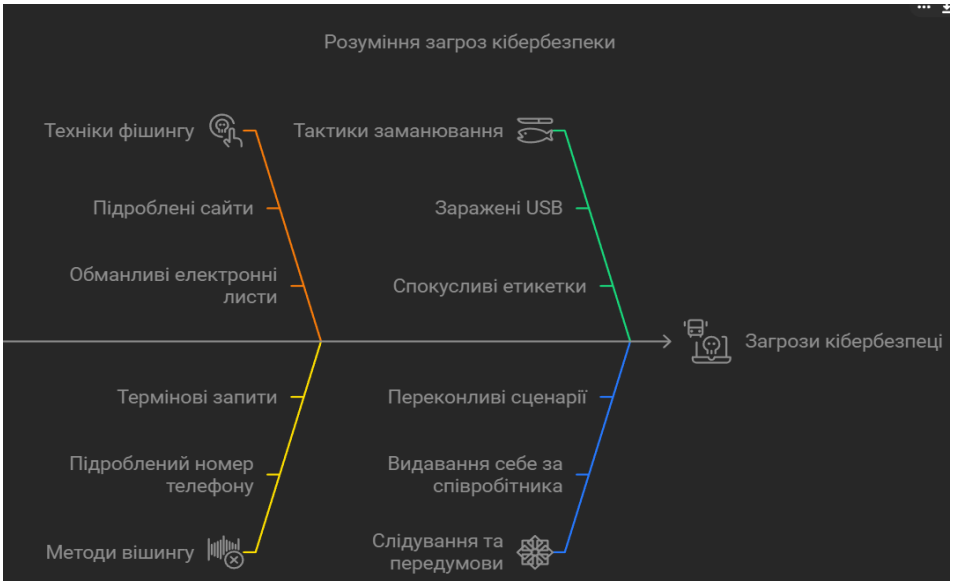


Рис 1.1 Основні методи реалізації атак соціальної інженерії

1.3 Вплив соціальної інженерії на організаційні процеси

Вплив атак соціальної інженерія є одним із найнебезпечніших. Має значний вплив на організації, порушуючи ключові аспекти їхньої діяльності. Нижче розглянемо основні наслідки таких атак.

Порушення конфіденційності, цілісності та доступності даних. Атаки соціальної інженерії часто спрямовані на отримання конфіденційної інформації, такої як фінансові дані, дані клієнтів чи внутрішні корпоративні документи. Використовуючи обман, зловмисники можуть отримати доступ до паролів, облікових записів чи навіть баз даних. Це ставить під загрозу конфіденційність інформації, роблячи її доступною для третіх осіб. Крім того, атаки можуть порушувати цілісність даних, змінюючи їх чи додаючи шкідливі елементи. Наприклад, у разі успішного проникнення до баз даних зловмисник може видалити чи модифікувати важливу інформацію, що негативно вплине на рішення, які приймає організація. Порушення доступності даних часто проявляється у вигляді блокування доступу до систем або інформації через шкідливе програмне забезпечення, наприклад, програми-здирники (ransomware). Це може призводити до простоїв у роботі, втрати даних або вимагання викупу.

Коли організація стає жертвою атак соціальної інженерії, це може значно підірвати довіру клієнтів, партнерів та навіть співробітників. Наприклад, витік персональних даних клієнтів через атаку фішингу не лише порушує юридичні норми, а й завдає репутаційної шкоди. Втрата довіри часто веде до скорочення клієнтської бази, зниження інвестиційної привабливості та складнощів у залученні нових партнерів. Для багатьох компаній імідж є важливішим активом, ніж фінансові ресурси. Один інцидент може зруйнувати репутацію, яку будували роками. Крім того, негативна публічність через медіа чи соціальні мережі може створити додаткові бар'єри для відновлення довіри.

Наприклад, успішна атака на фінансовий відділ, яка змушує співробітників перевести кошти на підроблені рахунки, може спричинити фінансові втрати, які важко відшкодувати. Додатково, атаки типу tailgating, що забезпечують фізичний доступ до критично важливих систем, можуть призвести до втрати обладнання або знищення даних. Внаслідок цього процеси організації можуть бути паралізовані на тривалий час. Також порушення доступності систем через соціальну інженерію, наприклад, через викрадення облікових даних чи блокування систем, ускладнює виконання операцій. Це впливає на продуктивність, порушує ланцюги постачання та створює додаткові витрати на відновлення роботи. [5]

1.4 Аналіз світової статистики успішних атак

Кількість кібератак у світі зростає щороку, відповідно до звітів провідних аналітичних компаній. За даними IBM Security X-Force, у 2023 році кількість атак на організації збільшилася на 38% у порівнянні з попереднім роком. Згідно з даними Verizon, понад 80% усіх кіберінцидентів пов’язані з людським фактором, що включає помилки співробітників, необережність та дії, спричинені соціальною інженерією. Найбільш поширеними типами атак є фішинг, викрадення облікових даних та атаки програм-здирників. У середньому кожна організація стикається з 10-12 спробами таких атак щомісяця. Інфраструктура

малого та середнього бізнесу, через обмежені ресурси на кіберзахист, часто стає основною ціллю злочинців. За даними звіту Proofpoint за 2023 рік, понад 75% компаній стикалися з фішингом, який є однією з форм соціальної інженерії. Близько 35% атак були пов'язані зі spear phishing — цільовими атаками на окремих осіб або відділи. Щороку соціальна інженерія стає складнішою: використовуються персоналізовані повідомлення, що базуються на попередньо зібраних даних про жертву. Атаки типу pretexting займають близько 20% від усіх атак, де використовується обман для отримання доступу до ресурсів або даних. Частка атак, які базуються на соціальній інженерії, особливо висока у фінансовому секторі, охороні здоров'я та IT-компаніях, де зберігаються критично важливі дані. Згідно з аналітиками компанії Cisco, понад 90% успішних атак на організації містять елементи соціальної інженерії.[6]

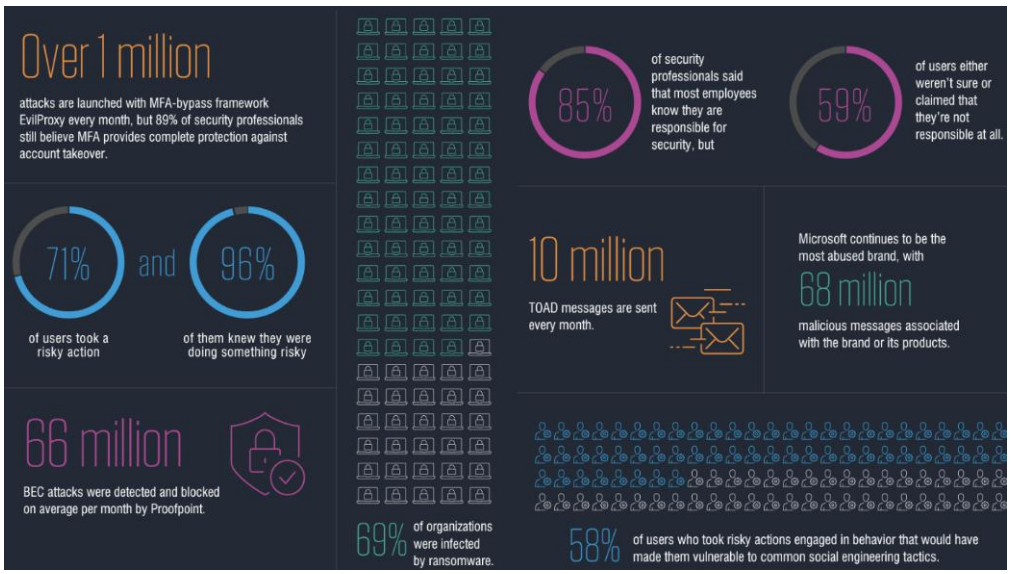


Рис 1.1 Статистика звіту State of the Phish report – кількості випадків соціальної інженерії на рік.[6]

