Міністерство освіти і науки України
Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп’ютерної інженерії та кібербезпеки

ПОЯСНЮВАЛЬНА ЗАПИСКА

до випускної кваліфікаційної роботи магістра на тему:
«Дослідження та послаблення впливу соціальної інженерії на сучасні системи безпеки»

Виконала студентка 2-го курсу групи КБм-23-1
спеціальності 125 «Кібербезпека та захист інформації»
_____ Дарина Шевчик
Керівник завідувач кафедри КІ та КБ, к.т.н., доцент
_____ Андрій Єфіменко
Рецензент доцент кафедри КІ та КБ, к.т.н.
_____ Олександр Пірог

м.Житомир – 2024

Державний університет «Житомирська політехніка»

Факультет інформаційно-комп'ютерних технологій

Кафедра комп'ютерної інженерії та кібербезпеки

Спеціальність 125 «Кібербезпека та захист інформації»

Освітня програма «Кібербезпека»

ЗАТВЕРДЖУЮ
Завідувач
кафедри комп'ютерної
інженерії та кібербезпеки
Андрій Єфіменко
17 вересня 2024 р.

ЗАВДАННЯ

на випускну кваліфікаційну роботу бакалавра

Студентка: Шевчик Дарина Анатоліївна

Тема роботи: «Дослідження та послаблення впливу соціальної інженерії на сучасні системи безпеки»

затверджена Наказом університету від 17 вересня 2024 р. № 479/с

Термін здачі студентом закінченої роботи ___15 грудня 2024_____.

Вихідні дані роботи (зазначається предмет і об'єкт дослідження):

Об'єктом дослідження є процес дослідження методів соціальної інженерії та розробки заходів послаблення її впливу на сучасні системи кібербезпеки. Предметом дослідження є методи атак соціальної інженерії та вразливості, на які вони націлені.

Обладнання та програмне забезпечення:

1. Kali Linux (2024.4)
2. Програмне забезпечення «VirtualBox» v. 7.1.4 r165100 (Qt6.5.3)
3. Ubuntu (20_04 LTS)
4. Програмне забезпечення «Social Engineer Toolkit» v. 6.0
5. Розширення для браузера «Bitwarden»

Консультанти з випускної кваліфікаційної роботи із зазначенням розділів, що їх стосуються

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Єфіменко А.А.	17.09.2024	17.09.2024
2	Єфіменко А.А.	05.10.2024	15.10.2024
3	Єфіменко А.А.	10.11.2024	20.11.2024

Студентка _____ Дарина Шевчик

Керівник _____ Андрій Єфіменко

Календарний план

№ з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка завдання	17.09.2024	Виконано
2	Аналіз об’єкта дослідження	18.09.2024	Виконано
3	Постановка задачі дослідження	19.09.2024	Виконано
4	Опрацювання літературних джерел	20.09.2024	Виконано
5	Пошук програмного забезпечення	21.09.2024	Виконано
6	Дослідження сучасних методів, що застосовуються в соціальній інженерії	01.10.2024	Виконано
7	Дослідження програмного забезпечення для симуляції атак соціальної інженерії	10.10.2024	Виконано
8	Моделювання фішингової атаки	15.10.2024	Виконано
9	Аналіз вразливостей систем захисту пов’язаних з соціальною інженерією	20.10.2024	Виконано
10	Розробка рекомендацій для навчальних програм для персоналу	10.11.2024	Виконано
11	Дослідження функціоналу парольних менеджерів	01.12.2024	Виконано
12	Оформлення пояснювальної записки	05.12.2024	Виконано
13	Отримання відгуку керівника та рецензії на кваліфікаційну роботу	15.12.2024	Виконано
14	Захист	26.12.2024	Виконано

Студентка _____ Дарина Шевчик

Керівник _____ Андрій Єфіменко

АНОТАЦІЯ

Випускна робота магістра складається з пояснювальної записки. Пояснювальна записка до випускної магітерської роботи містить 71 сторінку, 30 рисунків та 2 таблиці. Перелік посилань містить 31 літературне джерело.

Останнім часом все більша частина нашого життя, в тому числі робоча сфера, переходять у дистанційну форму. В зв'язку з цим, зросла кількість атак соціальної інженерії, що спрямовані на вразливості пов'язані з людським фактором.

Метою цієї кваліфікаційної роботи є дослідження та послаблення впливу соціальної інженерії на сучасні системи безпеки шляхом мінімізації пов'язаних вразливостей.

У першому розділі було розглянуто теоретичні відомості про соціальну інженерію та методи, що в ній використовуються.

У другому розділі було розглянуто програмне забезпечення, що використовуються соціальними інженерами, та визначено основні вразливості, на які націлені такі атаки.

У третьому розділі було розглянуто технічні заходи що впроваджуються для мінімізації впливу атак соціальної інженерії, в тому числі навчання персоналу; розглянуто впровадження безпекових політик та парольних менеджерів для мінімізації атак соціальної інженерії.

Ключові слова: СОЦІАЛЬНА ІНЖЕНЕРІЯ, АУТЕНТИФІКАЦІЯ, ЗАХИСТ ІНФОРМАЦІЙНИХ СИСТЕМ, ФІШИНГ.

ANNOTATION

A master's degree qualification work consists of an explanatory note. The explanatory note to the master's thesis contains 71 pages, 30 figures and 2 tables. The list of references includes 31 literary sources.

Recently, more and more parts of our lives, including the work sphere, are moving into a remote form. In this regard, the number of social engineering attacks aimed at vulnerabilities related to the human factor has increased.

The purpose of this qualification work is to study and mitigate the impact of social engineering on modern security systems by minimizing related vulnerabilities.

The first chapter reviewed theoretical information about social engineering and the methods used in it.

The second chapter reviewed the software used by social engineers and identified the main vulnerabilities that such attacks target.

The third chapter reviewed technical measures implemented to minimize the impact of social engineering attacks, including staff training; the implementation of security policies and password managers to minimize social engineering attacks was considered.

Keywords: SOCIAL ENGINEERING, AUTHENTICATION, PROTECTION OF INFORMATION SYSTEMS, PHISHING.

ЗМІСТ

АНОТАЦІЯ 5
ANNOTATION 6
ВСТУП 8
РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ 10
1.1. Поняття та історія розвитку соціальної інженерії 10
1.2. Основні методи та техніки соціальної інженерії 11
1.3. Психологічні аспекти впливу на людину, що використовуються в соціальній інженерії 13
1.4. Вплив соціальної інженерії на сучасну кібербезпеку 15
РОЗДІЛ 2. АНАЛІЗ ТА ДОСЛІДЖЕННЯ ЗАГРОЗ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ ... 18
2.1. Аналіз вразливостей систем безпеки пов'язані із соціальної інженерією 18
2.2. Огляд програмних інструментів що використовуються в соціальній інженерії 22
2.3. Моделювання соціально-інженерної атаки 29
РОЗДІЛ 3. РОЗРОБКА ЗАХОДІВ ЗАХИСТУ ВІД СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ 38
3.1. Технічні методи захисту від соціальної інженерії 38
3.2. Впровадження безпекових політик для протидії соціальній інженерії 46
3.3. Впровадження заходів щодо навчання персоналу 62
ВИСНОВКИ 67
ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ 69

ВСТУП

Актуальність теми. В сучасному світі все більша частина нашого життя переходить в «онлайн». Наше дозвілля часто пов'язане з Інтернетом, спілкування великою частиною відбувається через месенджери, велику частину послуг можна отримати не виходячи з дому. Значним поштовхом до цього стала епідемія вірусу COVID-19, в наслідок якої довгий час діяли обмеження на скупчення людей в публічних місцях. Не винятком стала й сфера роботи: усе більше людей почали працювати онлайн а не з офісу.

Результатом виявилось те, що організація роботи у великій частині сфер, особливо у сфері інформаційних технологій, може досить легко трансформуватись у віддалений тип, при цьому не втрачаючи своєї ефективності. В деяких випадках працівники, що працюють віддалено, показують навіть більшу ефективність. Для самих організацій такий тип роботи є більш економічно вигідним, оскільки зменшується кількість витрат на утримання офісного приміщення, оренду, фінансування послуг таксі для персоналу протягом нічних змін, тощо.

Але трансформація організації роботи у дистанційну форму має й суттєві мінуси. Не зважаючи на усі переваги, основною дилемою організації праці у форматі онлайн є питання безпеки. В таких умовах ускладнюється забезпечення безпечного процесу праці та захищеності внутрішніх систем, баз даних, серверів тощо.

Усе це дозволило виявити тенденції у вразливостях систем безпеки, що притаманні сучасним компаніям. Виявилось що однією з найслабших ланок в системах безпеки є людський фактор. Саме тому все сильніше розвивається соціальна інженерія, що спрямована на злам системи шляхом обходу технічного захисту через використання людських вразливостей. Досить часто жертвами атак соціальної інженерії є працівники служб підтримки, що в реальному часі спілкуються з великою кількістю людей та мають доступ до клієнтської інформації.

Саме тому, однією з найважливіших задач сучасних фахівців з кібербезпеки є дослідження методів соціальної інженерії та впровадження нових методів захисту

від впливу таких атак, зокрема шляхом постійного внутрішнього навчання персоналу та підвищення загального рівня обізнаності в цій темі.

Метою кваліфікаційної роботи дослідження впливу атак соціальної інженерії на сучасні системи безпеки; впровадження ефективних заходів мінімізації впливу таких атак, зокрема шляхом постійного внутрішнього навчання персоналу та підвищення загального рівня обізнаності в цій темі.

Для досягнення цієї мети необхідно виконати такі завдання:

– вивчення поняття соціальної інженерії;

– практичне дослідження вразливостей систем безпеки;

– дослідження програмного забезпечення що використовується в атак соціальної інженерії;

– моделювання атаки соціальної інженерії;

– дослідження та впровадження заходів зменшення впливу атак соціальної інженерії шляхом мінімізації пов’язаних вразливостей.

Об’єктом дослідження є процес дослідження методів соціальної інженерії та розробки заходів послаблення її впливу на сучасні системи кібербезпеки.

Предметом дослідження є методи атак соціальної інженерії та вразливості, на які вони націлені.

Для досягнення мети було використано такі **методи дослідження**: аналіз літературних джерел та відкрити інтернет ресурсів; експериментальне модулювання; порівняння програмного забезпечення за визначеними критеріями; апробація результатів.

Практичне значення роботи полягає у розробці системи заходів для мінімізації визначених вразливостей, впровадження яких дозволяє суттєво знизити вплив атак соціальної інженерії на системи безпеки.

.

РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ

1.1. Поняття та історія розвитку соціальної інженерії

Соціальна інженерія — це метод маніпуляції людьми з метою отримання конфіденційної інформації, доступу до систем та/або здійснення певних дій. На відміну від технічних атак, соціальна інженерія спрямована не на подолання технічних бар'єрів системи захисту, а фокусується на людському факторі, використовуючи психологічні прийоми для обману жертви [2].

Основними цілями соціальної інженерії є:

– Отримання конфіденційної інформації такої як логіни, паролі, персональні дані.

– Отримання доступу до інформаційних систем.

– Маніпуляція поведінкою жертви метою переконання у виконанні певної дії, наприклад, переказу грошей або встановлення шкідливого ПЗ).

Соціальна інженерія, як метод маніпуляції людьми, існувала ще задовго до появи сучасних технологій. У різні історичні періоди правителі, шпигуни та шахраї використовували обман для отримання інформації або досягнення своїх цілей. Прикладом може слугувати "Троянський кінь" — один із найвідоміших історичних випадків обману, коли греки використали хитрість для проникнення у Трою.

У період XIX — початок XX століття з’являється безліч аферистів, які вдосконалюють методи психологічного впливу. Один з найвідоміших шахраїв — Чарльз Понці, який створив схему, що стала основою для сучасних фінансових пірамід. Також відомі "баронети" або "люди, що продавали Ейфелеву вежу" — приклади складних афер, що використовували маніпуляцію довірою.

1960–1980-ті роки – початок ери технологій. З поширенням телефонного зв'язку шахраї почали використовувати нові методи, зокрема "phreaking" — маніпуляції телефонними мережами для отримання безкоштовних дзвінків. Один із найвідоміших прикладів — Джон Дрейпер, який використовував дитячі свистки для обходу телефонних систем. Також у цей період вів свою діяльність Кевін

Мітнік — один із першопроходьців сучасної соціальної інженерії, що починав як хакер, використовуючи психологічні маніпуляції для отримання доступу до комп'ютерних мереж ще в 1970-х роках. Згодом став консультантом з інформаційної безпеки та автором книг про соціальну інженерію. Одні за найвідоміших з них – «Мистецтво обману» та «Мистецтво вторгнення».

З поширенням інтернету та електронної пошти з'явилися нові можливості для соціальної інженерії. Перші фішингові атаки датуються серединою 1990-х. Шахраї надсилали електронні листи, що імітували відомі сервіси, щоб отримати паролі користувачів.

У 2000-их роках термін "соціальна інженерія" почав широко використовуватись у сфері кібербезпеки. Основи методів були описані в роботах Кевіна Мітніка, зокрема в книзі "Мистецтво обману" (2002 рік), яка стала своєрідним підручником для розуміння природи соціальної інженерії. З'являються масові розсилки фішингових листів, що імітують банки або платіжні системи. Почали поширюватися афери на кшталт "Нігерійських листів" (419 scam), де обіцяли великі суми грошей в обмін на "допомогу".

З поширенням Facebook, LinkedIn та інших платформ зловмисники отримали нові можливості для збору інформації про жертв (OSINT — Open Source Intelligence). Соціальні медіа стали основним інструментом для "претекстингу" та створення цільових атак (spear-phishing).

Сучасні соціальні інженери використовують штучний інтелект для створення реалістичних відео, аудіо або текстів. Технології deepfake дозволяють фальсифікувати відеодзвінки чи голосові повідомлення, що значно ускладнює виявлення атак.

1.2. Основні методи та техніки соціальної інженерії

Соціальна інженерія використовує різноманітні методи для маніпуляції людьми з метою отримання конфіденційної інформації або досягнення інших злочинних цілей. Розглянемо найпоширеніші методи і техніки [2]:

1) Фішинг — це метод, при якому зловмисник надсилає підроблені електронні листи або повідомлення, що імітують офіційні запити від відомих компаній (банків, сервісів тощо). Мета — змусити жертву надати конфіденційну інформацію або завантажити шкідливе ПЗ.

Види фішингу:

– Стандартний фішинг: Масова розсилка листів із загальними запитами.

– Spear-phishing: Цільова атака на конкретну особу чи організацію з використанням персоналізованої інформації.

– Whaling: Атака на топ-менеджерів або керівників компаній.

– Clone phishing: Створення підробленої копії легітимного листа з шкідливими посиланнями.

2) Вішинг — це форма фішингу, що використовує телефонні дзвінки. Зловмисники видають себе за співробітників компаній (банків, техпідтримки) для отримання конфіденційних даних.

Техніки вішингу:

– Використання підроблених номерів (спуфінг).

– Створення термінової ситуації (наприклад, "ваш рахунок заблоковано").

3) Смішинг — це фішинг через SMS-повідомлення. Зловмисник надсилає текстове повідомлення з посиланням на шкідливий сайт або з проханням зателефонувати за певним номером.

4) Претекстинг – передбачає створення фальшивої ситуації або історії для отримання інформації. Зловмисник видає себе за іншу особу (співробітника компанії, державного органу тощо).

Техніки:

– Використання авторитету (псевдо-дзвінок від "служби безпеки").

– Збір попередньої інформації для більшої переконливості.

5) Привілейований доступ (Baiting) — передбачає заманювання жертви за допомогою привабливого "гачка" (безкоштовне програмне забезпечення, виграші тощо), що насправді містить шкідливе ПЗ.

Види та приклади:

– Фізичний baiting: Розміщення зараженого USB-накопичувача у загальнодоступному місці. Співробітник підключає його до корпоративного комп'ютера, запускаючи шкідливе ПЗ.

– Цифровий baiting: Посилання на "безкоштовне" завантаження програм або фільмів.

6) Соціальні медіа атаки — це метод фізичного доступу до захищених приміщень компанії. Зловмисник проходить вслід за співробітником, який має доступ, використовуючи ввічливість або довіру.

Приклади:

– Імітація співробітника, кур'єра чи технічного працівника.

7) Соціальні медіа атаки — зловмисники використовують соціальні мережі для збору інформації про жертв або для маніпуляцій.

8) Reverse Social Engineering (зворотна соціальна інженерія). Зловмисник створює умови, при яких жертва сама звертається до нього за допомогою. Наприклад, поширює шкідливе ПЗ, а потім пропонує "усунення проблеми".

1.3. Психологічні аспекти впливу на людину, що використовуються в соціальній інженерії

Соціальна інженерія базується на глибокому розумінні людської психології. Зловмисники використовують різні психологічні прийоми для маніпулювання людьми з метою отримання конфіденційної інформації або досягнення інших цілей. Розглянемо ключові психологічні аспекти, що застосовуються в соціальних атаках:

1) Використання авторитету. Люди схильні довіряти інформації або виконувати вказівки, якщо вони надходять від осіб, які мають авторитет або займають вищу посаду.

Приклади:

– Зловмисник видає себе за керівника компанії або співробітника служби безпеки.

– Підроблені листи від імені банків чи державних установ.

2) Використання страху та паніки. Створення відчуття терміновості чи загрози, що призводить до імпульсивних рішень жертви.

Приклади:

– Листи з погрозами блокування облікового запису.

– Дзвінок із повідомленням про несанкціоновану транзакцію.

3) Ефект терміновості. Створення у жертви відчуття, що потрібно негайно виконати певну дію, інакше будуть негативні наслідки.