За звітом IBM, понад 60% клієнтів схильні відмовитися від послуг компанії, яка допустила витік даних. Це веде до додаткових втрат, які складно оцінити в короткостроковій перспективі. Соціальна інженерія також має вплив на продуктивність бізнесу. Наприклад, атаки, що блокують доступ до даних або систем, спричиняють простої, що може коштувати компаніям тисячі доларів за

кожну годину. У великих корпораціях ці витрати можуть досягати десятків мільйонів доларів. Соціальна інженерія спрямований на такі галузі як виробництво, інформаційний сектор, рітейл, охорона здоров'я, житловий сектор, держсектор, фінанси, освіта та інші. Див. рис1.2 [7]

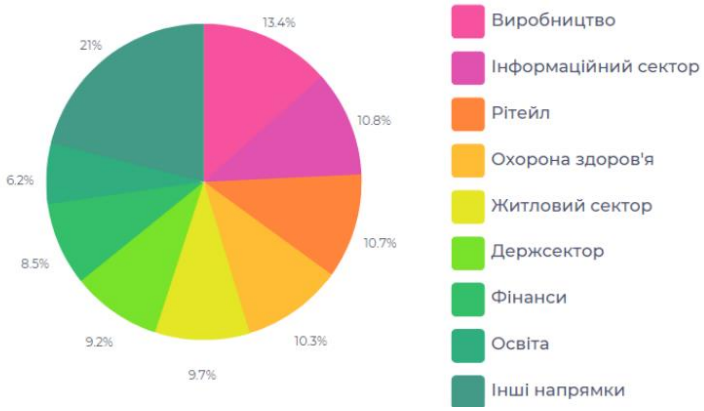


Рис 1.2 – Напрямки на які спрямована соціальна інженерія.[7]

В останні роки Україна стала об'єктом численних спрямованих кібератак, які мали значний вплив на національну безпеку та економіку. Відомі випадки включають масштабні фішингові кампанії та поширення шкідливого програмного забезпечення, що спричинило компрометацію важливих державних і приватних інформаційних систем. Такі події вказують на нагальну потребу в посиленні заходів кіберзахисту на національному рівні та підвищенні обізнаності серед корпоративного сектора щодо потенційних ризиків і методів їхньої нейтралізації.

Кібератаки на державні установи створюють суттєві ризики для функціонування критичної інфраструктури, порушуючи роботу інформаційних систем та підриваючи стабільність державного управління. Основною метою таких атак може бути доступ до конфіденційної інформації, злам комунікаційних систем або навіть спроби дестабілізувати ключові процеси управління. Це становить серйозну загрозу як для внутрішньої безпеки, так і для міжнародних відносин країни. [8]

Подібні загрози часто впливають на функціонування урядових служб, включаючи соціальні, фінансові та логістичні системи. Збої в їхній роботі можуть викликати затримки в наданні послуг населенню та зниження довіри до органів влади. Україна вже зіткнулася з такими проблемами, зокрема під час атак типу NotPetya, які спричинили значні фінансові втрати, порушили роботу державних систем і вплинули на стабільність ключових державних послуг.
Ці інциденти чітко демонструють необхідність розробки комплексної стратегії кіберзахисту. Така стратегія має включати сучасні технології моніторингу та виявлення загроз, проведення регулярних перевірок безпеки, а також постійне підвищення рівня обізнаності співробітників про ризики та методи захисту. Лише системний підхід до кібербезпеки дозволить мінімізувати наслідки подібних атак і підвищити стійкість України перед новими викликами.

Висновки до першого розділу

У першому розділі було проведено детальний аналіз соціальної інженерії як однієї з ключових загроз сучасним організаціям. Розглянуто поняття соціальної інженерії, яке базується на маніпуляціях довірою та психологічному впливі для отримання доступу до конфіденційної інформації або ресурсів. Було встановлено, що соціальна інженерія є не лише окремим видом кіберзагрози, але й складовою більшості сучасних атак.

Особливу увагу приділено аналізу впливу соціальної інженерії , що ці атаки порушують конфіденційність, цілісність та доступність даних, викликають втрати довіри до організацій та дестабілізують їхні бізнес-процеси. Внаслідок таких атак організації зазнають значних фінансових втрат і репутаційної шкоди, що ускладнює їхню діяльність у довгостроковій перспективі.[9]

Розгляд світової статистики підтвердив домінуюче місце соціальної інженерії серед кіберзагроз. Частка атак, що базуються на соціальній інженерії, перевищує 75% від загальної кількості інцидентів, а економічний вплив на бізнес вимірюється мільйонами доларів у прямих і непрямих витратах.

РОЗДІЛ 2. ПРОЕКТУВАННЯ СХЕМИ ВІДТВОРЕННЯ РЕАЛІСТИЧНИХ СЦЕНАРІЇВ АТАК ДЛЯ НАВЧАННЯ ПЕРСОНАЛУ ПРОТИДІЇ АТАКАМ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ

2.1 Процес реалізації атак за людським фактором

Атаки, орієнтовані на людський фактор, зосереджуються на маніпуляції людською психологією замість експлуатації технічних вразливостей. Такі атаки націлені на отримання доступу до конфіденційної інформації чи систем. Основні типи цих атак включають:

1. Фішинг (Phishing): Один із найпоширеніших методів шахрайства, що полягає у спробі обманом отримати конфіденційну інформацію, таку як паролі, логіни, номери банківських карт тощо. Атакувальники часто використовують електронні листи, які імітують комунікацію від офіційних установ, спрямовуючи жертв на фальшиві вебсайти.
2. Цільовий фішинг (Spear Phishing): Цей варіант фішингу націлений на конкретних осіб чи організації. Атакувальники ретельно готуються, збираючи інформацію про своїх жертв, щоб створити переконливі та персоналізовані повідомлення.
3. Вейлінг (Whaling): Різновид цільового фішингу, орієнтований на керівників вищої ланки або впливових осіб. Такі атаки часто спрямовані на отримання важливої корпоративної інформації чи фінансових вигод.
4. Вішинг (Vishing): Атаки, що здійснюються через голосовий зв’язок, наприклад, телефонні дзвінки. Шахраї використовують переконливі сценарії, щоб змусити жертву розкрити особисту чи фінансову інформацію.
5. Приманка (Baiting): Цей метод передбачає використання фізичних або цифрових "приманок", щоб залучити жертву. Наприклад, зловмисники можуть залишити заражені USB-накопичувачі у місцях, де їх легко знайдуть, сподіваючись, що жертва підключить їх до свого комп’ютера.

6. Квітинг (Quid Pro Quo): Атака, де жертві пропонують якусь вигоду в обмін на конфіденційну інформацію або доступ до системи. Наприклад, шахрай може зателефонувати під виглядом технічної підтримки, пропонуючи вирішити проблему, і попросити надати логін та пароль.

7. Спуфінг (Spoofing): Метод, коли атакувальники імітують іншу особу, компанію чи пристрій, щоб обдурити жертву та отримати доступ до конфіденційної інформації. Це може бути підробка електронної пошти (email spoofing) або IP-адреси (IP spoofing), що виглядає як легітимне джерело.

Для успішного здійснення будь-якої з цих атак необхідна ретельна підготовка. Знаючи основні принципи їх реалізації, процес можна умовно розділити на декілька ключових етапів:

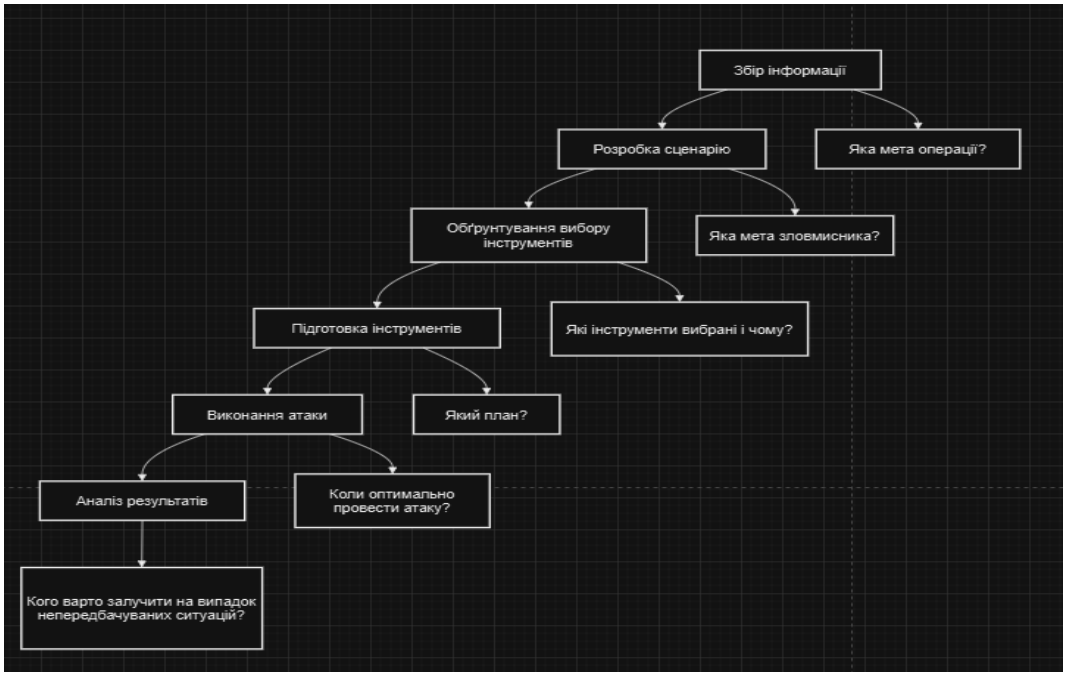


Рисунок. 2.1 – Діаграма процесу реалізації атаки за людськм фактором.

Збір даних із відкритих джерел є базовою складовою діяльності соціального інженера. Саме цей етап визначає основу всієї підготовки атаки, оскільки він займає ключову позицію в ієрархії процесу. Часто недооціненою залишається важливість розвідки з відкритих джерел, яка відіграє роль фундаментального етапу планування. Маючи доступ до вихідної інформації про ціль (особу чи організацію), фахівці використовують машинні методи (аналіз даних з інтернету,

соціальних мереж тощо) та фізичні спостереження (огляд місцевості або поведінки людей). Для цього часто застосовують техніки OSINT, що дозволяють зібрати необхідні відомості про об'єкт.

Успіх у соціальній інженерії залежить від ретельної підготовки, стратегічного планування та здатності швидко адаптуватися до нових умов і викликів, що виникають у процесі реалізації операції.

2.2 Планування реагування на інциденти

Ефективне управління ризиками вимагає постійного моніторингу та адаптації до змін навколишнього середовища. Це дозволяє забезпечити актуальність і дієвість захисних стратегій, які здатні реагувати на нові типи загроз і викликів у сфері кібербезпеки.

Планування дій у разі кіберінцидентів є ключовим елементом комплексної стратегії протидії кіберзагрозам. Цей процес охоплює розробку детальних інструкцій, які визначають порядок реагування організації на різні види порушень безпеки. Ефективні дії у відповідь дозволяють мінімізувати збитки від атак і прискорити процес відновлення роботи.Окрім технічних рішень, важливим є врахування організаційних аспектів, таких як розробка та впровадження ефективних політик безпеки, процесів реагування на інциденти та навчання співробітників. Це допомагає сформувати усвідомлення та підготовленість до ризиків в організації. [14]

Інтеграція різноманітних елементів безпеки в єдину систему дозволяє не лише захистити організацію від існуючих загроз, але й гнучко адаптуватися до нових викликів у майбутньому, забезпечуючи стабільний та ефективний захист від кібер атак.

Аналіз та управління ризиками в сфері кібербезпеки є важливими складовими стратегії протидії кібер атакам. Це процес, що включає виявлення потенційних загроз, оцінку вразливостей, які можуть бути використані зловмисниками, та розробку ефективних стратегій для мінімізації цих ризиків.

На першому етапі, ідентифікація ризиків, проводиться аналіз потенційних загроз, що можуть вплинути на інформаційні системи. Це можуть бути зовнішні загрози, такі як хакерські атаки, фішинг, шпигунські програми, а також внутрішні загрози, такі як помилки співробітників або неефективне управління даними.

Після ідентифікації загроз проводиться оцінка ризиків, яка включає аналіз потенційного впливу та ймовірності реалізації кожної загрози. Це допомагає визначити, які ризики є найбільш критичними та потребують негайної уваги.

На основі цієї оцінки розробляються стратегії управління ризиками, які включають різні заходи для їх зменшення або усунення. Це може включати технічні рішення, такі як впровадження сучасних технологій захисту, а також організаційні заходи, такі як розробка політик безпеки, навчання персоналу та створення планів реагування на інциденти.

Ефективне управління ризиками вимагає постійного моніторингу та адаптації до змінюваних умов. Це забезпечує актуальність і ефективність стратегій захисту в умовах нових загроз та викликів у сфері кібербезпеки.

Планування реагування на інциденти кібербезпеки є важливою складовою комплексної стратегії протидії кібер атакам. Цей процес включає розробку детальних планів, які визначають, як організація повинна реагувати на різні типи загроз безпеки. Ефективне реагування на інциденти може значно зменшити збитки від атак та пришвидшити процес відновлення, див. рисунок 2.1.

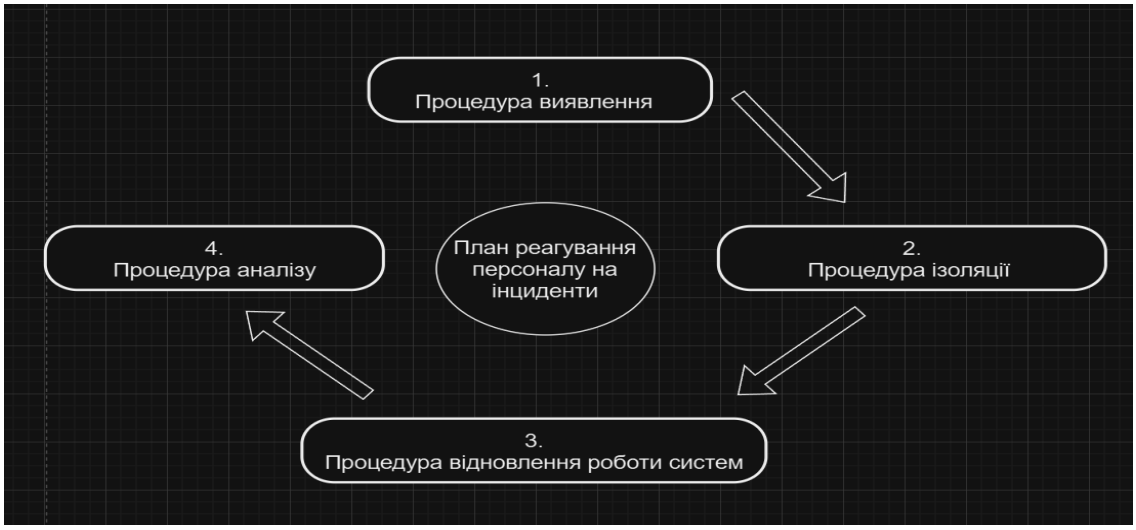


Рисунок.2.1- План реагування на інциденти

План реагування на кіберінциденти зазвичай складається з таких основних етапів:

1. Механізми виявленняці заходи передбачають використання інструментів для оперативного та точного ідентифікування загроз або порушень безпеки. Завдяки сучасним системам моніторингу можна швидко визначати підозрілі дії чи аномалії в роботі інфраструктури.
2. Ізоляція загрози при виявленні кібератаки необхідно негайно обмежити вплив загрози, ізолювавши постраждалі ділянки системи чи мережі. Це може включати відключення від мережевого доступу, блокування небажаного трафіку чи сегментацію вразливих частин.
3. Процедури відновлення: Після атаки здійснюються дії з відновлення даних за допомогою резервних копій, відновлення функцій системи та внесення змін, спрямованих на зниження ризику повторних інцидентів.
4. Оцінка та аналіз інциденту: Завершальним етапом є детальний аналіз причин інциденту, вивчення використаних атакувальниками вразливостей та формування рекомендацій для вдосконалення системи безпеки з метою уникнення подібних ситуацій у майбутньому.