Приклади:

– "Ваш акаунт буде видалено через 24 години, якщо ви не підтвердите свої дані.".

– "Акція діє лише сьогодні!".

4) Взаємність. Люди відчувають зобов’язання "відплатити" за отриману допомогу або послугу.).

Приклади:

– Зловмисник надає "допомогу" у вигляді фіктивного вирішення проблеми, а потім просить послугу у відповідь.

– Пропозиція "безкоштовного" ресурсу в обмін на інформацію.

5) Соціальне підтвердження (Social Proof). Люди схильні наслідувати поведінку інших, особливо в незрозумілих або нових ситуаціях.

Приклади:

– Фальшиві відгуки або коментарі для створення довіри до шахрайського ресурсу.

– Підроблені повідомлення про те, що "багато користувачів уже виграли" або "отримали компенсацію".

6) Використання жадібності. Пропонування "вигоди" чи "виграшу" для того, щоб змусити жертву виконати необхідну дію.

Приклади:

– Листи про виграш у лотерею.

– Пропозиція "безкоштовного доступу" до дорогого програмного забезпечення.

7) Використання довіри та співчуття. Зловмисник намагається викликати довіру або співчуття, щоб маніпулювати жертвою. Схильність довіряти знайомим або людям зі схожим досвідом.

Приклади:

– Шахрайські історії про хвороби або фінансові труднощі.

– Видавання себе за друга або знайомого.

8) Використання допитливості. Експлуатація природної людської цікавості для стимулювання певних дій.

Приклади:

– Підозрілі листи із темою "Важлива інформація про вас".

– Файли з назвами "конфіденційно" або "приватні дані".

9) Конформізм. Бажання бути частиною певної групи або колективу часто використовується для маніпуляції поведінкою.

Приклади:

– Фішингові атаки на співробітників компанії з використанням корпоративної культури.

– Запрошення до "закритих" спільнот у соцмережах.

10) Компліменти та лестощі. Використання лестощів для створення позитивного ставлення до зловмисника.

Приклади:

– Повідомлення з компліментами або "визнанням" досягнень.

– Запити від "шанувальників" або "потенційних партнерів".

1.4. Вплив соціальної інженерії на сучасну кібербезпеку

Соціальна інженерія є однією з найефективніших та небезпечних загроз для кібербезпеки, оскільки вона спрямована на вразливості пов’язані з людським фактором, а не на технічний злам системи. Зловмисники використовують

психологічні техніки для отримання конфіденційної інформації, доступу до систем або компрометації організаційних ресурсів.

Основні наслідки впливу соціальної інженерії:

– Компрометація даних: витік інформації, що може призвести до фінансових втрат і репутаційного збитку.

– Фінансові збитки: шахрайські дії, що спричиняють значні фінансові втрати для компаній.

– Підрив репутації: розголошення конфіденційної інформації чи успішні атаки можуть завдати шкоди іміджу організації.

– Порушення роботи систем: отримання доступу до внутрішніх мереж може призвести до саботажу чи зупинки критично важливих процесів.

Відомі приклади соціально-інженерних атак на компанії [1]

1. Атака на Twitter (2020)

Сутність атаки: хакери використали техніку фішингу та телефонного шахрайства для компрометації акаунтів співробітників Twitter. Вони переконали кількох працівників надати доступ до внутрішніх інструментів управління.

Наслідки: було захоплено акаунти відомих осіб, включаючи Ілона Маска, Джеффа Безоса та Барака Обами. Зловмисники опублікували шахрайські повідомлення з проханням надіслати біткоїни, що призвело до фінансових втрат користувачів. Атака також завдала серйозного удару по репутації Twitter.

2. Атака на Sony Pictures (2014)

Сутність атаки: зловмисники отримали доступ до корпоративної мережі Sony через фішингові атаки на співробітників. Соціальна інженерія дозволила їм заволодіти обліковими даними для входу в мережу.

Наслідки: були викрадені та оприлюднені конфіденційні дані, включаючи внутрішні електронні листи, фінансову інформацію та неопубліковані фільми. Це призвело до значних репутаційних і фінансових збитків для компанії.

3. Атака на Uber (2016)

Сутність атаки: хакери використали соціальну інженерію для отримання доступу до облікового запису одного з інженерів Uber. Згодом вони проникли у

внутрішню систему GitHub компанії, де зберігалися облікові дані до хмарних сервісів.

Наслідки: були викрадені особисті дані 57 мільйонів користувачів і водіїв. Uber сплатив зловмисникам $100 тисяч за знищення даних, але витік все одно став публічним, що призвело до великих штрафів і репутаційного збитку.

4. Атака на банк Bangladesh Bank (2016)

Сутність атаки: хакери використали соціальну інженерію для доступу до внутрішніх систем банку, а потім намагалися перевести $1 мільярд через систему SWIFT. Атака почалася з фішингового листа, який отримали працівники банку.

Наслідки: хоча більшість транзакцій вдалося зупинити, зловмисники все ж викрали $81 мільйон. Цей інцидент показав, як соціальна інженерія може бути використана для складних фінансових махінацій.

Висновки до першого розділу

Отже, було коротко розглянуто поняття соціальної інженерії та види атак соціальної інженерії. Вивчено основні методи що використовуються соціальними інженерами для здійснення атак та методи соціального впливу на людину. Розглянуто вплив атак соціальної інженерії та наслідки таких атак.

РОЗДІЛ 2. АНАЛІЗ ТА ДОСЛІДЖЕННЯ ЗАГРОЗ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ

2.1. Аналіз вразливостей систем безпеки пов'язані із соціальної інженерією

Соціальна інженерія використовує слабкі місця не в технологічних системах, а людський фактор, що робить її особливо небезпечною для корпоративної безпеки. Ці вразливості пов’язані з психологічними, організаційними та поведінковими аспектами роботи співробітників та структурою управління компанією. Розуміння цих вразливостей допомагає краще захищати корпоративні системи від атак.

Можна виділити такі основні вразливості систем безпеки, пов’язані із соціальною інженерією [4]:

1. Людський фактор як найслабша ланка

Системи безпеки можуть бути технічно досконалими, проте їх ефективність залежить від дій користувачів. Люди часто стають жертвами маніпуляцій через відсутність обізнаності, помилкове почуття довіри або необережність [11].

Прояви вразливості:

– Співробітники можуть випадково розкрити конфіденційну інформацію через запит, який здається легітимним.

– Надмірна довіра до джерел, які здаються авторитетними або знайомими.

– Ігнорування правил безпеки через поспіх, втому або недооцінку ризиків.

2. Недостатнє навчання персоналу

Якщо співробітники не отримують регулярного навчання з питань інформаційної безпеки, вони не здатні розпізнати спроби маніпуляції. Без знань про сучасні загрози персонал стає легкою мішенню для зловмисників.

Прояви вразливості:

– Невміння ідентифікувати підозрілі запити або аномальні дії.

– Відсутність реакції на спроби маніпуляцій.

– Незнання політик організації, пов'язаних із захистом даних.

3. Відсутність чітких політик безпеки

Якщо організація не має чітких правил та протоколів у сфері інформаційної безпеки, це створює можливості для експлуатації. Зловмисники використовують неузгодженість дій співробітників або прогалини в процедурах для досягнення своїх цілей.

Прояви вразливості:

– Співробітники не знають, як правильно реагувати на підозрілі ситуації.

– Відсутність стандартизованих процесів перевірки легітимності запитів.

– Невизначеність відповідальності за збереження інформації.

4. Надмірна залежність від технічних засобів захисту

Багато організацій покладаються лише на технічні рішення, такі як антивірусне програмне забезпечення, брандмауери та шифрування, недооцінюючи значення людського фактора.

Прояви вразливості:

– Працівники можуть вважати, що технології забезпечують абсолютний захист, і тому ігнорують базові правила безпеки.

– Відсутність перевірки дій персоналу через припущення, що технічні засоби автоматично блокують загрози.

– Зниження уваги до поведінкових аспектів захисту.

6. Використання спрощених або загальних процесів автентифікації

Слабкі механізми автентифікації або їх відсутність полегшують отримання доступу до систем для зловмисників, які маніпулюють працівниками.

Прояви вразливості:

– Використання простих паролів або однакових для кількох систем.

– Відсутність багатофакторної автентифікації.

– Недотримання політики регулярної зміни паролів.

6. Невпорядкованість у доступі до інформації

Відсутність чітко визначених правил доступу до даних збільшує ризик їх компрометації. Якщо всі співробітники мають доступ до інформації, яка не є необхідною для їхньої роботи, що створює додаткові ризики.

Прояви вразливості:

– Надмірний доступ до систем або даних для працівників, яким це не потрібно.

– Недостатній контроль за діями співробітників у корпоративних системах.

– Відсутність моніторингу та обмежень доступу для тимчасових працівників або підрядників.

7. Соціальні та культурні чинники

У деяких корпоративних культурах працівники можуть бути більш схильними до реагування на фішингові імейли, особливо якщо запит виглядає як прохання від авторитетної особи. Також важливим є небажання ставити під сумнів дії або запити колег.

Прояви вразливості:

– Перевищення повноважень через бажання допомогти колезі або клієнту.

– Небажання ставити додаткові запитання, щоб уникнути конфлікту.

– Залежність від неформальних комунікацій, які можуть бути підроблені.

8. Відсутність моніторингу та аудиту дій співробітників

Якщо організація не відстежує дії своїх працівників у системах або не проводить регулярного аудиту, це ускладнює виявлення потенційних порушень.

Прояви вразливості:

– Несанкціоновані дії співробітників залишаються непоміченими.

– Зловмисники можуть використовувати облікові записи співробітників без ризику бути виявленими.

– Недостатній контроль над доступом до систем після звільнення працівників.

Соціально-інженерні атаки можуть призводити до таких наслідків:

1. Підрив довіри в організації. Коли працівники стають жертвами соціальних атак, це може призвести до недовіри між колегами та до керівництва. Працівники можуть почати сумніватися у правдивості запитів, що надходять від керівників чи партнерів, що ускладнює комунікацію та знижує ефективність робочих процесів.

2. Підрив інформаційної безпеки. Соціальні інженери можуть отримати доступ до критично важливої інформації, обходячи технічні механізми захисту. Навіть найсучасніші системи кібербезпеки не можуть захистити компанію, якщо працівники піддаються маніпуляціям і добровільно передають важливі дані або надають доступ до системи.

3. Фінансові втрати та ризики. Корпоративні атаки через соціальну інженерію можуть завдати значних фінансових збитків. Організації можуть втратити кошти не лише через пряме шахрайство, а й через необхідність відновлення інфраструктури, виплати штрафів або компенсацій клієнтам. Серед фінансових втрат:

– Витрати на відновлення систем і даних після атаки.

– Втрати від несанкціонованих фінансових операцій.

– Штрафи за порушення регуляторних вимог щодо захисту даних.

4. Репутаційні ризики. Успішна соціально-інженерна атака може завдати серйозної шкоди репутації компанії. Витік конфіденційної інформації, особливо даних клієнтів, підриває довіру до організації. В епоху цифрових технологій будь-яка інформація про компрометацію може швидко поширюватися, викликаючи негативний резонанс. Як наслідок:

– Втрата довіри клієнтів та партнерів.

– Зниження вартості бренду.

– Труднощі у залученні нових клієнтів і партнерів.

5. Порушення операційної діяльності. Соціальна інженерія може призвести до серйозних перебоїв у роботі корпоративних систем. Зловмисники можуть отримати доступ до важливих систем або даних, що призводить до зупинки бізнес-процесів або втрати критично важливої інформації.

2.2. Огляд програмних інструментів що використовуються в соціальній інженерії

Зловмисники, які застосовують соціальну інженерію, часто використовують різноманітні програмні інструменти для автоматизації атак, збору інформації, створення підроблених ресурсів або маніпулювання жертвами. Розглянемо деякі види програм, що використовуються у цій сфері:

1) Інструменти для збору інформації (OSINT). OSINT (Open Source Intelligence) — це збір даних з відкритих джерел, що дозволяє отримати необхідну інформацію про ціль. Це можна робити «вручну», наприклад переглядаючи інформацію про людину в соціальних мережах чи відкритих реєстрах, або за допомогою спеціального програмного забезпечення.

Приклади:

– Maltego [23]: інструмент для візуалізації даних та аналізу взаємозв'язків між особами, компаніями, IP-адресами та іншими об'єктами. Використовується для побудови детальних профілів жертви.

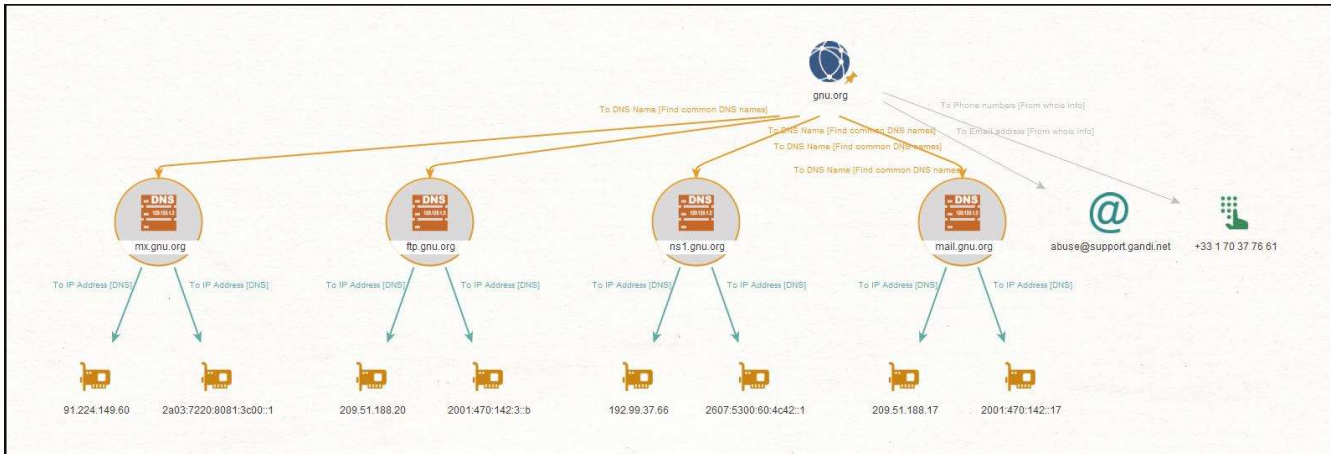


Рисунок 2.1 – Інтерфейс застосунку Maltego

– Recon-ng [24]: фреймворк для збору інформації, що дозволяє автоматизувати OSINT-процес. Має модульну структуру для різних завдань: від пошуку доменів до отримання даних із соціальних мереж.



Рисунок 2.2 – Інтерфейс застосунку Recon-ng

2) Інструменти для створення фішингових сторінок.

Приклади:

– Gophish: Платформа для створення та управління фішинговими кампаніями. Дозволяє легко створювати шаблони фішингових листів і веб-сторінок.

– Social Engineer Toolkit (SET) [21]: Один популярних інструментів для соціальної інженерії, який містить модулі для фішингу, клону веб-сайтів і генерації шкідливих листів.

3) Інструменти для розсилки фішингових листів.

– PhishX: Інструмент для створення фішингових кампаній, що дозволяє налаштовувати підроблені листи, розсилати їх і відстежувати відповіді.

– King Phisher: Рішення для запуску фішингових кампаній, з можливістю детального звітування та відстеження відкриттів листів.

– Microsoft Attack Simulator: інструмент з екосистеми Microsoft 365, який дозволяє моделювати фішингові атаки, тренувати співробітників та оцінювати стійкість організації до загроз соціальної інженерії [31].

4) Інструменти для соціального інжинірингу через телефон (Vishing).

– Caller ID Spoofing Tools: Програми, що дозволяють підробляти номери телефонів, щоб дзвінок виглядав так, ніби він надійшов від офіційної організації..

– iSpoof: Використовується для зміни номера під час дзвінка, що допомагає зловмисникам переконати жертву в автентичності їхніх намірів.

5) Інструменти для створення шкідливого ПЗ і приманок (Baiting).

– Metasploit: Фреймворк для створення та експлуатації вразливостей. У контексті соціальної інженерії використовується для генерації шкідливих файлів, що можуть бути доставлені жертві через електронну пошту..

– MSFvenom: Інструмент для створення корисного навантаження (payloads), що може бути вбудоване у документи або програми.

6) Інструменти для зламу паролів.

Приклади:

– John the Ripper [12]: Програма для підбору паролів. Може використовуватися для розшифровки викрадених хешів паролів.

– Hydra [13]: Інструмент для brute-force атак на онлайн-сервіси та форми аутентифікації.

На основі розглянутого програмного забезпечення, зробимо порівняльну таблицю за такими критеріями:

– Основний функціонал (для чого використовується ПЗ);

– Наявність графічного інтерфейсу;

– Кастомізація (за рівнями – високий, середній, низький);

– Виявлення антивірусами.

Таблиця 2.1 – Порівняння ПЗ що використовується для атак соціальної інженерії

Назва	**Основний функціонал**	**Наявність графічного інтерфейсу**	**Рівень кастомізації**	**Виявлення антивірусами**
Maltego	OSINT-аналіз, створення графів взаємозв'язків між даними	Є	Високий: налаштування джерел даних, власних "трансформів" і автоматизації.	Низьке: не викликає підозр, оскільки орієнтоване на збір даних.