2.3 Структурна схема системи відтворення реалістичних сценаріїв атак для навчання співробітників протидії атакам соціальної інженерії

Навчальні тренінги з кібербезпеки є важливим інструментом підвищення обізнаності співробітників про сучасні загрози, такі як атаки соціальної інженерії. Програми кібербезпеки включають інтерактивні курси, семінари та вебінари, спрямовані на формування базових навичок розпізнавання загроз, управління паролями та дотримання політик безпеки. Практичні вправи, наприклад, аналіз підозрілих електронних листів або телефонних дзвінків, дозволяють співробітникам застосовувати отримані знання на практиці. Ефективним підходом до навчання є відтворення реалістичних сценаріїв атак. Імітації фішингових кампаній, спроб фізичного проникнення чи сценарії соціальної інженерії дозволяють співробітникам навчатися у безпечному середовищі, не створюючи ризиків для організації. Система симуляції, яка допомагає працівникам ідентифікувати загрози та розуміти наслідки неправильних дій, одночасно дозволяючи організаціям оцінити їхній рівень підготовки зображена на рисунку 2.2.

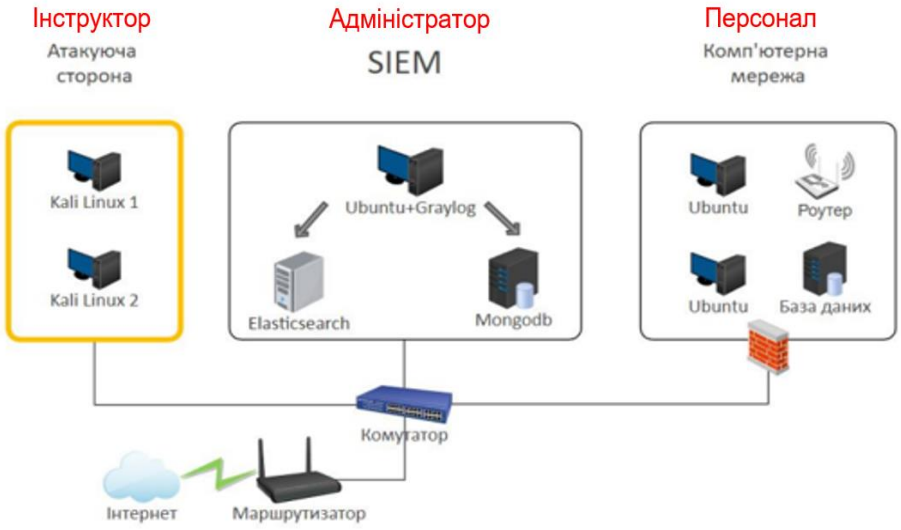


Рисунок 2.2 Структурна схема системи відтворення реалістичних сценаріїв для навчання персоналу протидії атакам методами соціальної інженерії.

Опис компонентів:

Атакуюча сторона (Інструктор):

Kali Linux 1 та Kali Linux 2: Це операційні системи, спеціально розроблені для проведення тестів на проникнення та кіберзагроз. Вони використовуються атакуючою стороною для проведення атак на персонал.

SIEM (Security Information and Event Management)(Адміністратор):

Ubuntu + Graylog: Сервер, який обробляє та аналізує журнали подій. Graylog — це платформа для збору, індексації та аналізу даних.

Elasticsearch: Система для пошуку та аналітики, яка використовується для зберігання даних із Graylog.

MongoDB: База даних для зберігання структурованої інформації, яка підтримує роботу Graylog , див.додаток А.

Комп'ютерна мережа (персонал який навчається):

Ubuntu (2 ПК): Комп'ютери в локальній мережі організації, які є потенційними цілями для атак.

Роутер: Забезпечує зв’язок між локальною мережею та Інтернетом.

База даних: Сервер, на якому зберігається конфіденційна інформація, що також може бути об'єктом атак.

Мережевий екран (Firewall): Використовується для захисту мережі від зовнішніх загроз.

*М*ережеве обладнання:

Комутатор (Switch): Здійснює зв'язок між SIEM, комп'ютерами в локальній мережі та іншими пристроями.

Маршрутизатор (Router): Забезпечує підключення до Інтернету.

Опис взаємодії:

Атакуюча сторона (Kali Linux) здійснює спроби атак на персонал в локальній мережі та базу даних.

Graylog у системі SIEM збирає та аналізує дані про всі події, пов’язані з мережею, включаючи підозрілі дії, що можуть свідчити про атаку.

Elasticsearch та MongoDB підтримують роботу SIEM, забезпечуючи зберігання та швидкий доступ до великих обсягів даних.

Комп'ютерна мережа підключена через комутатор та захищена брандмауером, щоб мінімізувати ризики атак**.**

Для забезпечення ефективності тренінгів важливо проводити регулярну оцінку готовності співробітників. Це включає тестування знань, аналіз результатів симуляцій атак і збір зворотного зв'язку. Наприклад, відстеження, яка частка працівників успішно виявляє підозрілі листи або дії, дозволяє виявляти слабкі місця в системі навчання. Регулярна оцінка результатів допомагає адаптувати програми тренінгів до потреб організації, забезпечуючи постійне підвищення рівня обізнаності та готовності співробітників до реальних загроз.

На представленій діаграмі відображено структуру системи тренувань, спрямованих на підвищення ефективності протидії атакам соціальної інженерії в організаціях.

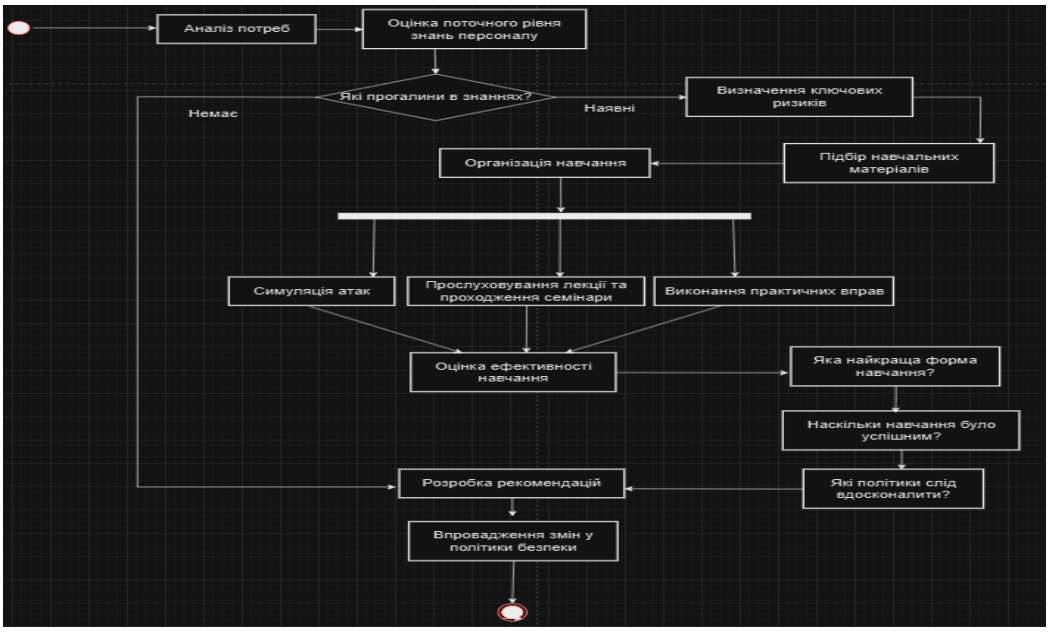


Рисунок 2.3 – UML діаграма процесів

Основними учасниками системи є співробітник, інструктор і адміністратор. Співробітники, як ключові учасники, проходять тренувальні сценарії, що включають імітацію реальних кібератак, виконання завдань, аналіз

результатів і отримання зворотного зв’язку. Інструктор забезпечує налаштування сценаріїв, моніторинг виконання завдань і оцінку ефективності тренувань. Адміністратор відповідає за технічну підтримку процесу, запис активності користувачів і формування звітів. Така система дозволяє організації ефективно виявляти та усувати слабкі місця в інформаційній безпеці, підвищуючи обізнаність співробітників і зменшуючи ризики успішного застосування методів соціальної інженерії, таких як фішинг, вішинг, смішинг тощо.