Продовження таблиці 2.1

Recon-ng	Збір OSINT-даних, інтеграція зі сторонніми API	Немає (CLI)	Високий: розширення модулів, налаштування скриптів для збору даних.	Низьке: використовується для пасивного збору даних.
Gophish	Автоматизація фішингових кампаній, генерація звітів	Є	Середній: редагування шаблонів фішингових листів і сценаріїв.	Середнє: може бути заблоковане антивірусами через шкідливі URL.
Social Engineer Toolkit (SET)	Фішингові атаки, клонування сайтів, генерація підроблених сторінок і шкідливого коду	Немає (CLI)	Високий: гнучке налаштування під різні сценарії атак, можливість інтеграції з іншими інструментами.	Високе: багато функцій можуть бути виявлені антивірусами, почти можуть бути додані в блеклисти
PhishX	Створення фішингових кампаній, налаштування шаблонів повідомлень	Немає (CLI)	Середній: редагування шаблонів листів та вибір цільової аудиторії.	Середнє: залежить від налаштувань шаблонів і серверів.
King Phisher	Управління фішинговими кампаніями, відстеження жертв	Є	Середній: можливість налаштувати листи, сторінки та звіти.	Середнє: може бути виявлено через аналіз IP та URL.
Microsoft Attack Simulator	Моделювання фішингових атак, перевірка стійкості організації до атак соціальної інженерії та тренування персоналу.	Є	Середній рівень: можливість налаштування сценаріїв атак відповідно до потреб організації. Обмежений екосистемою Microsoft 365	Низька ймовірність виявлення, оскільки симулятор використовує легітимні інструменти для тестування.

Продовження таблиці 2.1

iSpoof	Спуфінг телефонних номерів, підробка SMS	Немає (CLI)	Низький: мінімальне налаштування тексту повідомлень і номерів.	Низьке: зазвичай не детектується антивірусами.
Metasploit	Експлуатація вразливостей, інтеграція з OSINT-інструментами	Немає (CLI)	Високий: створення модулів та модифікація експлойтів.	Високе: експлойти часто виявляються антивірусами.
MSFvenom	Генерація шкідливого коду та корисних навантажень для експлойтів	Немає (CLI)	Високий: налаштування форматів шкідливого коду, параметрів для обходу антивірусів.	Високе: антивіруси постійно оновлюють бази для детектування.
John the Ripper	Взлом паролів методом брутфорсу або підбору словників	Немає (CLI)	Середній: додавання власних словників, налаштування методів і швидкості атаки.	Низьке: програма орієнтована на локальний аналіз.
Hydra	Атаки на онлайн-сервіси (SSH, HTTP, FTP тощо), брутфорс паролів	Немає (CLI)	Середній: налаштування словників, методів атак і цільових сервісів.	Середнє: може бути виявлено мережевими захисними системами.

2.2.1 Приклад використання інструменту для взламу паролів

Соціальна інженерія використовується в тому числі для отримання паролів користувачів. Часто слабкі паролі (короткі паролі, ті що використовуються стандартні комбінацію типу «12345678» чи «qwerty», або такі, що містять інформацію про користувача, таку як ім’я, кличка домашнього улюбленця чи дата

народження) є причиною того, що зловмисник досить швидко отримує доступ до бажаного ресурсу [9].

John the Ripper - це інструмент з відкритим вихідним кодом для перевірки безпеки паролів і відновлення паролів, доступний для багатьох операційних систем та надає такий функціонал [12]:

– Використання брутфорс атак;

– Словникові атаки: використання заготовлених словників (підтримує понад 20 мов світу), в тому числі зі створенням власних словників;

– Розподілені атаки: John the Ripper має розподілені обчислювальні можливості, які дозволяють кільком комп'ютерам працювати разом для швидкого зламу паролів.

– Підтримка різних форматів хешів: John the Ripper працювати з різними форматами хешів паролів, включаючи MD5, MD4, SHA1, SHA-256, SHA-512.

– Паралельне обчислення: Ця програма використовує багатопотоковість і може розподіляти обчислення між кількома ядрами процесора, дозволяючи їй швидше зламувати паролі.

– Використовується також для аналізу вразливостей систем.

Для використання застосунку, необхідно зробити копію файлу паролів:

```
umask 077
unshadow /etc/passwd /etc/shadow > mypasswd
```

Для зламу паролів використовується команда 'john':

```
john mypasswd
```

Для перегляду зламаних паролів використовується команда:

```
john --show mypasswd
```

Також можна використовувати словники, встановлювати додаткові правила для зламу (такі як довжина паролю або тип хешування):

```
john --wordlist=all.lst --rules --stdout=8 | unique mangled8.lst
john --wordlist=mangled8.lst mypasswd
```

Подивимося, як працює програма, і дізнаємося, як довжина пароля впливає на час, необхідний для його зламу. Для цього ми будемо використовувати віртуальну машину, що працює на дистрибутиві Linux, а саме Ubuntu 20.04 LTS. Створимо кілька користувачів та паролі для кожного з них. Для більшості просто

використаємо прості паролі або так, що співпадають з іменами користувачів: «admin», «qwerty», «123456», «test2», «test3». Для останнього користувача використаємо довгий пароль із великими літерами та спеціальними символами: "longP@assword":

```
student@student-VirtualBox:~$ sudo useradd test1
student@student-VirtualBox:~$ sudo useradd test2
student@student-VirtualBox:~$ sudo useradd test3
student@student-VirtualBox:~$ sudo useradd test4
student@student-VirtualBox:~$ sudo useradd test5
student@student-VirtualBox:~$ sudo useradd test6
student@student-VirtualBox:~$ sudo passwd test1
Новий пароль :
Повторіть новий пароль :
passwd: пароль було успішно змінено
student@student-VirtualBox:~$ sudo passwd test2
Новий пароль :
Повторіть новий пароль :
passwd: пароль було успішно змінено
student@student-VirtualBox:~$ sudo passwd test3
Новий пароль :
Повторіть новий пароль :
passwd: пароль було успішно змінено
student@student-VirtualBox:~$ sudo passwd test4
Новий пароль :
Повторіть новий пароль :
passwd: пароль було успішно змінено
student@student-VirtualBox:~$ sudo passwd test5
Новий пароль :
Повторіть новий пароль :
passwd: пароль було успішно змінено
student@student-VirtualBox:~$ sudo passwd test6
Новий пароль :
Повторіть новий пароль :
passwd: пароль було успішно змінено
```

Рисунок 2.3 – Створення тестових користувачів

Після цього, виконаємо інсталяцію John the Ripper на робочій станції, виконаємо необхідне налаштування та спробуємо зламати паролі користувачів:

```
student@student-VirtualBox:~$ sudo unshadow /etc/passwd /etc/shadow > m
ypasswd
student@student-VirtualBox:~$ johnsudo john mypasswd
johnsudo: команду не знайдено
student@student-VirtualBox:~$ sudo john mypasswd
Created directory: /root/.john
Loaded 7 password hashes with 7 different salts (crypt, generic crypt(3
) [?/64])
Press 'q' or Ctrl-C to abort, almost any other key for status
test2            (test2)
test3            (test3)
qwerty           (test1)
123456           (test5)
111111           (student)
admin            (test4)
```

Рисунок – 2.4 Використання John the Ripper для зламу паролів користувачів

В результаті дослідження можемо побачити, що усі паролі крім останнього були зламані менше ніж за 1 секунду. Натомість пароль ‘longP@assword’ не вдалося зламати за більш ніж 7 годин. Використовуючи відкрите джерело https://www.security.org/how-secure-is-my-password/ , отримуємо орієнтовний час зламу 84 тисячі років. Для порівняння, така сама комбінація без спеціального символу (‘longPassword’) буде зламана приблизно за триста років, а тільки з маленьких літер (‘longpassword’) – лише за 3 тижні.

Можна зробити висновок, що чим довший і оригінальніший пароль (більша кількість символів, використання спеціальних символів, поєднання великих і малих літер), тим складніше комп’ютеру буде його зламати.

2.3. Моделювання соціально-інженерної атаки

2.3.1 Підготовка до проведення експерименту

На базі проходження виробничої практики було отримано досвід проведення внутрішньої фішингової атаки з метою аналізу обізнаності та рівня підготовки персоналу щодо алгоритму дій у такій ситуації. З міркувань безпеки, усі домени, імена та імейли було змінено.

Політикою компанії передбачено проходження тренінгу з кібербезпеки раз на півроку – Security Workshop (далі – Тренінг). Тренінг проводиться фахівцями з кібербезпеки у форматі трьох годинної онлайн-зустрічі з лекцією та інтерактивами, в групі до 15ти людей. Без попереднього узгодження, учасникам одного з таких Тренінгів було надіслано імейл замаскований під інформацію від технічного відділу.

Уявимо що назва компанії – Space1001, відповідно домен внутрішньої комунікації – @space1001.net. Уся комунікація в середині компанії відбувається через внутрішній імейл-сервіс, кожен співробітник має адресу формату name.surname@space1001.net.

Напередодні Тренінгу, кожен з учасників отримав імейл на робочу поштову скриньку наступного змісту (дата проведення тренінгу – 25.06.2024, імейл отримано 23.06.2024):

==========

Subject: Local IT: Важливо! Опитування стосовно роботи програмного забезпечення

From: Igor Shevchenko <igor.shevchenko@space1oo1.net>

Content:

Шановні колеги!

Задля покращення перфомансу програмного забезпечення, яким користується наш Customer Support, наш відділ підготував опитування про програми, які ви використовуєте під час своєї роботи найчастіше та якості їх роботи - https://forms.space1oo1.net/software-performance-form , яке ми просимо Вас заповнити до 25.06.2024 включно.

Мета опитування - дізнатися чи задоволені ви роботою програмного забезпечення та які програми використовуєте найчастіше. Враховуючи Ваші відповіді ми зможемо краще зрозуміти теперішнє становище та спланувати наступні кроки з метою його покращення.

Ми будемо вдячні за Ваш зворотній зв'язок.

Час на заповнення опитування ~ **5 хвилин**.

Дякуємо за Ваші відповіді!

Kind regards,
Igor Shevchenko

==========

Проаналізуємо цей імейл:

З першого погляду, електронний лист виглядає цілком легально, усі працівники час від часу отримують листи подібного вмісту. Текст оформлений структуровано, відсутні граматичні та орфографічні помилки, витримано офіційний стиль листування.

Але якщо дослідити його більш детально, можна побачити ознаки фішингового імейлу:

1. Було застосовано тайпосквотинг — це форма атаки, під час якої зловмисники реєструють доменне ім'я, дуже схоже на відоме або легальне доменне ім'я. Мета — обманути користувачів, які випадково роблять друкарські помилки під час введення URL-адреси в браузері.

Як ми можемо помітити, замість офіційного домену @space1001.net було застосовано @space1oo1.net (нулі з домену було замінено на літеру «о»):

– From: Igor Shevchenko <igor.shevchenko@space1oo1.net>

– https://forms.space1oo1.net/software-performance-form

2. Крім того, що в листі витриманий офіційний стиль спілкування, притаманний для цієї компанії, в листі було застосовано ефект терміновості:

– заповнити до 25.06.2024 включно;

– Час на заповнення опитування ~ **5 хвилин**.

Таким чином, можна сказати що було застосовану потенційно досить ефективну фішингову атаку, яку доволі важко розпізнати неозброєним оком. На основі експерименту отримано такі результати (кількість учасників тренінгу – 15):

– кількість людей, що натиснули на злоякісне посилання: 5;

– кількість людей, що заповнили та відправили форму «опитування»: 2;

– кількість людей, що зарепортили про електронний лист через внутрішню систему: 1.

На основі цього можна сказати, що група учасників показала досить непоганий результати (менше 40% перейшли за посиланням та менше 15% заповнили форму опитування). В той самий час, лише одна людина відреагувала на лист та зробила репорт, що є низьким результатом.

Результати експерименту обговорили з учасниками Тренінгу. Серед тих, хто не натиснув на злоякісне посилання, 3 людини не звернули увагу на лист, оскільки опитування не є обов’язковим, а решта 6 на питання «Чому ви не зарепортили про інцидент», дали відповідь «ми думали що це зарепортить хтось інший/вже зарепортили інші».

З учасниками тренінгу провели додаткове обговорення щодо того, як можна розпізнати фішинговий лист. Також обговорили те, що важливо не лише розпізнавати соціально-інженерні атаки, а й вчасно на них реагувати та репортити інциденти відповідно до внутрішньої процедури.

2.3.2 Social Engineer Toolkit (SET)

Social Engineer Toolkit (SET) - це потужний інструмент для моделювання соціально-інженерних атак, розроблений для тестування безпеки організацій. SET був створений Девідом Кеннеді, засновником компанії TrustedSec, і є одним із найпопулярніших інструментів у сфері тестування на проникнення (penetration testing), орієнтованих на людський фактор.

Основні можливості SET [21]:

1. Моделювання соціально-інженерних атак: SET дозволяє створювати реалістичні сценарії атак, щоб оцінити стійкість організації до фішингу, вішингу та інших методів соціальної інженерії.

2. Атаки через електронну пошту: Генерація фішингових листів зі шкідливими вкладеннями або посиланнями на підроблені веб-сайти.

3. Клонування веб-сайтів: Створення копій справжніх сайтів для викрадення облікових даних (наприклад, логінів та паролів).

4. Формування шкідливих файлів: Генерація файлів з вбудованими експлойтами для отримання доступу до системи жертви.

5. Атаки на основі USB-дисків: Створення шкідливих файлів для автоматичного виконання при підключенні USB-накопичувача.

Основні модулі SET:

1. Social-Engineering Attacks (Соціально-інженерні атаки): Цей модуль дозволяє створювати різні типи атак, такі як фішинг, вішинг та інші. Він містить кілька підмодулів:

– Spear-Phishing Attack Vectors: Створення цільових фішингових кампаній.

– Website Attack Vectors: Клонування веб-сайтів і створення фальшивих сторінок входу.

– Infectious Media Generator: Створення шкідливих USB-дисків або CD/DVD.

2. Penetration Testing (Fast-Track): Цей модуль автоматизує багато процесів тестування на проникнення.

3. Third-Party Modules: Підтримка додаткових модулів, які можна інтегрувати для розширення функціоналу SET.

4. Wireless Access Point Attack: Моделювання атак на бездротові мережі.

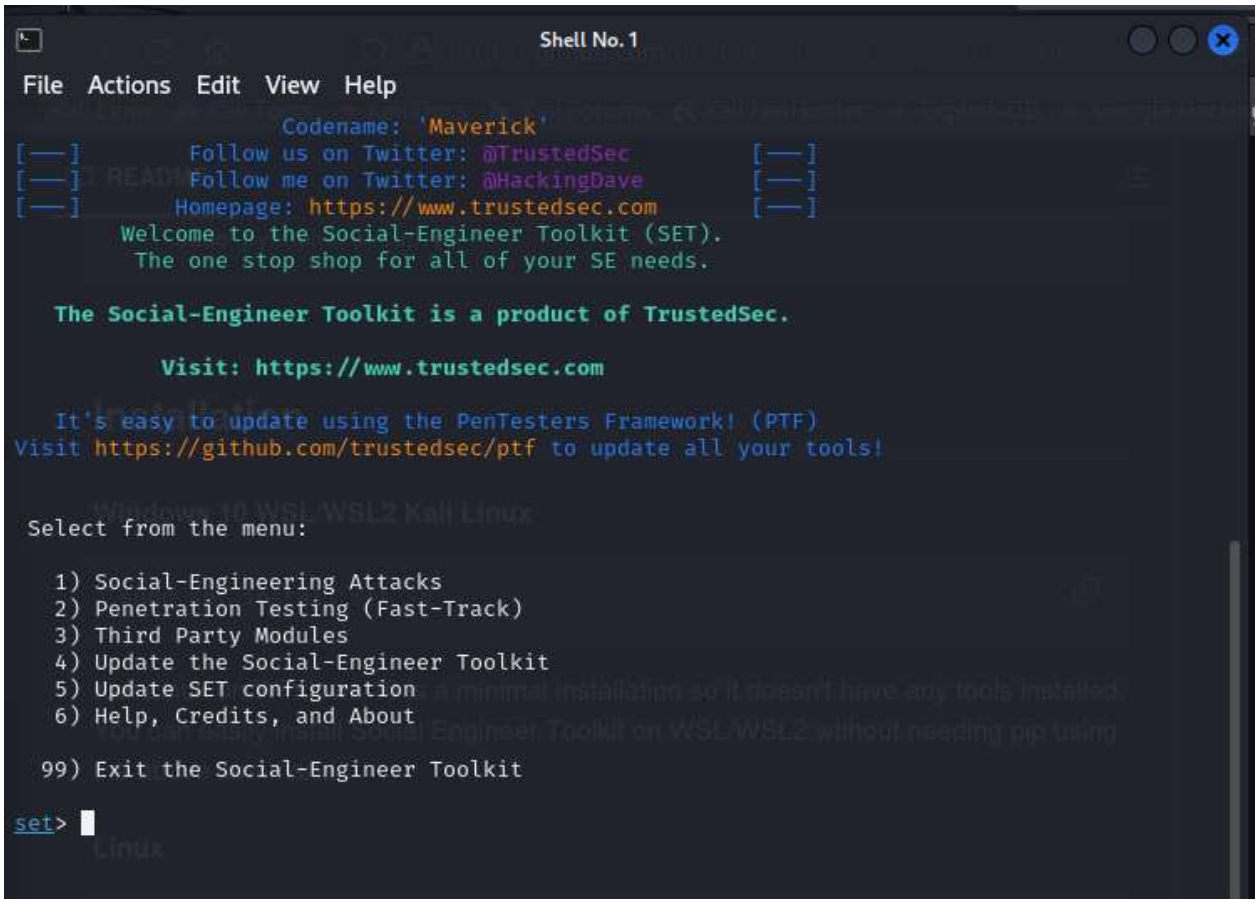


Рисунок 2.5 – Основні модулі SET

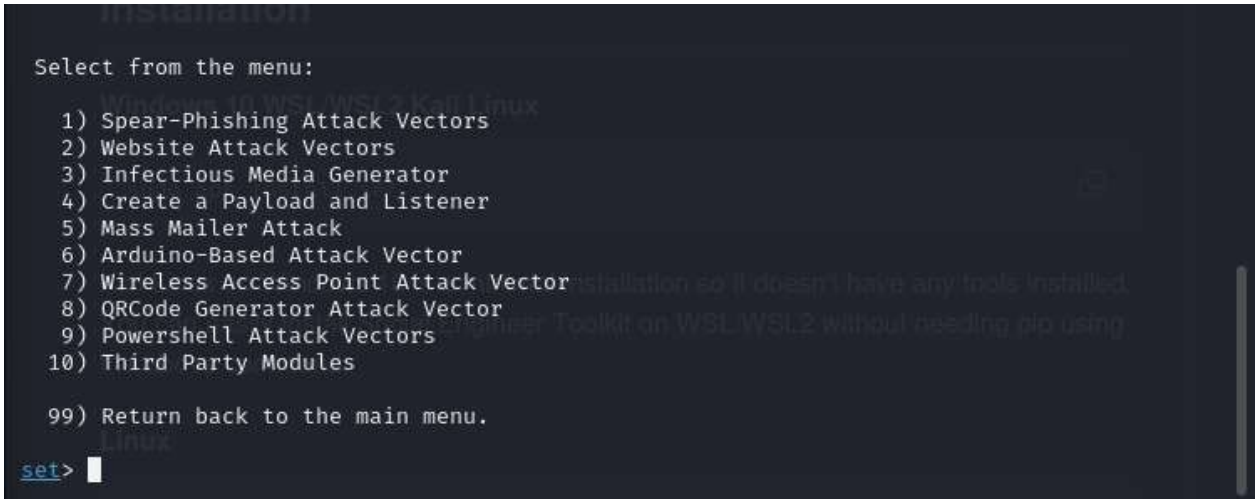


Рисунок 2.6 – Огляд модуля Social-Engineering Attacks SET

Переваги SET:

– Широкі можливості моделювання: SET підтримує багато видів соціально-інженерних атак, що дозволяє створити реалістичне тестове середовище.