Структура послідовностей для відтворення реалістичних сценаріїв атак на навчання персоналу виглядає наступним чином:

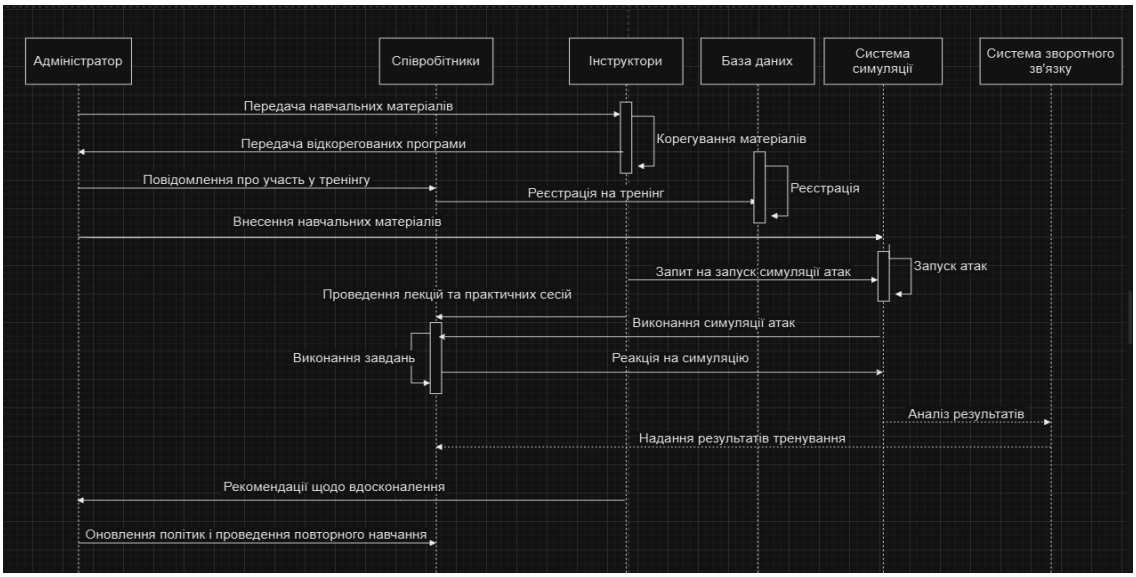


Рисунок 2.4 – Діаграма послідовностей навчальної системи

1. Адміністратор ключова особа, яка управляє всіма процесами симуляцій і тренувань. Адміністратор відповідає за налаштування системи симуляцій, управління доступом до даних, моніторинг прогресу учасників і забезпечення безпеки всієї навчальної інфраструктури. Він має доступ до статистики, результатів тестувань і може вносити корективи в сценарії або систему.
(див.дод А.2)
2. Співробітники є основними учасниками тренувань. Вони проходять різні симуляції кібератак, такі як фішинг, соціальна інженерія або злом систем. Співробітники повинні застосовувати отримані знання з кібербезпеки, щоб

виявити та відреагувати на загрози, зберігаючи при цьому свої персональні дані і конфіденційну інформацію. (див.дод А.2)

3. Інструктор відповідає за навчання і підтримку співробітників під час тренінгів. Вони організовують та проводять заняття, здійснюють оцінку ефективності навчання, надають зворотний зв'язок і допомагають учасникам покращити свої навички. Інструктор може надавати пояснення щодо методів протидії конкретним видам атак або проводити повторні тренування для посилення знань. (див.дод А.2)

4. База даних зберігає всю інформацію про симуляції, користувачів, їх прогрес і результати. Вона може містити статистику за результатами виконаних тестів, а також звіти, що використовуються для аналізу рівня готовності співробітників до реальних атак. Важливими аспектами є збереження історії дій, а також метааналіз помилок та успіхів учасників. (див.дод А.2)

5. Система, яка моделює реалістичні сценарії атак, дозволяючи співробітникам відпрацьовувати реагування на різноманітні кіберзагрози. Це може включати симуляції фішинг-атак, навмисних зломів систем або спроб зловмисників маніпулювати співробітниками для отримання конфіденційної інформації. Система симуляції має бути інтерактивною та гнучкою, щоб забезпечити ефективне навчання в умовах, наближених до реальних. (див.дод А.2)

6. Система надає учасникам оцінку їхніх дій під час симуляцій, зібравши дані з бази та системи симуляції. Зворотний зв'язок може бути в автоматичному режимі або через інструктора, який оцінює виконання завдання, надає рекомендації та вказує на слабкі місця, що потребують додаткового вдосконалення. Важливо, щоб цей процес був конструктивним і допомагав співробітникам усвідомити свої помилки та вдосконалити реакцію на майбутні загрози. (див.дод А.2)

Ця структура дозволяє забезпечити ефективне навчання та підготовку персоналу до реальних кіберзагроз, надаючи можливість тренуватися в умовах, що максимально наближені до реальності.

Висновки до другого розділу

У другому розділі розглянуто важливість атак, орієнтованих на людський фактор, як одного з основних аспектів кіберзагроз. Ці атаки, такі як фішинг, вейлінг, вішинг та інші методи соціальної інженерії, спрямовані на маніпулювання психологією людини для отримання доступу до конфіденційної інформації. Важливим етапом у їх реалізації є збір даних з відкритих джерел, що дозволяє створити переконливі атаки, які можуть ефективно обійти технічні системи захисту.

Крім того, розглянуто процес планування реагування на кіберінциденти, який є невід'ємною частиною стратегії безпеки організації. Розробка детальних планів реагування, що включають механізми виявлення загроз, ізоляцію інцидентів, відновлення після атак і їх аналіз, дозволяє організаціям мінімізувати збитки та швидко відновлювати свою діяльність. Цей підхід не лише забезпечує оперативне реагування на інциденти, але й дозволяє адаптувати стратегії захисту до нових загроз.

Завершенням розділу є підхід до навчання співробітників, що є критично важливим для протидії атакам соціальної інженерії. Використання реалістичних сценаріїв атак та системи симуляції дозволяє працівникам покращити свої навички виявлення загроз і формувати відповідну поведінку в умовах кіберзагроз. Регулярні тренування та оцінка результатів допомагають підвищити ефективність боротьби з соціальною інженерією та знижують ризики успішних атак на організацію.

РОЗДІЛ 3. РЕКОМЕНДАЦІЇ КОМЛЕКСНОЇ ПРОТИДІЇ МЕТОДАМ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ

3.1 Психологічний методи протидії атакам соціальної інженерії

У цьому розділі увага зосереджена на аналізі психологічних аспектів кіберзагроз і методах протидії їм. Оскільки більшість соціальних кібератак ґрунтуються на маніпуляціях та обмані, важливо зрозуміти, як застосування психологічних знань може допомогти посилити рівень кібербезпеки. Це включає аналіз того, як зловмисники використовують соціальні та психологічні впливи, а також розробку стратегій для підготовки й захисту співробітників від таких загроз.

Основними психологічними тактиками є експлуатація довіри, авторитету та створення тиску.[15]

1. Експлуатація довіри: Один із найпоширеніших методів соціальної інженерії – використання довіри. Зловмисники формують враження надійності чи знайомства, щоб знизити пильність жертви. Наприклад, вони можуть імітувати повідомлення від відомих компаній або колег, використовуючи знайомі логотипи та стилі оформлення (див.дод. Б).

2. Зловживання авторитетом: Часто зловмисники вдаються до імітації авторитету, наприклад, прикидаючись керівниками або представниками офіційних органів. Це може спонукати жертву виконувати певні дії або надавати інформацію, якої зазвичай вони б не розголосили (див.дод. Б).

3. Соціальний вплив і психологічний тиск: Зловмисники також можуть створювати відчуття терміновості або використовувати страх. Наприклад, вони можуть стверджувати, що якщо жертва негайно не виконає певні дії, це матиме негативні наслідки (див.дод. Б).

Розуміння психологічних механізмів соціальної інженерії є критично важливим у боротьбі з людино-орієнтованими кібератаками. Зловмисники часто

використовують психологічні прийоми для впливу на поведінку жертви, щоб отримати доступ до конфіденційної інформації або систем (див.дод. Б).

3.2 Практичні рекомендації для забезпечення ефективного захисту від атак соціальної інженерії.

Розвиток культури кібербезпеки в компанії

Регулярні навчання та освітні програми: Проведення регулярних навчальних сесій для співробітників, що охоплюють основи кібербезпеки, методи виявлення фішингових атак, безпечне використання електронної пошти та Інтернету. Ці тренінги повинні містити практичні завдання та симуляції атак для кращого усвідомлення потенційних ризиків.

На осноі вище згаданого було надано перелік сертифікованих курсів та лекцій в якості рекомендацій. (див. дод. В) [17][19][22]

Внутрішнє інформування та підвищення обізнаності: Постійне інформування співробітників про нові кіберзагрози, методи шахрайства та зміни в політиці безпеки компанії. Це може здійснюватися через електронні бюлетені, вебінари та інформаційні зустрічі.[16]

Впровадження технічних заходів безпеки

Використання двофакторної автентифікації (2FA): Запровадження 2FA для всіх корпоративних платформ та сервісів з метою підвищення рівня захисту облікових записів від несанкціонованого доступу. (див. дод. В)

Оновлення програмного забезпечення та впровадження патчів безпеки: Регулярне оновлення ПЗ і операційних систем до останніх версій для усунення виявлених уразливостей.

Використання програм для захисту від фішингу та шкідливих програм: Інсталяція та налаштування ефективних антивірусних і антиспамових програм на всіх пристроях.

Розробка та впровадження комплексної політики безпеки

Визначення чітких процедур і політик безпеки: Створення детальних вказівок і норм для працівників щодо користування корпоративними ресурсами, обробки інформації та реагування на інциденти безпеки.

Політика обмеженого доступу: Надання доступу до систем і даних тільки на рівні, необхідному для виконання конкретних обов'язків співробітника, з метою зниження ризиків зловживання або помилкового використання інформації.

Періодичний аудит та перевірка системи безпеки

Організація періодичних пентестів: Наймання зовнішніх експертів для проведення тестування системи на наявність вразливостей та розробка заходів для усунення знайдених недоліків.

Моделювання кібератак: Проведення регулярних навчальних атак для оцінки реакції персоналу та ефективності технічних заходів безпеки.Розробка плану реагування на інциденти. (див. дод. В)

Розробка чіткого плану реагування на інциденти безпеки: Створення детального алгоритму дій для різних кіберінцидентів, таких як фішинг, витоки даних або вірусні атаки. План має включати етапи ізоляції інциденту, зменшення шкоди та відновлення нормальної роботи систем.

3.3 Методи та підходи для протидії від атак соціальної інженерії.

Ось кілька ключових методів та підходів, які можна використовувати для протидії кібератакам, що базуються на соціальній інженерії:

1. Підвищення рівня обізнаності про соціальну інженерію: Організація тренінгів і семінарів, спрямованих на навчання співробітників різноманітним тактикам, які використовуються зловмисниками. Це допомагає краще розуміти можливі ризики і бути готовими до виявлення підозрілої поведінки або запитів.

2. Розвиток критичного мислення: Навчання співробітників оцінювати інформацію об’єктивно, перевіряти джерела та встановлювати реальність запитів. Це включає уникнення негайної реакції на термінові вимоги, які можуть виявитися маніпулятивними.

3. Впровадження чітких процедур реагування: Розробка інструкцій для дій у разі підозрілих запитів або повідомлень. Це може включати кроки з перевірки, звітності та передачі інформації відповідним відділам безпеки.

4. Використання симуляцій та практичних тренінгів: Проведення тренінгів, які імітують різні сценарії соціальної інженерії, допомагає співробітникам розвивати практичні навички розпізнавання та протидії таким атакам.

4. Створення культури безпеки: Формування у співробітників відчуття відповідальності за захист інформаційних активів. Це включає регулярне нагадування про важливість дотримання стандартів безпеки і стимулювання відкритого обговорення можливих загроз.[18]

5. Реалізація цих підходів сприяє формуванню свідомого та підготовленого колективу, який здатен ефективно протидіяти психологічним маніпуляціям, що є невід’ємною частиною людино-орієнтованих кібератак.

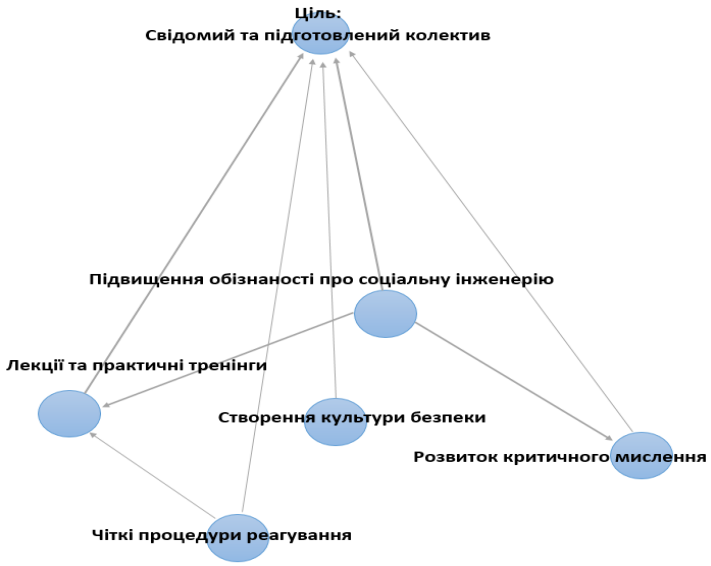


Рисунок 3.2 Діаграма рекомендацій комлексної протидії методам соціальної інженерії.

Успішна протидія атакам соціальної інженерії потребує комплексного підходу, який включає підвищення обізнаності, розвиток критичного мислення, впровадження чітких процедур реагування та проведення практичних тренінгів. Реалізація цих заходів, разом із формуванням культури безпеки, створює свідомий та підготовлений колектив, здатний ефективно захищати організацію від кібератак соціальної інженерії.

Висновки до третього розділу

У третьому розділі розглянуто комплексні підходи до протидії атакам соціальної інженерії, зокрема через психологічні методи та технічні заходи. Зловмисники часто використовують маніпуляції з довірою, авторитетом і психологічний тиск, що ставить під загрозу кібербезпеку організацій. Для ефективного захисту необхідно поєднувати психологічні методи та технічні засоби. Рекомендовано підвищувати обізнаність працівників через навчальні програми та симуляції атак, впроваджувати двофакторну автентифікацію та регулярні оновлення програмного забезпечення, а також розробляти чіткі політики безпеки і реагування на інциденти. Важливим аспектом є створення культури безпеки, де кожен співробітник усвідомлює свою роль у захисті інформаційних ресурсів. Всі ці заходи разом забезпечують формування свідомого та підготовленого колективу, здатного протистояти сучасним методам соціальної інженерії.

ВИСНОВОК

У межах роботи було досліджено основні методи соціальної інженерії, та їх впливу на організації, зокрема на їх інформаційну безпеку.

Статистичний аналіз показав кількість випадків атак методами соціальної інженерії на організації та впливу у розрізі сфер економічної діяльності.