– Автоматизація процесів: Інструмент автоматизує більшість завдань, що значно спрощує тестування.

– Ефективне навчання персоналу: Використання SET для створення навчальних сценаріїв допомагає виявити слабкі місця у знаннях співробітників.

Розглянемо сценарій фішингової атаки. Дії виконуються із застосуванням SET на базі віртуальної машини Kali Linux 2024.3. Використаємо модуль Social-Engineering Attacks > Mass Mailer Attack [22]:

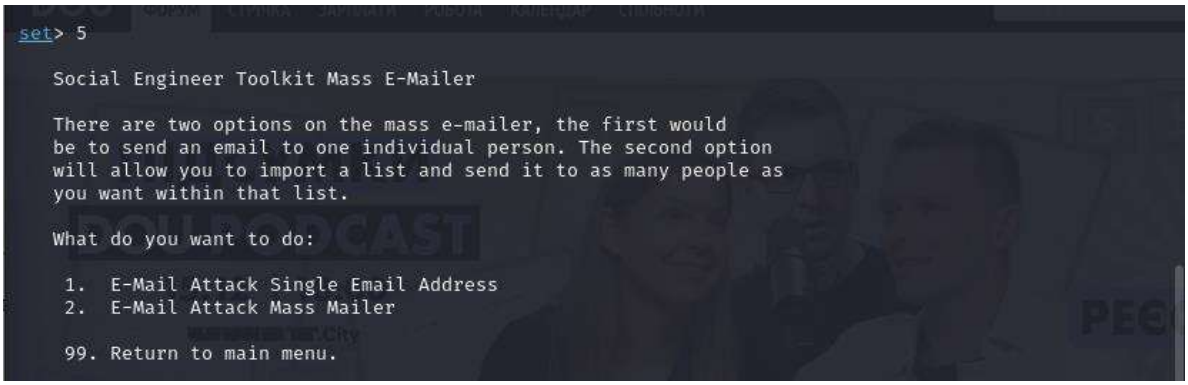


Рисунок 2.7 – Модуль Social-Engineering Attacks > Mass Mailer Attack

Використаємо опцію E-mail Attack Single Email Address. Далі програма запропонує використати готовий шаблон електронного листа або створити власний. Створимо власний одноразовий шаблон. Нам потрібно буде заповнити наступні деталі:

– Send email to: електронна адреса «цілі».

– Далможна використати власну Gmail пошту або деталі свого серверу з власним доменом. Ми використаємо власну Gmail пошту.

– Your Gmail account: електронна пошта, з якою буде надіслано лист.

– The FROM NAME the user will see: Формат імені який буде відображений у листі.

– Flag this message(s) as high priority: чи має бути імейл позначений як такий що має високий пріоритет.

– Do you want to attach a file: Чи буде прикріплений файл до листа

– Do you want to attach an inline file: Чи буде прикріплений вбудований файл до листа

– E-mail Subject: Тема листа.

– Send the message as HTML or plain text: надіслати імейл як HTML або у вигляді тексту

– Enter the body of the message: текст листа.

Заповнимо наші деталі у відповідних полях, текст листа:

==========

Hello everyone!

Please vote for our company in the annual ‘Best Company for Employing 2024’ nomination from DOU. To leave your vote, please visit this page: https://dou.ua/forums/

Hope for your cooperation. Have a great day!

Best regards,

Daryna Sh.,

Space1001 People Partner

==========

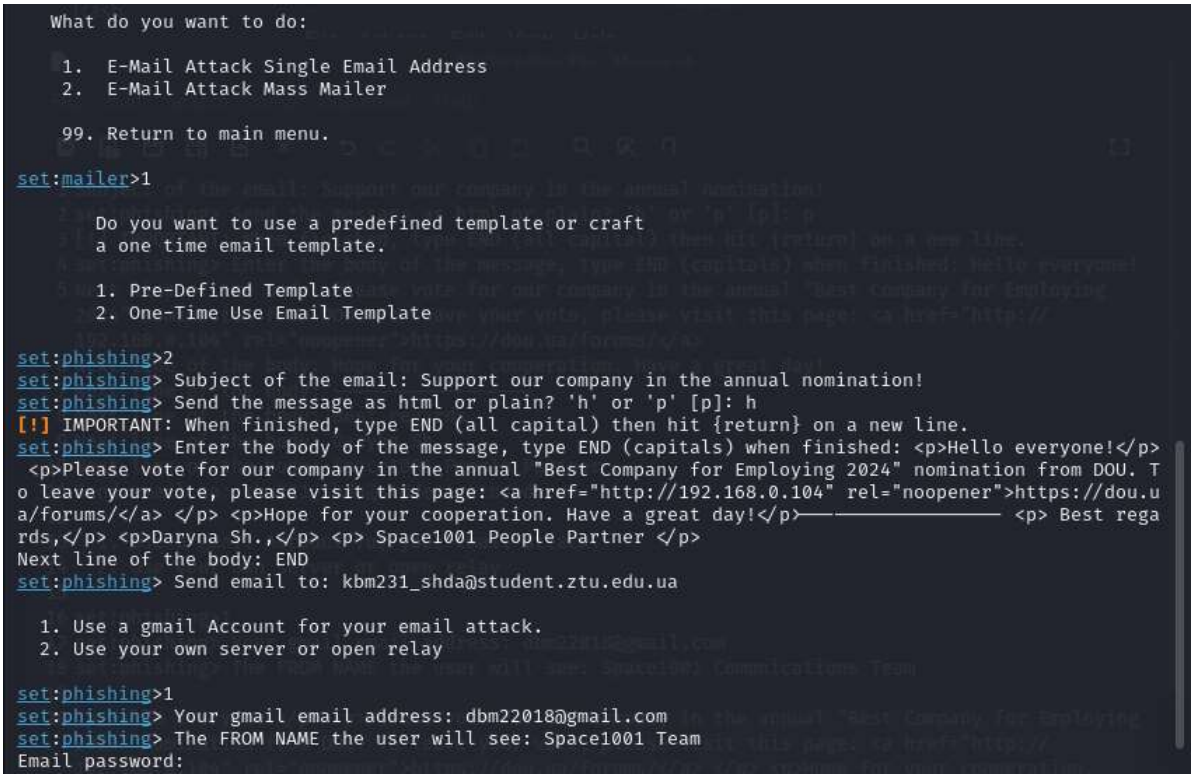


Рисунок 2.8 – Створення фішинг-імейлу за допомогою SET

В цей самий час, посилання буде замаскованим під посилання на хост зловмисника. Атаку також можна доповнити підробленою сторінкою сайту DOU.

Через нещодавні обмеження введені компанією Google, ново-створена пошта не завжди може бути використаною для такої атаки через обмеження на використання паролів для застосунків. Це зумовлене тим, що для входу в обліковий запис необхідно пройти двофакторну аутентифікацію, в той час як у Social Engineer Toolkit вхід виконується лише за допомогою паролю. Наразі, це можна було обійти шляхом налаштування паролів для окремих застосунків (що й було застосовано у продемонстрованому сценарії). Але компанія Google обмежує цей функціонал для нових акаунтів, та планує прибрати його для існуючих акаунтів [25].

Застосовані налаштування відправки електронного листа:

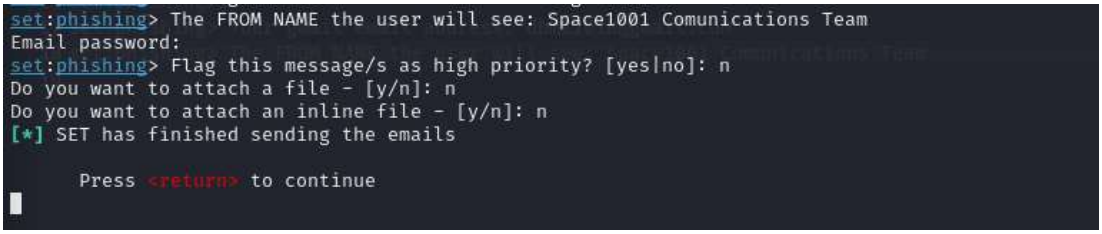


Рисунок 2.9 – Створення фішинг-імейлу за допомогою SET

Імейл отриманий користувачем:



Рисунок 2.10 – Фішинг-імейл отриманий користувачем

Вміст отриманого електронного листа:

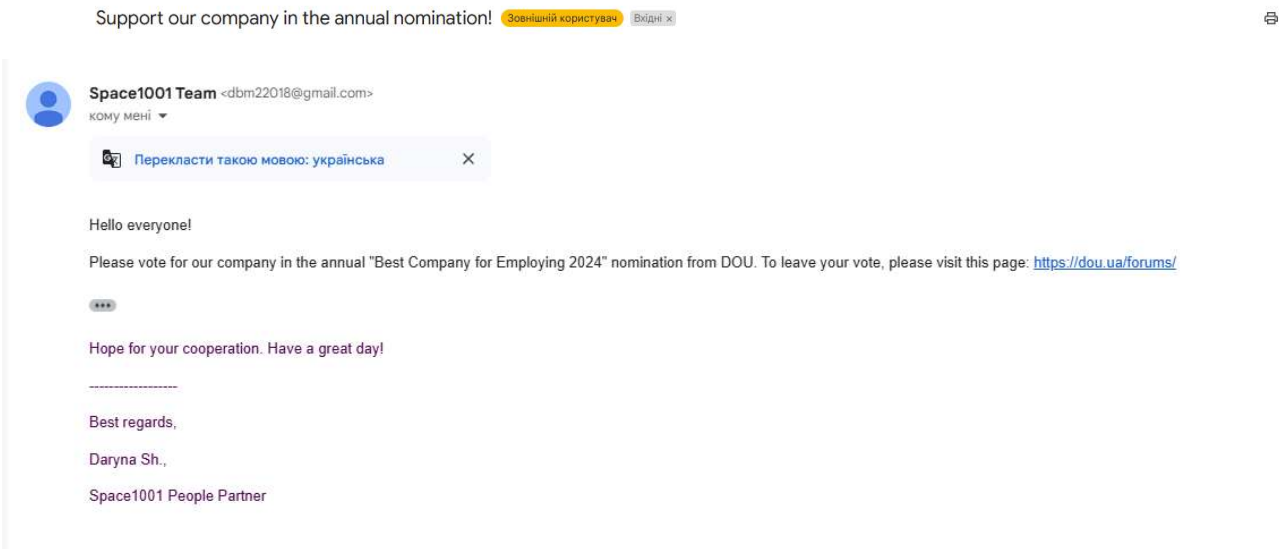


Рисунок 2.11 – Вміст фішинг-імейлу отриманого користувачем

Якщо навести курсор на посилання в листі, можна побачити що посилання насправді веде не на вказаний ресурс, а на сервер з якого було здійснено атаку:

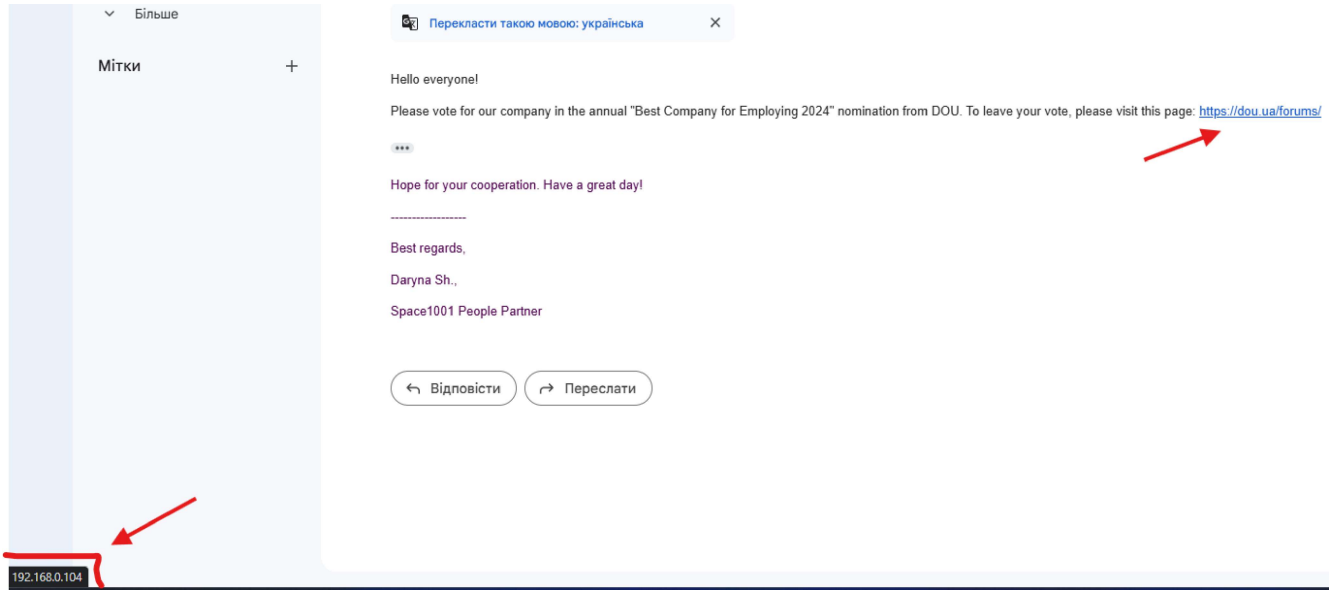


Рисунок 2.12 – Справжнє посилання у фішинг-імейлі

Таким чином, можна створювати, наприклад, фейкову логін-сторінку відомого ресурсу чи соціальної мережі. Після того як користувач введе свої деталі, вони будуть надіслані на сервер зловмисника.

Висновки до другого розділу

Отже, було коротко розглянуто основні приклади програмного забезпечення, що використовуються в соціальній інженерії; проведено моделювання фішингової атаки в середині компанії з використанням Social Engineer Toolkit; виділено основні вразливості систем безпеки пов’язаних з соціальною інженерією та їх наслідки.

РОЗДІЛ 3. РОЗРОБКА ЗАХОДІВ ЗАХИСТУ ВІД СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ

3.1. Технічні методи захисту від соціальної інженерії

3.1.1 Двофакторна аутентифікація (2FA)

Технічні заходи є першою лінією оборони проти загроз соціальної інженерії, оскільки вони створюють бар'єри, які зловмисникам важко подолати навіть за умови успішного впливу на людський фактор. У цьому підрозділі розглядаються ключові технічні рішення, які допомагають протидіяти атакам, спрямованим на обман користувачів та отримання несанкціонованого доступу до корпоративних систем [5]. Одним з таких засобів є двофакторна аутентифікація.

Двофакторна аутентифікація (2FA) — це захисний механізм, що підвищує рівень безпеки, додаючи додатковий рівень перевірки особистості користувача. У процесі аутентифікації користувач має підтвердити свою особу за допомогою двох незалежних факторів:

1. Щось, що знає користувач (наприклад, пароль або PIN-код).

2. Щось, що має користувач (наприклад, смартфон із доступом до коду), чи щось, що є частиною користувача (наприклад, відбиток пальця чи розпізнавання обличчя).

Ця комбінація ускладнює для зловмисників отримання доступу навіть у разі компрометації одного з факторів.

Основні компоненти 2FA

– Одноразові коди (OTP). Генеруються спеціальними додатками (Google Authenticator, Microsoft Authenticator [18]) або надходять через SMS. Коди мають короткий час дії, зазвичай від 30 секунд до 1 хвилини.

– Апаратні токени. Спеціальні пристрої, які генерують унікальні одноразові коди (наприклад, YubiKey [19]). Їх можна підключати до комп'ютерів або використовувати бездротово.

– Біометричні дані. Використання фізичних характеристик користувача, таких як відбитки пальців, сканування сітківки або розпізнавання обличчя [10].

– Push-сповіщення. Повідомлення на смартфон користувача, де можна підтвердити вхід одним кліком. Такі методи використовуються у мобільних додатках банків чи соціальних мереж.

Переваги використання 2FA

– Захист від крадіжки паролів. Навіть якщо зловмисник отримує пароль, йому також потрібно мати доступ до другого фактора. Це ускладнює більшість атак, таких як фішинг або перебір паролів.

– Універсальність. Двофакторну аутентифікацію можна застосовувати до широкого спектра систем: від особистих акаунтів у соціальних мережах до корпоративних платформ і фінансових інструментів.

– Простота впровадження. Багато популярних платформ, таких як Google, Microsoft, Amazon, мають вбудовану підтримку 2FA, що спрощує інтеграцію.

– Висока ефективність при низькій вартості. Впровадження 2FA вимагає мінімальних фінансових витрат, особливо якщо використовуються безкоштовні інструменти, такі як мобільні додатки для генерації OTP.

Обмеження 2FA

– Чутливість до атак на другий фактор. Наприклад, зловмисники можуть перехопити SMS-коди через слабкість мобільних мереж (SIM-свапінг).

– Проблеми з доступністю. Якщо користувач втрачає смартфон або апаратний токен, це може створити тимчасові труднощі у вході в систему.

– Залежність від інтернету. Деякі типи 2FA (наприклад, push-сповіщення) вимагають підключення до інтернету.

Реалізація 2FA в організації

1. Вибір технології:

– Програмні токени: Інструменти, що генерують OTP (Authy, Google Authenticator).

– Апаратні токени: Використання пристроїв, таких як YubiKey.

– Біометрія: Інтеграція пристроїв для сканування відбитків пальців або розпізнавання облич.

2. Інтеграція з системами:

– Налаштування 2FA на поштових сервісах (Gmail, Outlook).

– Додання двофакторного захисту до CRM-систем, ERP-систем, хмарних сервісів (AWS, Azure).

– Захист доступу до VPN для віддаленої роботи.

3. Розробка політик:

– Зобов'язати всіх співробітників використовувати 2FA для критично важливих ресурсів.

– Регламентувати використання перевірених додатків або токенів.

4. Навчання співробітників

– Проведення тренінгів із налаштування 2FA.

– Створення покрокових інструкцій із підключення 2FA до робочих акаунтів.

Одними з найпопулярніших застосунків для двофакторної аутентифікації є Google Authenticator та Microsoft Authenticator, мають такий вигляд (взято з відкритого джерела – сторінок застосунків у Google Play Store):

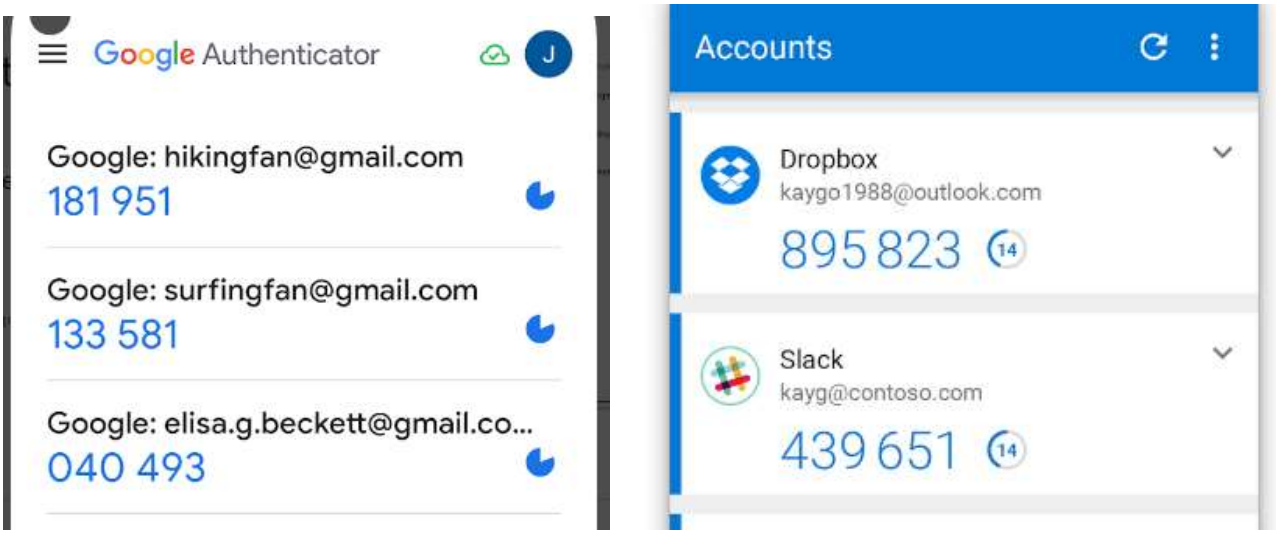


Рисунок 3.1 – Вигляд Google Authenticator та Microsoft Authenticator

3.1.2 Системи моніторингу загроз

Системи моніторингу загроз (Threat Monitoring Systems) — це комплекс програмних і апаратних засобів, які забезпечують постійне спостереження за

активністю в корпоративній мережі, аналізують зібрані дані та ідентифікують потенційно небезпечні події або аномальну поведінку. Метою таких систем є виявлення, запобігання та мінімізація впливу кіберзагроз.

Соціальна інженерія часто фокусується на людських слабкостях, але успішне проведення таких атак зазвичай залишає сліди у цифровій інфраструктурі компанії. Системи моніторингу загроз дозволяють виявляти ці сліди, аналізувати поведінку користувачів і виявляти аномальні дії, що можуть свідчити про реалізацію атаки [7].

Системи моніторингу загроз можна класифікувати за їх функціоналом, технологіями та підходами до виявлення загроз.

1. SIEM-системи (Security Information and Event Management)

Призначення: Збирають та аналізують лог-файли і події з усієї корпоративної мережі, об'єднуючи їх у єдину систему.

Особливості:

– Автоматична кореляція подій для виявлення складних загроз.

– Генерація звітів для відповідності стандартам (наприклад, PCI DSS, ISO 27001).

Приклади: Splunk, IBM QRadar, ArcSight.

2. IDS/IPS (Intrusion Detection/Prevention Systems)

IDS (Система виявлення вторгнень): Виявляє потенційні загрози, але не блокує їх.

IPS (Система запобігання вторгнень): Може автоматично зупиняти небезпечні дії.

Особливості:

– Використовують сигнатури загроз для виявлення відомих атак.

– Мають обмеження у виявленні нових або складних атак.

Приклади: Snort, Suricata, Cisco Secure IPS.

3. EDR-системи (Endpoint Detection and Response)

Призначення: Моніторинг кінцевих пристроїв (ПК, серверів, мобільних пристроїв) для виявлення загроз.

Особливості:

– Можливість аналізу дій користувачів і процесів.

– Автоматичне реагування на виявлені загрози.

Приклади: CrowdStrike Falcon, SentinelOne, Carbon Black.

4. SOC (Security Operations Center)

Призначення: Комплексний підхід, що включає інструменти моніторингу загроз і команду аналітиків для виявлення та реагування на загрози.

Особливості:

– Постійний моніторинг 24/7.

– Використання кількох технологій для зниження ризиків (SIEM, EDR, IDS/IPS).

5. Хмарні рішення для моніторингу загроз

Призначення: Забезпечують моніторинг безпеки через хмарні сервіси.

Особливості:

– Зручні для малих і середніх підприємств.

– Доступні в моделі SaaS (Software as a Service).

Приклади: Azure Sentinel, AWS GuardDuty, Google Chronicle.

Застосування систем моніторингу допомагає зменшити вплив соціальної інженерії введенням таких заходів:

– Реакція на підозрілі дії користувачів;

– Виявлення загроз у реальному часі;

– Кореляція подій;

– Попередження компрометації критичних ресурсів;

– Захист від "внутрішніх загроз".

Розглянемо детальніше кожен з аспектів:

– Реакція на підозрілі дії користувачів. Успішна атака соціальної інженерії, наприклад, фішинг, часто призводить до несанкціонованого доступу до системи або виконання нетипових дій з облікового запису жертви (завантаження файлів, зміна паролів, масове пересилання даних). Системи моніторингу загроз виявляють аномалії, такі як спроби входу з нетипових IP-адрес, велика кількість невдалих

спроб авторизації за різних акаунтів, підозрілу активність у невідповідний час, або з'єднання з незнайомими серверами.

– Виявлення загроз у реальному часі. Завдяки постійному спостереженню системи здатні миттєво реагувати на підозрілі дії. Наприклад, якщо зловмисник отримав доступ до мережі через фішингову атаку, система може автоматично заблокувати обліковий запис і попередити адміністратора.

– Кореляція подій. Більшість атак соціальної інженерії є частиною більшого ланцюга. Наприклад, успішний фішинг може призвести до впровадження шкідливого ПЗ. Системи моніторингу загроз аналізують події в різних частинах інфраструктури та виявляють взаємозв’язок між діями, який може свідчити про атаку.

– Попередження компрометації критичних ресурсів. Соціальні інженери можуть спробувати отримати доступ до конфіденційних даних компанії. За допомогою моніторингу доступу до файлів і баз даних можна оперативно виявити підозрілі спроби масового копіювання даних або зміну прав доступу.

– Захист від "внутрішніх загроз". Соціальна інженерія нерідко націлюється на співробітників компанії, які несвідомо сприяють зловмисникам. Системи можуть виявляти незвичну поведінку користувачів, навіть якщо вони діють ненавмисно.

Реалізація системи моніторингу загроз в організації

1. Оцінка потреб організації.

Перед впровадженням необхідно:

– Визначити критично важливі системи та ресурси.

– Оцінити ймовірні загрози та слабкі місця інфраструктури.

– Врахувати регуляторні вимоги (наприклад, GDPR).

2. Вибір відповідного рішення.

Вибір типу системи залежить від:

– Розміру компанії (малі організації можуть обирати хмарні рішення, великі — комплексні SIEM).

– Інфраструктури (локальна чи хмарна).

– Бюджету та доступності кадрів.

3. Інтеграція з існуючими системами

– Систему потрібно налаштувати для збору даних із серверів, мережевих пристроїв, додатків і кінцевих точок.

– Інтеграція з іншими інструментами безпеки (DLP, VPN, антивіруси).

4. Налаштування політик безпеки та автоматизації [8]

– Створення правил виявлення загроз, наприклад:

– Вхід із нетипових локацій.

– Спроби масового копіювання файлів.

– Налаштування автоматичних дій, таких як блокування IP-адрес або облікових записів.

5. Тестування та калібрування системи

– Проведення тестових сценаріїв для перевірки ефективності системи (наприклад, симуляції фішингових атак).

– Уточнення порогів для зменшення хибних спрацювань.

6. Постійний моніторинг і оновлення

– Регулярне оновлення сигнатур і алгоритмів виявлення загроз.

– Аналіз логів і звітів для виявлення нових вразливостей.

Виклики впровадження

– Хибні спрацьовування. Система може ідентифікувати легітимну активність як загрозу. Це може відволікати адміністраторів і викликати незручності для користувачів.

– Складність інтеграції. Інтеграція з наявними корпоративними системами може вимагати значних ресурсів.

– Потреба в наявності кваліфікованого персоналу. Ефективне використання систем моніторингу потребує вмінь кваліфікованих фахівців із безпеки.

3.1.3 Системи захисту від фішингу

Фішинг залишається одним із найпоширеніших методів соціальної інженерії, спрямованих на викрадення конфіденційної інформації, доступу до облікових

записів або фінансових даних. Системи захисту від фішингу поєднують технічні, організаційні, та освітні засоби, спрямовані на запобігання таким атакам.

Основні принципи роботи систем захисту від фішингу:

– Ідентифікація шкідливих елементів: Аналіз електронної пошти, веб-сайтів і файлів для виявлення ознак фішингу.

– Блокування загроз: Заборона доступу до підозрілих ресурсів або блокування повідомлень.

– Навчання та обізнаність: Підвищення обізнаності співробітників про фішингові атаки.

Реалізація системи захисту від фішингу в організації

Реалізація системи захисту від фішингу вимагає комплексного підходу, що охоплює технічні, організаційні та навчальні заходи. Нижче описано основні етапи впровадження.

1. Оцінка ризиків і потреб організації

– Аналіз існуючих загроз:

– Оцінка минулих інцидентів, пов’язаних із фішингом.

– Визначення вразливих підрозділів (наприклад, фінансового або HR-відділу).

– Аудит інфраструктури: Аналіз захищеності електронної пошти, веб-доступу та кінцевих точок.

– Розробка стратегії захисту: Визначення пріоритетів і вибір технологій відповідно до бюджету та обсягів організації.

2. Технічна реалізація

– Впровадження рішень для захисту електронної пошти:

– Налаштування систем DMARC, SPF, DKIM: Забезпечує автентифікацію відправників, що мінімізує ризик підробки електронних листів.

– Інтеграція антифішингових фільтрів: Встановлення інструментів для виявлення та блокування фішингових повідомлень.

– Використання «пісочниць» (sandbox tools): Автоматична перевірка вкладень у захищеному середовищі.

– Захист доступу до веб-ресурсів:

– DNS-фільтрація: Блокування доступу до відомих фішингових сайтів.

– Браузерні плагіни: Встановлення розширень для перевірки безпеки URL-адрес.

– SSL/TLS-захист: Гарантує шифрування даних між користувачем і веб-серверами.

– Моніторинг і виявлення загроз

– Інтеграція SIEM-систем для збору та аналізу даних про підозрілі активності.

– Використання EDR-систем для моніторингу кінцевих точок і швидкого реагування на інциденти.

– Розробка політик інформаційної безпеки:

– Заборона використання робочої електронної пошти для особистих цілей.

– Чіткі правила щодо відкриття листів і вкладень від невідомих відправників.

– Контроль доступу:

– Налаштування ролей і прав доступу до корпоративних ресурсів.

– Використання двофакторної аутентифікації (2FA).

– Регулярні перевірки: Проведення аудитів безпеки для перевірки ефективності впроваджених рішень.

3.2. Впровадження безпекових політик для протидії соціальній інженерії

3.2.1 Безпекові політики, їх види та призначення

Безпекові політики – це набір правил, процедур і керівних принципів, створених для захисту інформаційних активів організації. Вони формують основу інформаційної безпеки, визначаючи стандарти використання ресурсів, доступу до даних і реакції на інциденти [27].

Метою впровадження безпекових політик є:

– Захист конфіденційної інформації: зменшення ризику витоку даних або їх несанкціонованого використання.

– Запобігання атакам: визначення заходів для захисту від кіберзагроз і фізичних атак.

– Дотримання законодавства: забезпечення відповідності нормам і стандартам (наприклад, GDPR, ISO 27001 [26]).

– Формування культури безпеки: залучення співробітників до активної участі в захисті організації.

Виділяють декілька видів безпекових політик:

– Політики інформаційної безпеки (Information Security Policies).

– Політики фізичної безпеки (Physical Security Policies).

– Політики реагування на інциденти (Incident Response Policies).

– Політики використання ресурсів (Acceptable Use Policies).

– Політики управління ризиками (Risk Management Policies).

Розглянемо детальні кожен з видів:

1. Політики інформаційної безпеки (Information Security Policies).

Основні політики, які забезпечують загальний захист інформаційних активів. До цієї групи входять такі політики:

– Політика доступу: регламентує, хто може отримувати доступ до даних і систем.

– Політика паролів: встановлює вимоги до складності паролів, частоти їх зміни тощо.

–Політика зберігання даних: правила зберігання інформації (шифрування, резервне копіювання).

2. Політики фізичної безпеки (Physical Security Policies)

Спрямовані на захист фізичного доступу до обладнання, офісів і інших об’єктів. Включають:

– Контроль доступу до приміщень (ключі, картки доступу).

– Моніторинг за допомогою камер і сигналізацій.

– Захист серверних кімнат і критичних зон.

3. Політики реагування на інциденти (Incident Response Policies)

Регламентують дії організації під час виявлення інцидентів безпеки:

– Виявлення і класифікація інцидентів.

– Інформування відповідальних осіб.

– Аналіз і документування інциденту для майбутнього покращення політик.

4. Політики використання ресурсів (Acceptable Use Policies)

Регламентують використання ресурсів організації, таких як:

– Робочі пристрої (комп'ютери, телефони).

– Поштові сервіси та Інтернет.

– Програмне забезпечення (заборона встановлення сторонніх програм).

5. Політики управління ризиками (Risk Management Policies)

Забезпечують системний підхід до виявлення потенційних загроз, оцінки їхнього впливу і розробки заходів для їхньої мінімізації або усунення та включать в себе:

– Ідентифікацію ризиків: визначення можливих загроз для інформаційних систем, фізичних об'єктів і процесів.

– Оцінку ризиків: аналіз ймовірності реалізації загроз і їх впливу на організацію (використання методик, наприклад, FMEA або аналізу сценаріїв).

– Розробка плану управління ризиками.

– Моніторинг і перегляд: регулярний аналіз змін у ризиках, пов'язаних із новими загрозами чи технологіями.

Основними компонентами безпекових політик є:

– Цілі політики: Описують, для чого створена політика і які проблеми вона вирішує.

– Область застосування: вказують до яких співробітників, систем або процесів застосовується політика.

– Відповідальність: визначають осіб чи відділи, відповідальні за дотримання політик.

– Процедури: детальні інструкції щодо виконання конкретних завдань (наприклад, створення резервних копій).