Запропонована структурна схема системи відтворення реалістичних сценаріїв для навчання персоналу, що може значно підвищити протидію атакам соціальної інженерії та створити свідомий та підготовлений колектив.

І нарешті, для ефективної протидії атакам соціальної інженерії необхідно впроваджувати комплексні заходи, які включають як психологічні методи впливу, так і технічні інструменти, що забезпечують високий рівень кібербезпеки в організації. Всі ці заходи сприяють створенню культури безпеки та підготовленості, що допомагає мінімізувати ризики від сучасних кіберзагроз.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Що таке соціальна інженерія? Microsoft 2024 URL: https://support.microsoft.com/uk- ua/skype/%D1%89%D0%BE- %D1%82%D0%B0%D0%BA%D0%B5- %D1%81%D0%BE%D1%86%D1%96%D0%B0%D0%BB%D1%8C%D0%BD%D0%B0- %D1%96%D0%BD%D0%B6%D0%B5%D0%BD%D0%B5%D1%80%D1%96%D1%8F-085cdf83-eade-4482-8eea-284b9ae97951
2. IBM Security X- Force URL:https://secure- iss.com/wp- content/uploads/2023/02/IBM-Security-X-Force-Threat-Intelligence-Index-2023.pdf.
3. Соціальна інженерія: ТОП 5 атак та методик захисту. URL: https://nwu.com.ua/bloh/statti/top-5-naipopuliarnishykh-metodiv-sotsialnoi-inzhenerii-i-metody-zakhystu-vid-nykh (дата звернення 18.05.2020).
4. Кібернетична модель APT атаки / Яковів, І. Кібернетична модель APT атаки / Ігор Яковів // Information Technology and Security. – 2018. – Vol. 6, Iss. 1 (10). – Pp. 46–58. – Bibliogr.: 11 ref. URL: https://ela.kpi.ua/items/7da2c443-bbb4-4d32-b11b-f4fb4bb1c21e
5. Дослідження потенційного впливу соціальної інженерії на процеси цифрової трансформації Савченко В. А: 2024. №4 .
6. Proofpoint за 2023 рік URL:https://www.proofpoint.com/us/blog/security-awareness-training/2024-state-of-phish-report
7. Top Cybersecurity Statistics for 2024 / Jacob Fox URL: https://www.dqsglobal.com/uk-ua/navchajtesya/blog/cili-informacijnoyi-bezpeki-ta-yihznachennya (дата звернення 8.12.2023).
8. Цілі інформаційної безпеки та їх значення. URL: https://www.dqsglobal.com/uk-ua/navchajtesya/blog/cili-informacijnoyi-bezpeki-ta-yihznachennya (дата звернення 12.10.2024).
9. Кібербезпека та захист інформації. URL: http://tr.knute.edu.ua/files/2021/05.pdf (дата звернення 28.02.2024).

10. Соціальна інженерія: Огляд та методи захисту. веб-сайт. URL: https://www.sans.org/white-papers/3380/
11. Phishing.org. веб-сайт. URL: https://www.phishing.org/
12. OWASP: Список найпоширеніших атак, орієнтованих на людський фактор. веб-сайт. URL: https://owasp.org/www-project-top-ten/
13. Книга "Social Engineering: The Art of Human Hacking". веб-сайт. URL: https://www.amazon.com/Social- Engineering- Art- Human- Hacking/dp/0470 639539.
14. Як захиститися від атак соціальної інженерії. веб-сайт. URL: https://www.csoonline.com/article/3544210/how-to-defend-against-social-engineering-attacks.html
15. Шпигунство. 2014. №1. С. 16- 22. URL: http://nbuv.gov.ua/UJRN/szi_2014 _1_5 (дата звернення 09.05.2024).
16. Лебедєв О.М., Ладик О.І. Цифрова техніка: навч. посіб. Київ : Політехніка, 2004. 320 с.
17. Дія Освіта.Кібербезпека. Веб- сайт. URL: https://osvita.diia.gov.ua/catalog/topic/cyber-security (дата звернення 24.10.2024).
18. Photonic approach for microwave spectral analysis based on Fourier cosine transform / Yun Wang, Hao Chi, Xianmin Zhang, Shilie Zheng, Xiaofeng Jin : Optics let. 2011. Vol. 36, № 19. P. 377-389.
19. Кібербезпека для ГО. Веб- сайт. URL: https://courses.zrozumilo.in.ua/courses/course-v1:eef+EEF-034+March2023/about (дата звернення 24.10.2024).
20. Дія Освіта.Кібербезпека. Персональні дані Веб- сайт. URL: https://osvita.diia.gov.ua/courses/personaldata (дата звернення 24.10.2024).
21. Дія Освіта.Кібербезпека. Персональні дані Веб- сайт. URL: https://osvita.diia.gov.ua/courses/personal-cyberhygiene (дата звернення 24.10.2024).
22. Prometheus.Cyber- security. URL: https://prometheus.org.ua/prometheus-plus/cyber-security-google/ (дата звернення 24.11.2024).