– Контроль і аудит: включають механізми перевірки дотримання політик (регулярний аудит, звіти, моніторинг тощо).

– Санкції за порушення: визначають наслідки недотримання політик (від усних попереджень до звільнення).

3.2.2 Парольні політики як метод протидії атакам соціальної інженерії

Однією з основних проміжних цілей соціальних інженерів часто стають паролі користувачів, що дозволяють здійснити вхід до внутрішньою системи та авторизуватися як легітимний користувач цієї системи. Саме тому, впровадження парольних політик є важливим заходом протидії атак соціальної інженерії [25].

Парольні політики регулюються міжнародними стандартами [29]. Серед основних:

– ISO/IEC 27001:Системи менеджменту інформаційною безпекою.

– NIST SP 800-53: Security and Privacy Controls for Information Systems and Organizations. Контроль безпеки та конфіденційності для інформаційних систем і організацій.

– PCI DSS: Payment Card Industry Data Security Standard. Сукупність вимог щодо забезпечення безпеки даних власників платіжних карток, які зберігаються, передаються та/або обробляються в інформаційній інфраструктурі організацій.

Беручи до уваги досліджені вразливості безпекових систем на основі людського фактору, мінімізувати їх вплив можна впровадженням парольних політик з такими вимогами:

1. Довжина та складність пароля: довжина пароля має складати щонайменше 8 символів та не перевищувати 25 символів. При цьому пароль має складатися з комбінації літер різного регістру, цифр і спеціальних символів таких як <*&(^%$>!. При цьому заборонено використовувати очевидні паролі типу “qwerty”, “admin”, “password”, “11111111”, “12345678” та такі, що містять особисту інформацію користувача.

2. Процес створення паролів: необхідно уникати використання онлайн генераторів паролів в зв’язку з їх ненадійністю та невизначеністю щодо методів обробки інформації, що ввів користувач. Натомість краще використовувати генератори паролів вбудовані у парольні менеджери такі як KeePass, Bitwarden чи LastPass.

3. Термін дії та історія паролів: паролі необхідно змінювати не рідше кожні 90 днів. Заборонено повторне використання своїх останніх 5-ти паролів.

4. Обмеження на шеринг паролів: заборонено ділитись своїм паролем будь з ким, включаючи сім’ю та колег будь-якого відділу.

5. Таємні питання: для таких питань, що можуть бути частиною, наприклад, процесу скидання паролю, заборонене використання загальних питань що містять особисту публічну інформацію користувача, таку як: місце народження, клики тварин, дати народження користувача чи близьких до нього людей, уподобання тощо.

Якщо уникнути таких питань неможливо (через обмеження системи), користувач має надавати неправдиву, доступну лише йому інформацію.

6. Використання та зберігання паролів: заборонено зберігати паролі в незахищеному місці окрім як парольних менеджерів. При цьому для використання логін деталей краще використовувати автоматичну підстановку даних, доступну в парольних менеджера (наприклад за допомогою розширень для браузера). Якщо такий варіант неможливий, то необхідно копіювати дані з парольного менеджера та НЕ вводити пароль вручну.

7. Блокування облікових записів: якщо до облікового запису було виконано декілька підряд невдалих спроб аутентифікації, такий акаунт має бути тимчасово заблокований.

8. Заборонено використовувати один й той самий пароль для облікових записів на інших ресурсах – для кожного має бути свій унікальний пароль.

9. Періодично має проводитись аудит активних паролів на можливі витоки.

3.2.3 Парольні менеджери. KeePass та Bitwarden

Парольні менеджери — це програмне забезпечення або сервіси, призначені для безпечного зберігання, управління та автоматичного введення паролів у різних облікових записах користувача. Вони забезпечують централізоване місце для збереження облікових даних, які шифруються та захищаються за допомогою одного "майстер-пароля" або інших методів автентифікації (наприклад, біометрії).

Парольні менеджери є одним з методів захисту від атак соціальної інженерії оскільки дозволяють зменшити вразливості систем аутентифікацій таких як:

– Ненадійне зберігання паролів працівниками;

– Використання простих паролів;

– Використання одних й тих самих паролів для різних систем через необхідність їх запам'ятовувати.

KeePass — це безкоштовний, відкритий і потужний менеджер паролів, який зберігає паролі в локальній зашифрованій базі даних. Завдяки гнучкості, високій безпеці та відкритому вихідному коду KeePass став популярним серед технічно підкованих користувачів та організацій, які цінують повний контроль над своїми даними.

Основні характеристики KeePass:

– Відкритий вихідний код (Open Source).

– Локальне зберігання даних (база даних паролів зберігається на пристрої користувача у форматі .kdbx.).

– Шифрування AES-256, ChaCha20, Twofish що гарантує високий рівень захисту.

– Широка підтримка плагінів.

– Кросплатформність через порти (KeePass офіційно розробляється для Windows, але існують сторонні порти та додатки для macOS, Linux, Android, iOS (KeePassXC, KeePass2Android, iKeePass).

– Гнучкі налаштування.

– Вбудований генератор паролів.

– Підтримка двофакторної автентифікації (2FA).

– Резервні копії та синхронізація.

– Складне початкове налаштування що вимагає технічних навичків.

Оглянемо функціонал парольного менеджеру на практиці. Для початку, створимо нову базу даних та майстер-пароль до неї [26]:

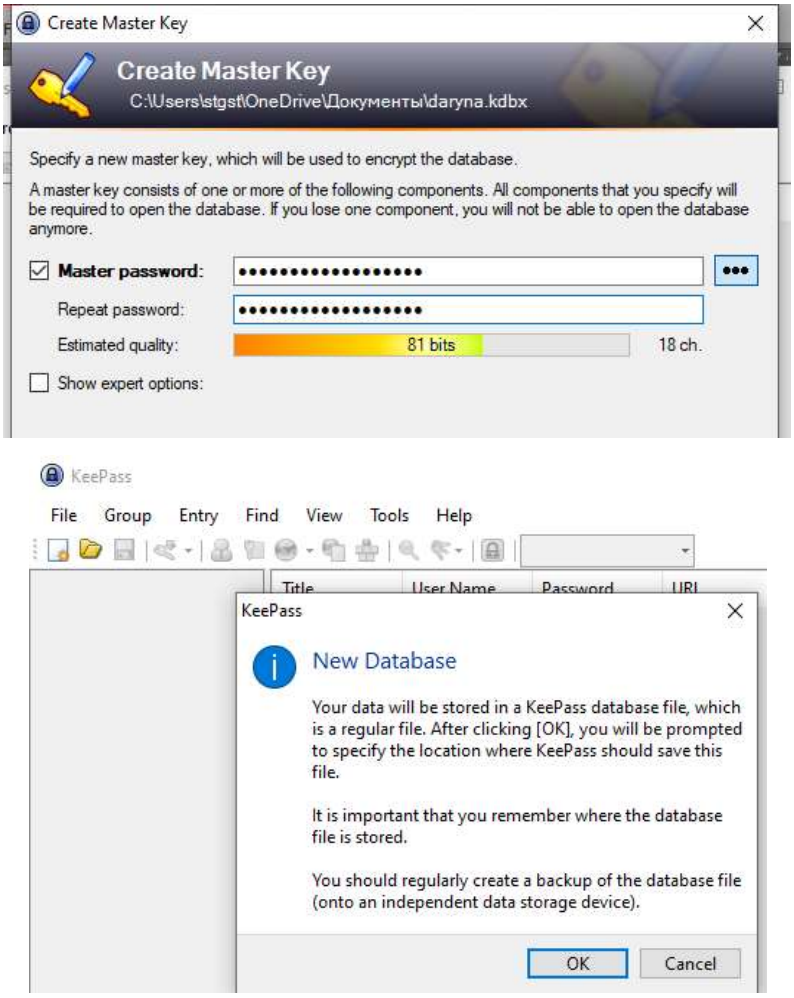


Рисунок 3.2 – Створення бази даних та майстер-паролю

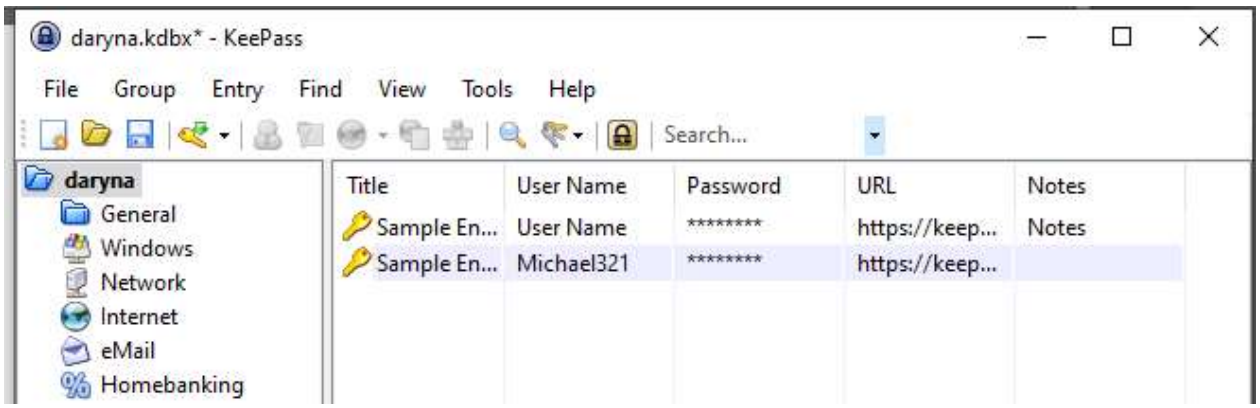


Рисунок 3.3 – Огляд основного функціоналу KeePass

KeePass надає такий основний функціонал: додавання парольних карт, створення захищених нотаток, групування парольних карт за теками.

Переглянемо процес створення парольної карти:

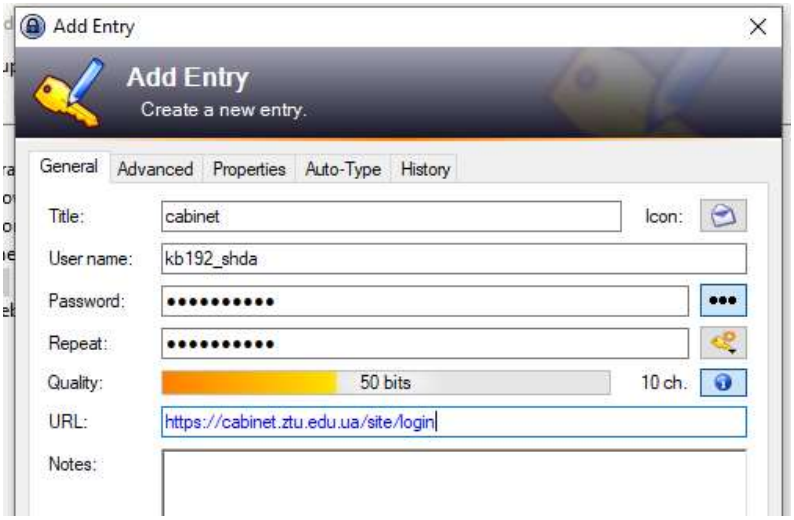


Рисунок 3.4 – Створення парольної карти в KeePass

Переглянемо налаштування безпеки:

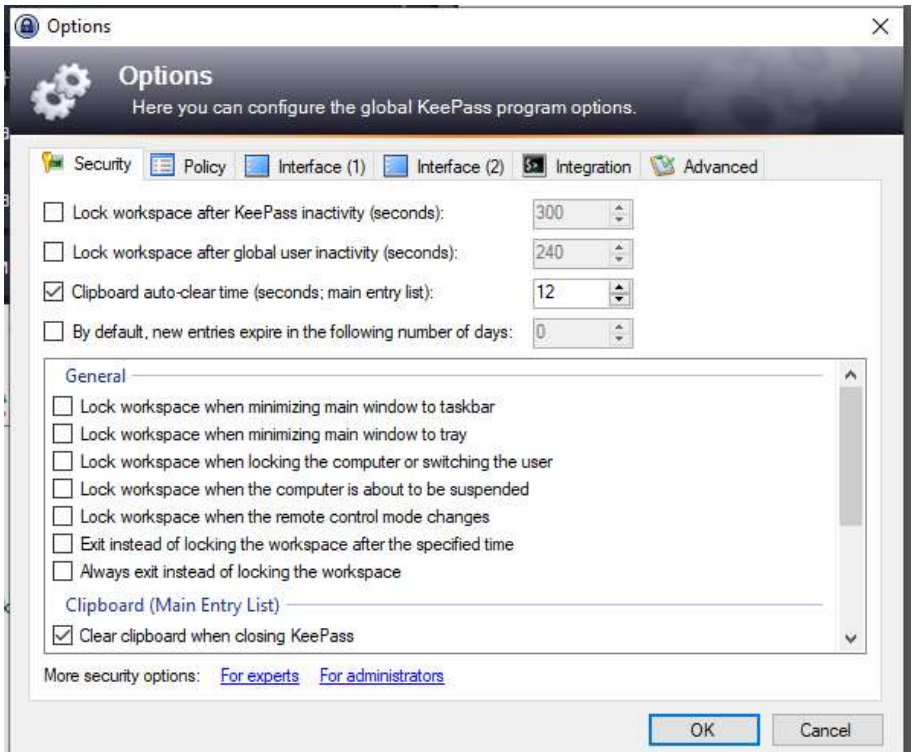


Рисунок 3.5 – Налаштування безпеки KeePass

Можемо побачити що KeePass дозволяє блокувати активне вікно, налаштувати нагадування про необхідність змінити пароль, автоматично деактивувати поточну сесію тощо. За замовчуванням, опція автозаповнення паролів на логін-сторінках відсутня та має налаштовуватись окремо за допомогою браузера «KeePassHttp» та розширення для браузеру KeePassHttp-Connector.

Завантаження плагіну відбувається з офіційного репозиторію на GitHub та встановлення з використанням команди ‘choco install keepass-keepasshttp’) [30]:

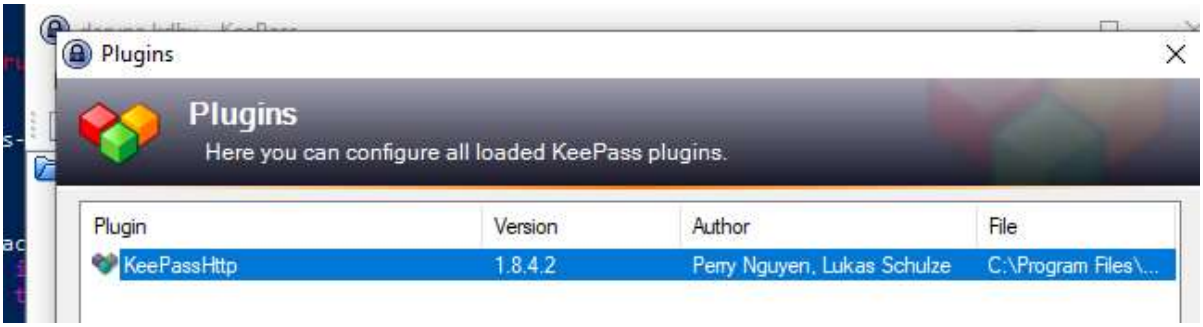


Рисунок 3.6 – Встановлення плагіну «KeePassHttp»

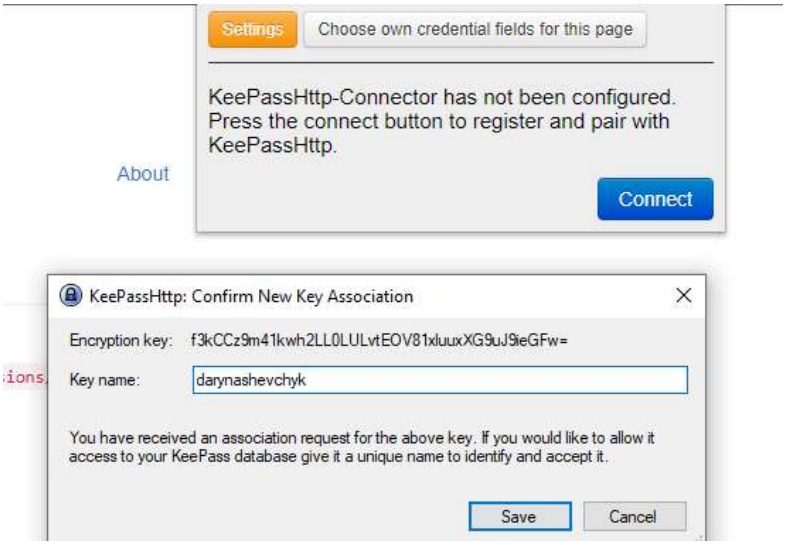


Рисунок 3.7 – З’єднання розширення для браузера з локальною базою даних паролів

Після цього, у KeePass створиться новий запис з інформацією про ключ з’єднання, а розширення для браузеру відображатиме назву ключа поточного з’єднання:

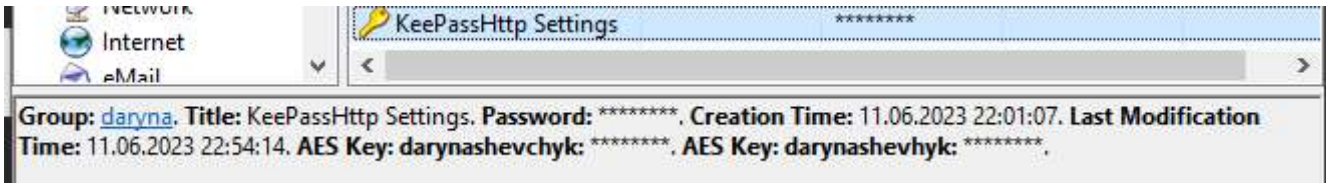


Рисунок 3.8 – Інформація про ключ з’єднання у KeePass

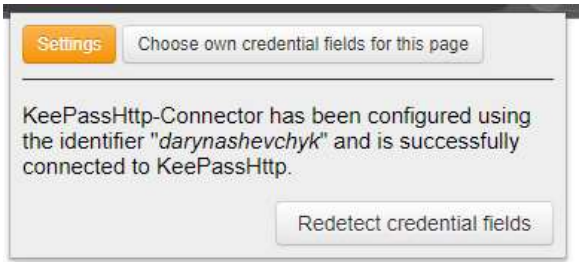


Рисунок 3.9 – Інформація про ключ з’єднання у розширенні для браузера

Після проведених налаштувань, KeePass пропонуватиме автоматичне заповнення паролів:

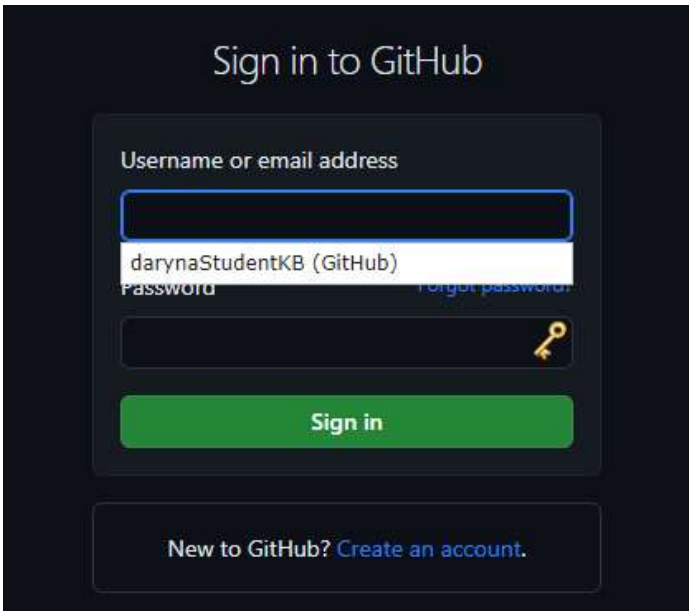


Рисунок 3.10 – Автозаповнення даних для входу

Під час такого використання, дані між застосунком та розширенням для браузера передаються з за допомогою симетричного шифрування AES у режимі CBC. Шифрування повідомлення відбувається ключем довжиною 256 біт. Якщо не проводити додаткових налаштувань, комунікація відбувається через http://localhost на порт 19455, що прослуховується розширенням.

Такий функціонал є корисним для великих компаній, оскільки це дає можливість налаштування власного серверу для створення окремих баз даних для працівників, встановивши для кожного унікальний ідентифікатор та окремий порт. Таким чином, у випадку взламу бази окремого працівника, інцидент можна локалізувати з мінімальними наслідками для інших баз. В той самий час, за умови використання «шаредних» акаунтів (наприклад створення акаунта на сторонньому ресурсі компанії партнера), оновлений пароль потрібно надсилати кожному з працівників окремо за допомогою інших ресурсів.

Bitwarden

Bitwarden — це популярний відкритий менеджер паролів, який забезпечує безпечне зберігання, управління та синхронізацію паролів між пристроями.

Завдяки прозорій моделі з відкритим вихідним кодом, Bitwarden отримав визнання як надійний і зручний інструмент для управління паролями [16].

Основні характеристики Bitwarden:

– Відкритий вихідний код (Open Source).

– Підтримка багатьох платформ (Windows, macOS, Linux, iOS, Android; розширення для браузерів Chrome, Firefox, Edge, Safari та ін.).

– Синхронізація між пристроями.

– Використання AES-256, PBKDF2 та SHA-256 для шифрування паролів. Дані розшифровуються тільки на пристрої користувача, що гарантує захист навіть у разі компрометації сервера.

– Автозаповнення паролів.

– Вбудований генератор паролів.

– Аудит безпеки паролів: Bitwarden аналізує ваші паролі, виявляє слабкі, повторювані чи ті, що потрапили в бази зламаних даних.

– Можливість хостингу: користувачі або організації можуть розміщувати Bitwarden на власних серверах для додаткового контролю над даними.

Оглянемо функціонал парольного менеджеру на практиці, а – розширення для браузера [16]:

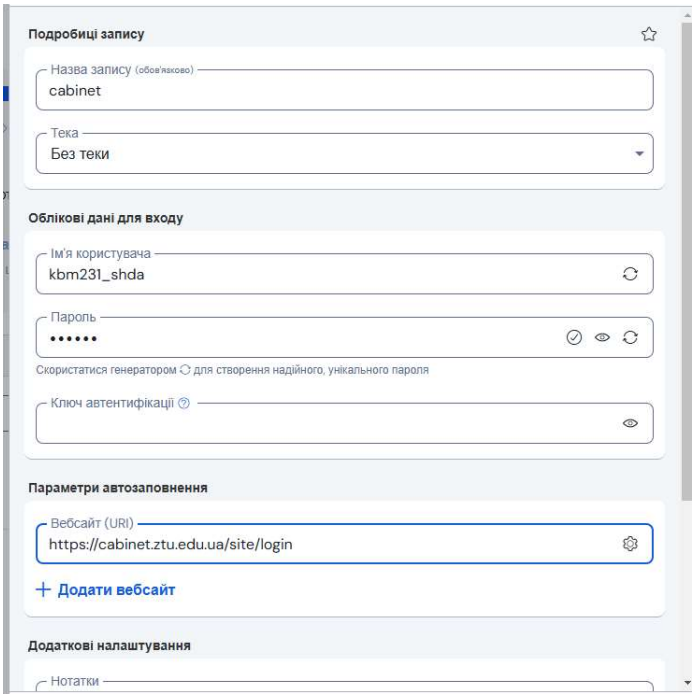


Рисунок 3.11 – Створення парольної карти вручну

Парольну карту можна створювати вручну (рис. 3.11) або зберігати дані для входу під час вдалого логіну до веб-ресурсу:

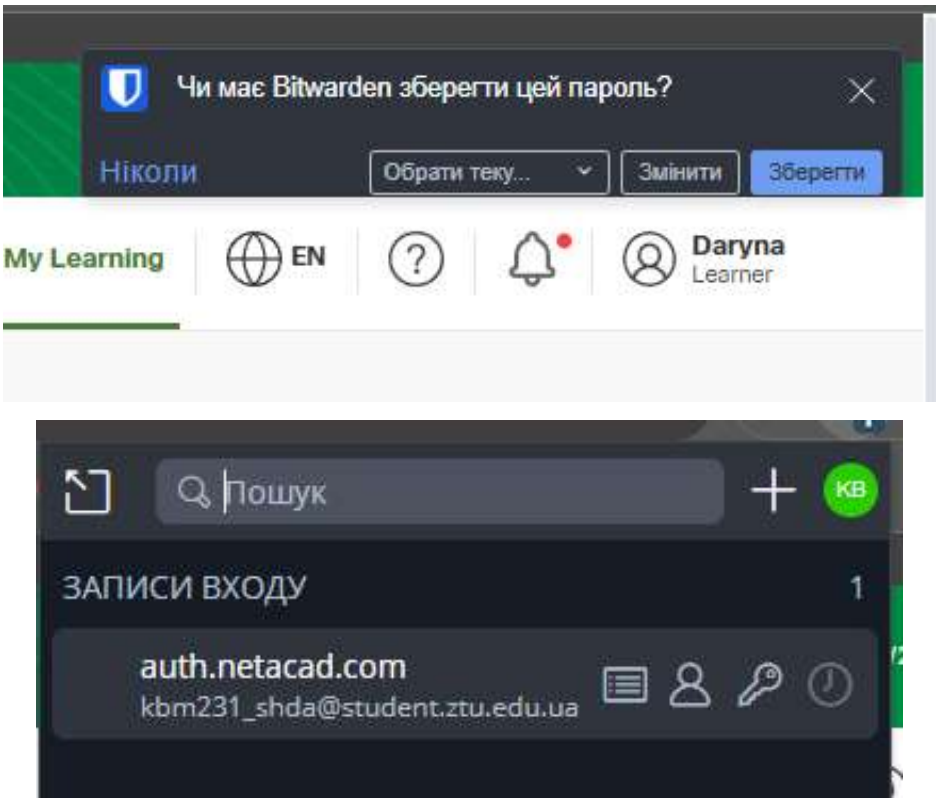


Рисунок 3.12 – Автоматичне створення парольної картки

Усі парольні картки – створені вручну чи автоматично – зберігаються локально та можуть буту згруповані за теками:

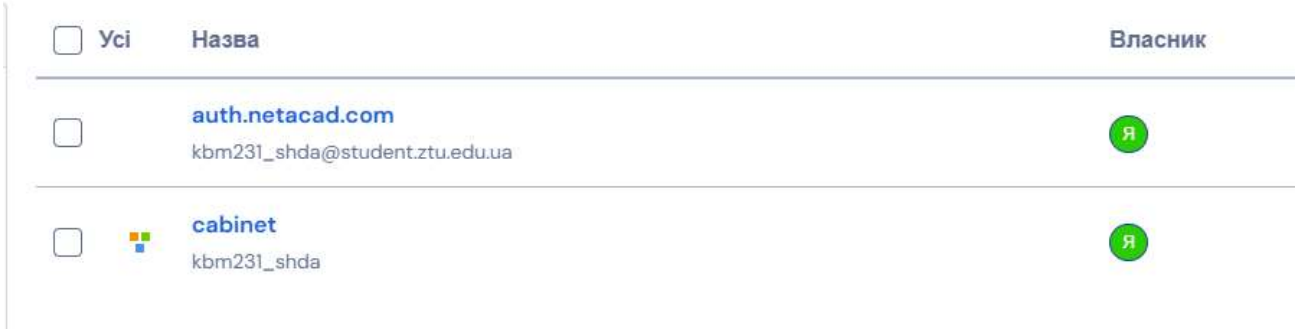


Рисунок 3.13 – Збережені парольні картки

Крім цього, Bitwarden має вбудований парольний генератор з гнучким функціоналом, що дозволяє створювати паролі та логіни з різними налаштуваннями (також вимогу можуть бути встановлені компанією). Також Bitwarden підтримує створення парольних фраз:

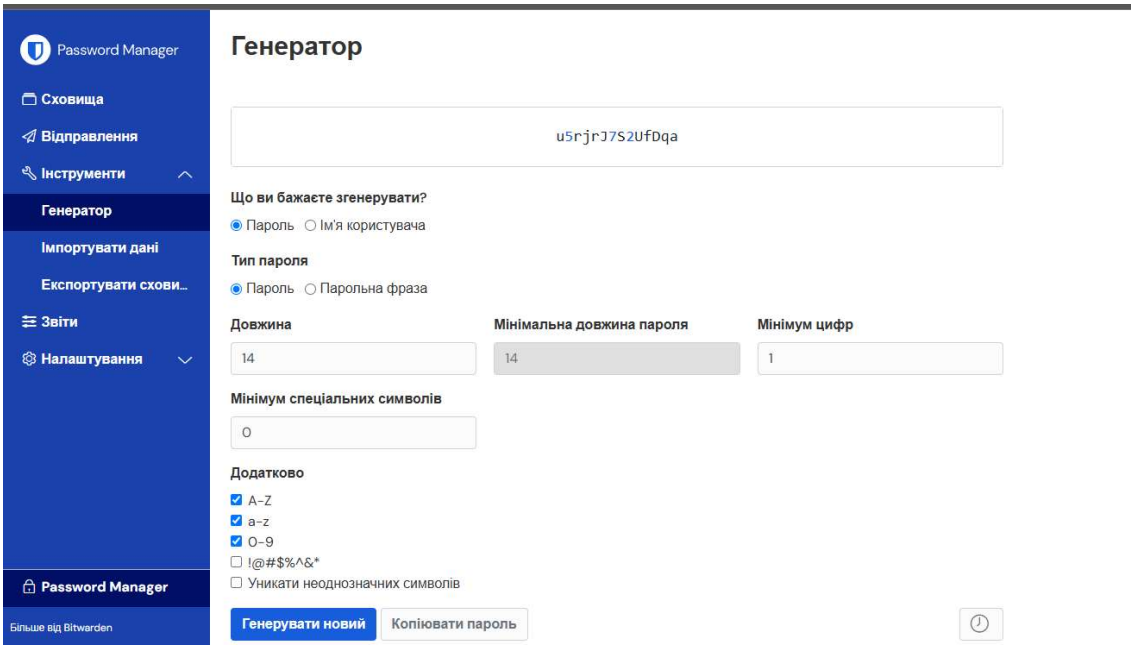


Рисунок 3.14 – Вбудований генератор паролів

Великою перевагою Bitwarden є система звітів (більшість налаштувань доступні з преміум підпискою), що значно полегшують процес аудиту паролів в середині компанії:

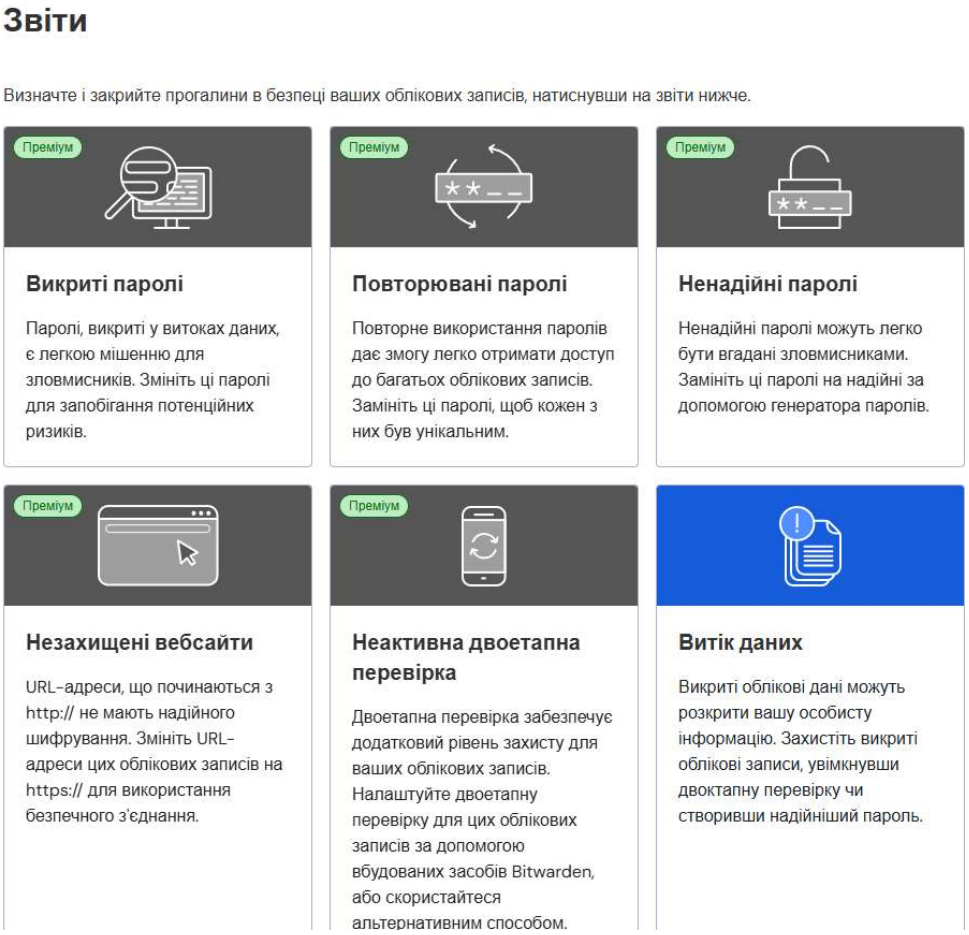


Рисунок 3.15 – Вбудовані звіти

Проведемо перевірку на витік даних (перевірка облікового запису на можливе розкриття особистої інформації):

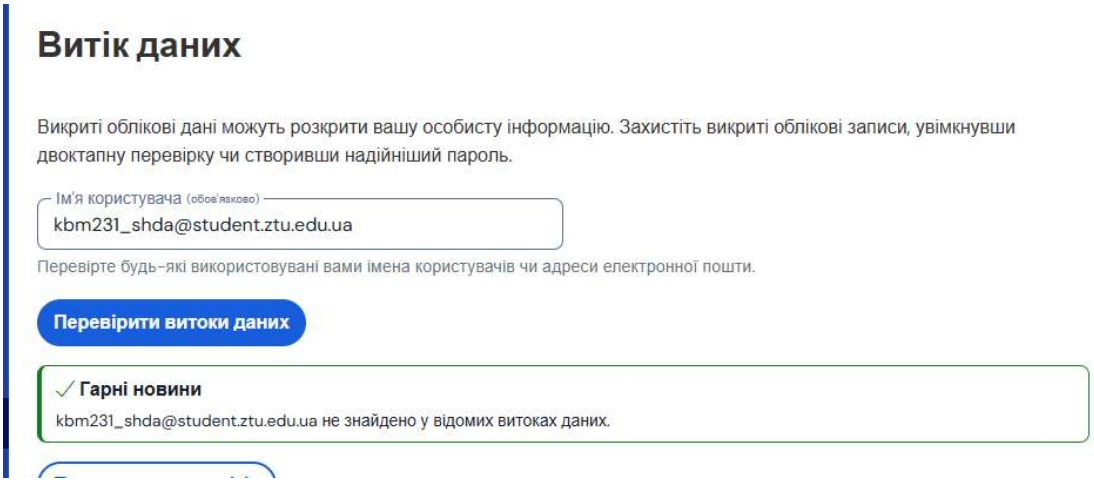


Рисунок 3.16 – Перевірка облікового запису на витік даних

Крім цього, на відміну від KeePass, Bitwarden має вбудований функціонал приєднання деталей «шаредних» акаунтів та паролів внутрішніх систем безпосередньо до акаунтів користувачів, без необхідності надсилати кожному працівнику дані вручну та змінювати парольну картку.