ДОДАТКИ

Додаток А

Рисунок А.1 – ER-діаграма бази даних

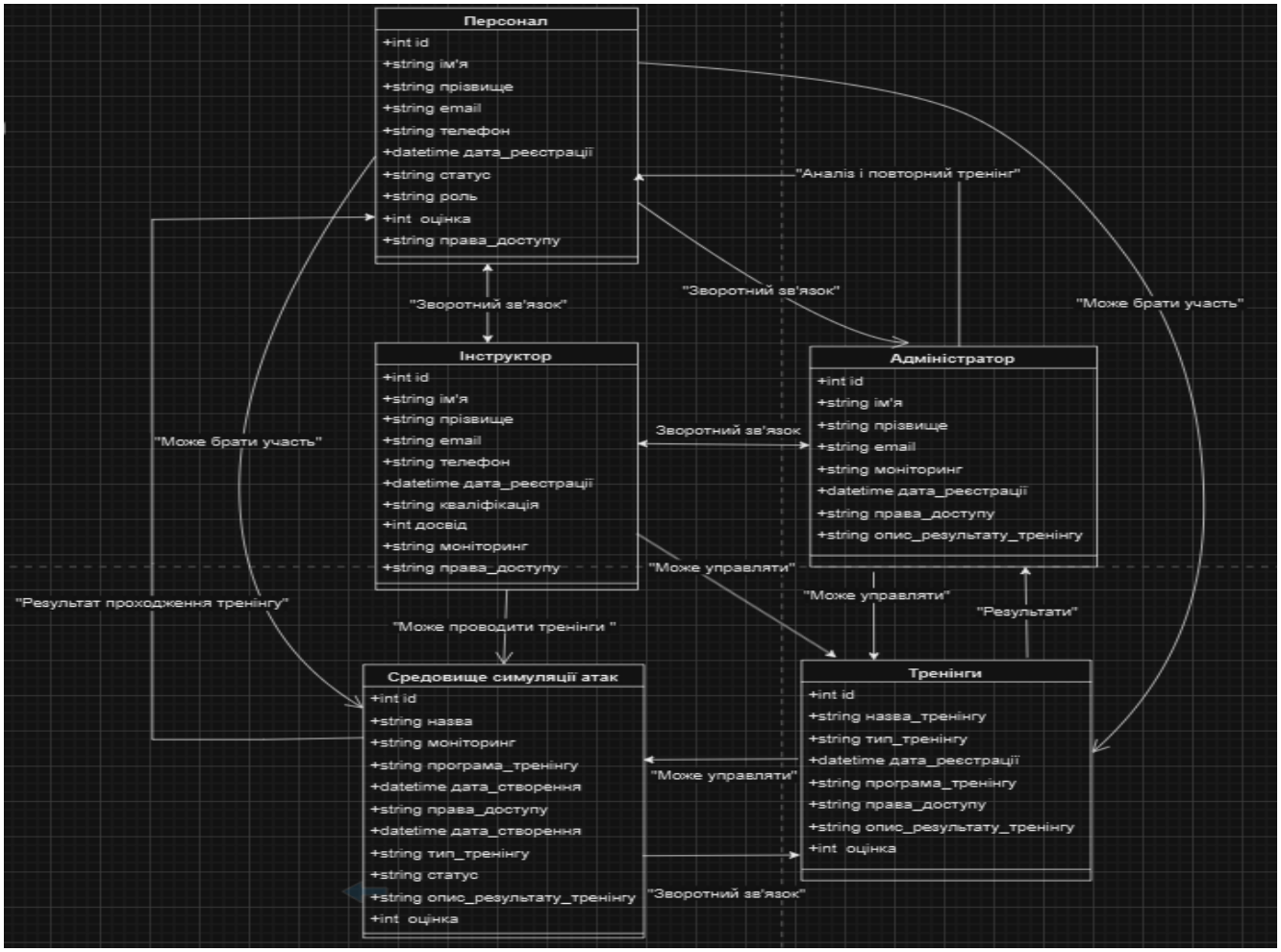
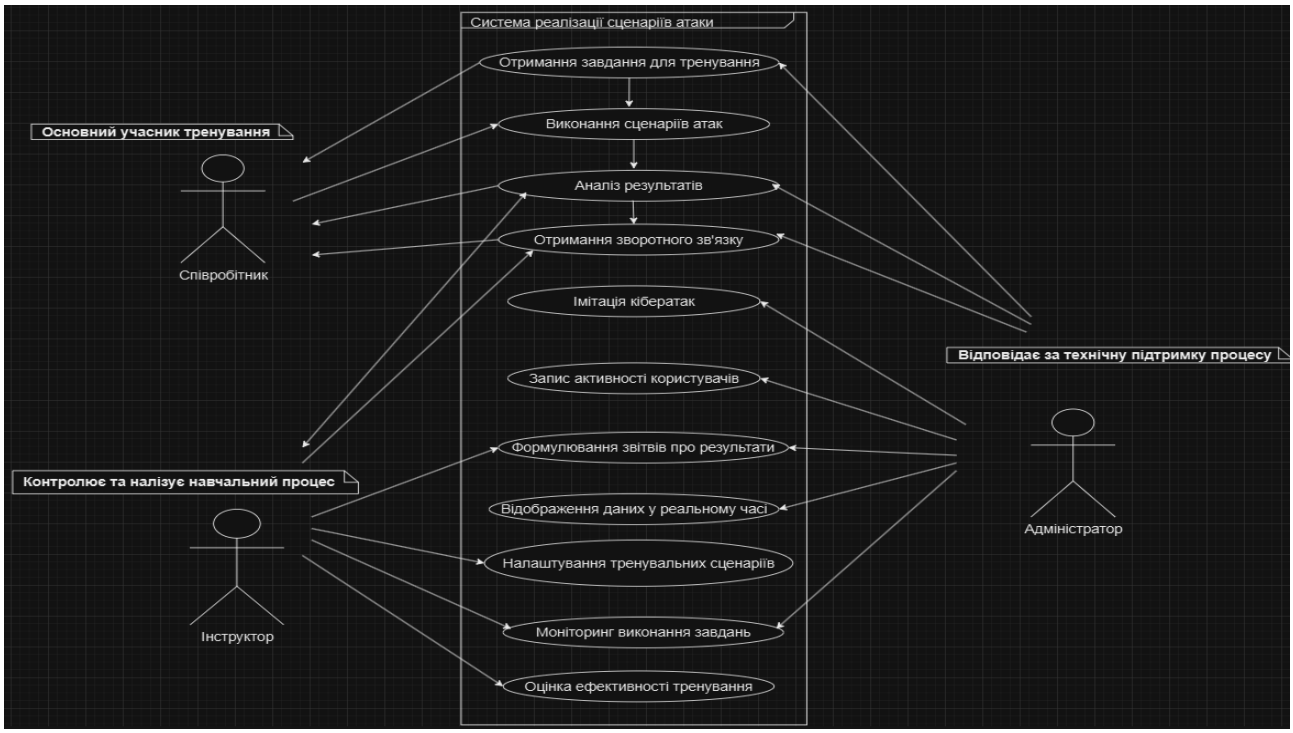


Рисунок А.2 – UML діаграма прецидентів



Додаток Б

Розробка рекомендацій психологічної протидії атакам соціальної інженерії

Психологічна підтримка та консультації для працівників, які можуть стикнутися зі стресом або травматичними наслідками через кібератаки, є важливою складовою комплексної стратегії забезпечення кібербезпеки. Такі атаки здатні спричинити значний психологічний тиск, особливо якщо вони призводять до витоку конфіденційної інформації чи порушення звичних робочих процесів.

1. Роль психологічної підтримки: У разі успішних кібератак працівники можуть відчувати провину, стрес або навіть емоційну травму. Надання їм підтримки допомагає справитися з цими переживаннями та зменшити довгострокові негативні наслідки для їхнього психічного стану.

2. Організація консультацій та сесій зі стрес-менеджменту: Забезпечення доступу до професійних психологів чи терапевтів, які можуть надати індивідуальні або групові консультації. Такі сесії допомагають співробітникам розробити ефективні стратегії управління стресом і подолання труднощів, викликаних кібератаками.
3. Створення безпечного середовища для обговорення проблем: Важливо формувати атмосферу довіри, де працівники можуть відкрито ділитися своїми переживаннями та обговорювати вплив кібератак на їхнє професійне і особисте життя.
4. Розробка програм підтримки персоналу (EAP): Впровадження програм допомоги співробітникам, які включають психологічну підтримку, може стати ключовим елементом для забезпечення всебічної турботи про працівників

Додаток В

Кібербезпека для ГО

Курс про захист даних, налаштування месенджерів, пошуковиків і хмарних сервісів, та загалом — як дбати про особисту і корпоративну цифрову безпеку.

Структура курсу
Курс містить 10 лекцій із практичними завданнями:

Серія 1: Інтро. Про що курс. Знайомство з героями курсу.
Серія 2: Аудит цифрової безпеки та персональних даних в акаунтах Google.
Серія 3: Аудит цифрової безпеки та персональних даних в акаунтах Facebook.
Серія 4: Що таке менеджери паролів та як ними користуватися?
Серія 5: На що звернути увагу при виборі месенджерів? Комунікація у Viber і Telegram

Серія 6: Комунікація у WhatsApp і Signal, а також — Seassion і Thereema.

Серія 7: Комунікація за відсутності стільникового зв’язку.

Серія 8: Шифрування важливих документів.

Серія 9: Резервне копіювання важливих документів.

Серія 10: Захист документів від інтернет-шахраїв.

Дія.Освіта Кібербезпека

Персональні дані і політика приватності: що це та як безпечно ними управляти. [20]

Персональна кібергігієна. Базові правила гігієни в інтернеті. [21]

Prometheus

Foundations of Cybersecurity. [22]

Познайомтеся зі світом кібербезпеки за допомогою інтерактивної навчальної програми, розробленої Google. Дізнайтеся про важливі події, які призвели до розвитку сфери кібербезпеки, зрозумійте важливість кібербезпеки в сучасних бізнес-операціях, а також вивчіть посадові обов’язки та навички аналітика з кібербезпеки початкового рівня.

Після після закінчення цього курсу ви:

• матимете основні навички та знання, необхідні, щоб стати аналітиком з кібербезпеки;

• знатимете, як атаки на безпеку впливають на бізнес-операції;

• вивчите 8 доменів безпеки CISSP.

• визначите сфери безпеки, фреймворки та засоби контролю;

• засвоїте етику безпеки;

• опануєте загальні інструменти, якими користуються аналітики кібербезпеки.

Структура курсу:

- Play It Safe: Manage Security Risks
- Connect and Protect: Networks and Network Security
- Tools of the Trade: Linux and SQL
- Assets, Threats, and Vulnerabilities
- Sound the Alarm: Detection and Response
- Automate Cybersecurity Tasks with Python
- Put It to Work: Prepare for Cybersecurity Jobs