Якщо все ж є необхідність надіслати пароль чи секретну ноту іншому працівнику (наприклад, поділитись з технічною командою логін деталями від серверу клієнта), Bitwarden має функціонал «Відправлення». Створимо таке відправлення та розглянемо його можливості:

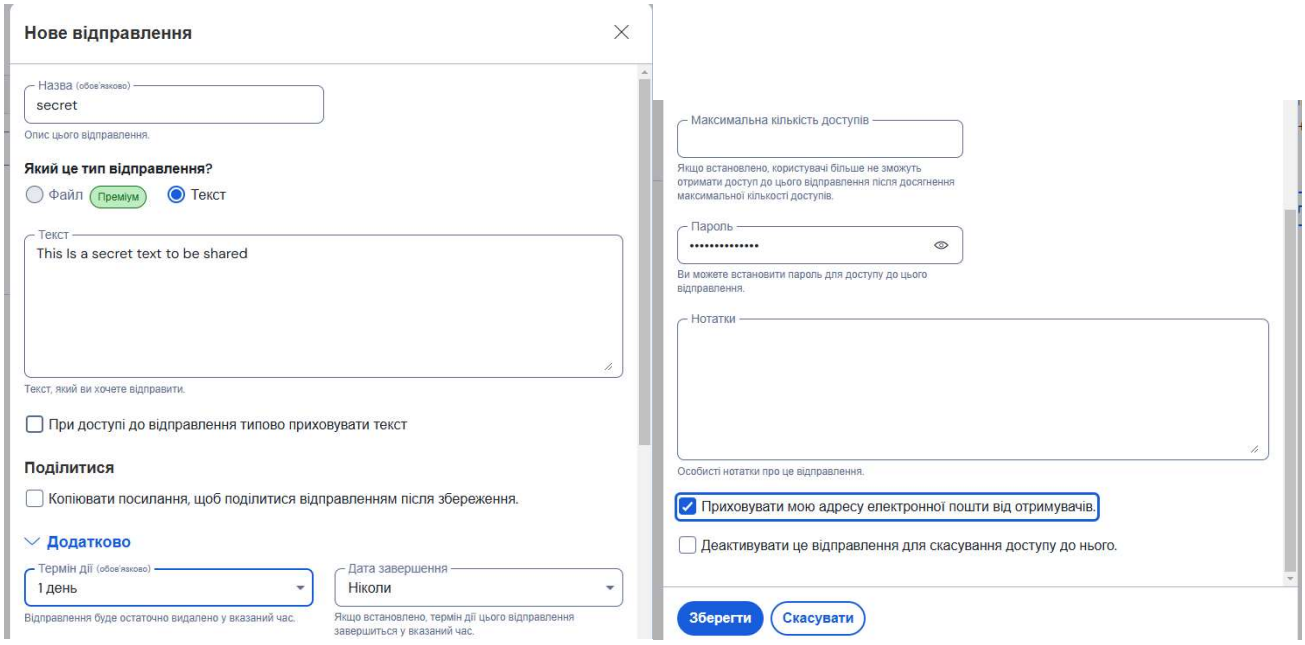


Рисунок 3.17 – Створення відправлення

Бачимо що під час створення, ми можемо ввести необхідну до відправки інформацію, встановити термін дії посилання, встановити пароль для відкриття відправлення та приховати адресу відправника для отримувача. Після створення відправлення, ми отримуємо посилання, з яким ми можемо поділитись з отримувачем. В нашому випадку, після відкриття отримувач має ввести відповідний пароль щоб відрити відправлення:

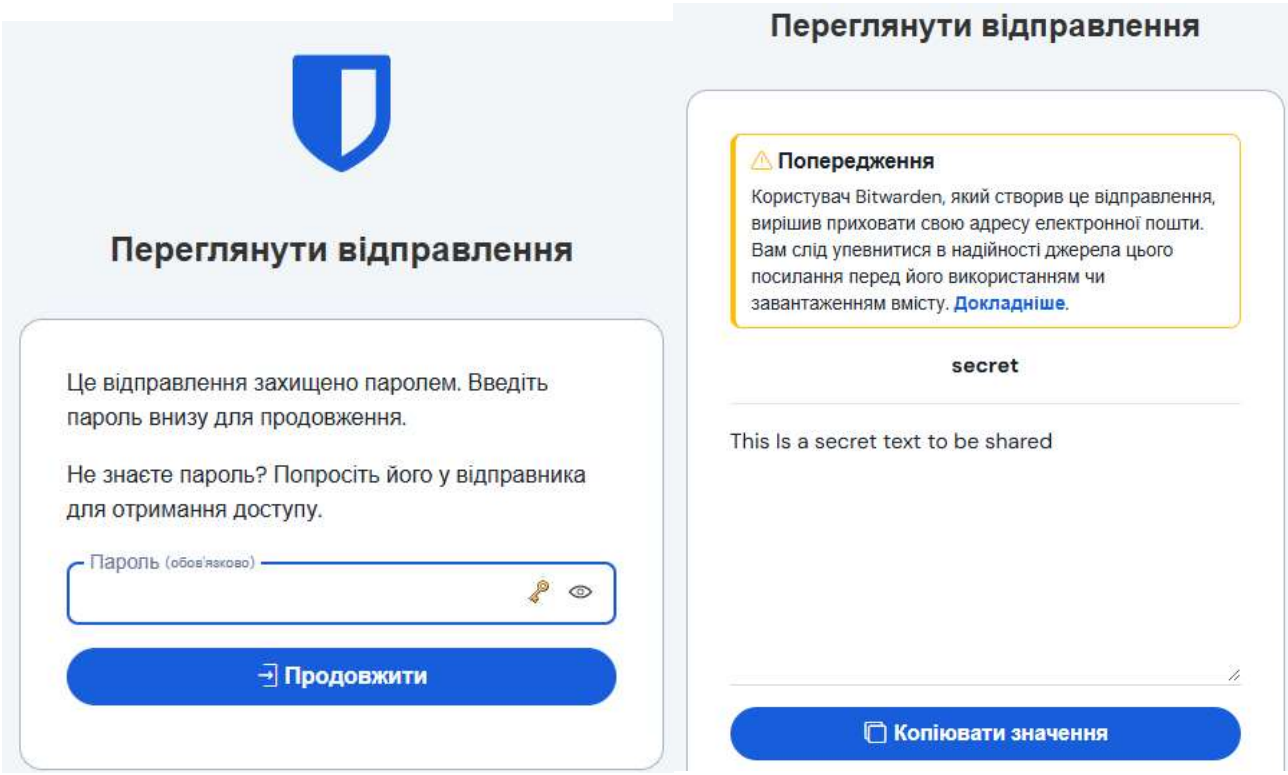


Рисунок 3.18 – Перегляд відправлення отримувачем

На основі опрацьованого матеріалу, зробимо порівняльну табличку парольних менеджерів KeePass та Bitwarden.

Таблиця 3.1 – Порівняння застосунків Bitwarden та KeePass

Характеристика	KeePass	Bitwarden
Модель поширення	Безкоштовна	Freemium: безкоштовна базова версія; платна преміум ($10/рік) та бізнес-плани.
Зберігання даних	Локально на пристрої у вигляді зашифрованого файлу бази даних.	Хмарне зберігання за замовчуванням (сервери Bitwarden), можливість самостійного хостингу.
Шифрування	AES-256, Twofish, ChaCha20.	AES-256, PBKDF2 для шифрування паролів.

Продовження таблиці 3.1

Доступність платформ	Офіційно — Windows. Сторонні порти для macOS, Linux, Android, iOS (KeePassXC, KeePass2Android).	Windows, macOS, Linux, iOS, Android, веб-інтерфейс, розширення для браузерів.
Графічний інтерфейс	Спрощений, функціональний, але виглядає застарілим.	Сучасний, інтуїтивний, зручний для користувачів.
Синхронізація між пристроями	Не підтримується за замовчуванням. Використовуються сторонні сервіси (наприклад, Dropbox, Google Drive).	Автоматична хмарна синхронізація (безкоштовно для базового плану).
Автозаповнення паролів	Підтримується через сторонні плагіни.	Підтримується у додатках та браузерах.
Генерація паролів	Гнучкий генератор з можливістю налаштування шаблонів.	Простий генератор, налаштування довжини та типу символів.
Кастомізація	Висока: безліч плагінів, можливість змінювати функціональність і шифрування бази даних.	Середня: обмежена набіром функцій програми, кастомізація через API або налаштування сервера.
Аудит паролів	Немає вбудованого аудиту, доступний через плагіни або сторонні сервіси.	Інструмент аудиту безпеки (доступний у платній версії).
Багатофакторна автентифікація	Підтримка ключових файлів, токенів, додаткових плагінів.	Підтримка 2FA (Google Authenticator, YubiKey), доступна в безкоштовній версії.
Рівень безпеки	Високий: зберігання локально, контроль шифрування, відсутність залежності від хмарних сервісів.	Високий: шифрування на стороні клієнта, але залежність від сервісів Bitwarden (окрім self-hosting).
Підтримка спільної роботи	Обмежена: поділ бази даних через сторонні сервіси.	Підтримка командної роботи та поділу паролів у платних бізнес-планах.
Зручність для новачків	Нижча через складний інтерфейс і потребу в налаштуванні.	Вища завдяки простоті, інтуїтивному дизайну та готовим рішенням.

3.3. Впровадження заходів щодо навчання персоналу

Навчання персоналу щодо соціальної інженерії є критично важливим для захисту компанії від кібератак, спрямованих на маніпуляцію співробітниками. Воно підвищує обізнаність про загрози, допомагає виявляти спроби шахрайства, знижує ризики витоку даних і фінансових втрат. Такі тренінги зміцнюють культуру безпеки в компанії, формують навички правильної реакції на інциденти та демонструють відповідальність перед клієнтами й партнерами.

Мета такого навчання: навчити співробітників виявляти спроби соціальної інженерії, розуміти ризики, які вона несе, та застосовувати ефективні методи протидії для захисту компанії та її даних.

Зміст навчальних програм відрізняється в залежності від специфіки діяльності компанії та на конкретний відділ компанії, на який таке навчання спрямоване. Основу такого навчання (для прикладу візьмемо курс) можна відокремити в такі змістові модулі:

Модуль 1. Вступ до соціальної інженерії

1. Що таке соціальна інженерія?

– Визначення поняття.

– Роль соціальної інженерії в кіберзагрозах.

– Чому людина — найслабша ланка в системі безпеки?

2. Основні методи соціальної інженерії:

– Фішинг (підроблені електронні листи, повідомлення).

– Вішинг (телефонні дзвінки з метою отримання даних).

– Смішинг (шахрайські SMS-повідомлення).

– Претекстинг (створення вигаданого сценарію для отримання довіри).

– Бейтинг (використання "приманки": USB, рекламні пропозиції).

– Tailgating (фізичний доступ до приміщення, слідуючи за працівником).

3. Приклади атак: реальні кейси атак, їх наслідки та уроки.

Модуль 2. Психологія соціальної інженерії

1. Чому люди піддаються маніпуляціям? Довіра, страх, цікавість, бажання допомогти.

2. Методи впливу:

– Використання авторитету або фальшивих повноважень.

– Створення відчуття терміновості або страху.

– Використання довіри, цікавості, бажання допомогти.

3. Як розпізнати маніпуляцію?

– Знаки, що можуть свідчити про спробу маніпуляції.

Модуль 3. Запобігання атакам

1. Як уникати фішингових атак:

– Аналіз електронних листів та повідомлень: перевірка адреси, змісту, посилань.

– Уникнення завантаження підозрілих файлів або використання невідомих пристроїв.

– Використання антифішингових інструментів.

2. Безпечна комунікація:

– Правила спілкування з незнайомими особами.

– Політика не розголошення інформації телефоном чи через SMS.

3. Робота з підозрілими об’єктами:

– Як діяти, знайшовши USB-носій або інший пристрій.

– Політика поводження з документами та паролями.

Модуль 4. Реагування на атаки

1. Що робити у разі підозри на атаку?

– Процедура повідомлення відповідального відділу.

– Аналіз потенційних втрат.

2. План дій після виявлення витоку:

– Ізоляція проблеми. Процедура репортування відповідного відділу.

– Процедура репортування відповідного відділу.

– Співпраця з ІТ-відділом та службою безпеки.

Модуль 5. Практичні вправи та симуляції

1. Фішингові тренування:

– Симуляція отримання підозрілого листа.

– Розбір помилок після вправи.

2. Аналіз кейсів:

– Робота над реальними сценаріями атак.

– Обговорення та презентація рішень.

3. Реакція в кризових ситуаціях:

– Інтерактивні вправи на швидкість прийняття рішень.

Модуль 6. Політика інформаційної безпеки в компанії

1. Правила використання корпоративних ресурсів:

– Захист облікових записів: паролі, двофакторна аутентифікація.

– Політика доступу до конфіденційних даних.

– Ознайомлення з парольною політикою.

2. Оновлення знань:

– Регулярні тренінги та оновлення процедур безпеки.

3. Роль культури безпеки в компанії:

– Вплив на репутацію та фінансовий стан компанії.

Модуль 7. Тестування та зворотний зв’язок

1. Оцінювання якості проходження курсу:

– Теоретичні запитання у формі тестування.

– Виконання практичні завдань.

2. Оцінка ефективності курсу:

– Анкетування учасників.

– Аналіз отриманих знань і їх застосування у роботі.

Очікувані результати навчання для персоналу щодо соціальної інженерії

1. Підвищення обізнаності:

– Співробітники розуміють, що таке соціальна інженерія, її основні методи та цілі.

– Знають, як зловмисники використовують психологічні методи впливу для маніпуляцій.

2. Вміння розпізнавати загрози:

– Працівники здатні ідентифікувати підозрілі електронні листи, дзвінки, повідомлення чи дії.

– Вміють помічати знаки маніпуляції, такі як тиск часу, створення термінових ситуацій чи використання авторитету.

3. Формування навичок безпечної поведінки:

– Уникання розголошення конфіденційної інформації стороннім особам.

– Дотримання корпоративних політик безпеки, включаючи використання надійних паролів, двофакторної аутентифікації та шифрування.

– Захист корпоративних пристроїв та даних у публічних місцях.

4. Ефективне реагування на інциденти:

– Знання процедур повідомлення про підозрілі дії або можливі атаки.

– Вміння мінімізувати наслідки потенційного витоку інформації.

– Участь у командних заходах для швидкого розв'язання інцидентів.

5. Покращення культури інформаційної безпеки:

– Формування звички до критичного аналізу запитів і повідомлень.

– Активне сприяння створенню безпечного середовища в компанії.

– Використання парольних менеджерів [16], в тому числі в особистому житті.

6. Зменшення ризиків для компанії:

– Зниження кількості успішних атак соціальної інженерії через підвищену обізнаність працівників.

– Захист конфіденційних даних компанії, її клієнтів та партнерів.

– Зниження фінансових втрат, викликаних кібератаками.

Варто відмітити, що таке навчання рекомендовано проводити з працівниками на початкових етапах роботи, щоб людина мала необхідну базу знань та правила поводження з внутрішніми системами, особливо якщо працівник має доступ до конфіденційної інформації та бази даних клієнтської інформації (наприклад – працівники технічної підтримки).

Попри це, необхідно періодично (1-2 рази на рік) проводити додаткове навчання з метою оновлення та актуалізації знань з урахуваннями розвитку соціальної інженерії.

Висновки до третього розділу

Отже, було коротко розглянуто технічні заходи що впроваджуються для мінімізації впливу атак соціальної інженерії, зроблено порівняльну характеристику парольних менеджерів KeePass та Bitwarden, розглянуто безпекові політики як метод протидії атакам соціальної інженерії та розглянуто аспекти впровадження навчання персоналу щодо соціальної інженерії.

ВИСНОВКИ

В результаті виконання цієї роботи було досліджено вразливості на які націлені атаки соціальної інженерії.

У першому розділі було коротко розглянуто поняття соціальної інженерії, види атак, основні методи що використовуються соціальними інженерами та методи соціального впливу на людину.

У другому розділі роботи було коротко розглянуто основні приклади програмного забезпечення, що використовуються в соціальній інженерії; проведено моделювання фішингової атаки в середині компанії; виділено основні вразливості систем безпеки пов'язаних з соціальною інженерією та їх наслідки.

У третьому розділі було коротко розглянуто технічні заходи що впроваджуються для мінімізації впливу атак соціальної інженерії, зроблено порівняльну характеристику парольних менеджерів KeePass та Bitwarden, розглянуто безпекові політики як метод протидії атакам соціальної інженерії та розглянуто аспекти впровадження навчання персоналу щодо соціальної інженерії.

Атаки соціальної інженерії є однією з найбільших загроз сучасних систем безпеки. Причиною цьому є стрімкий зріст кількості користувачів мережі Інтернет та міграцією значної частини сфер роботи компаній в онлайн-формат. Зловмисники знаходять усе більше шляхів до обману користувачів з метою заволодінням особистим даними, конфіденційною інформацією. Як результат, значна кількість компаній зазнають компрометації, підриву репутації, та фінансових втрат.

Попри це, знаючи основні вразливості на які спрямовані атаки соціальної інженерії, можна суттєво зменшити їх вплив за допомогою впровадження відповідних захисних механізмів. Серед таких:

– впровадження технічних заходів захисту таких як використання антифішингових систем, використання двофакторної аунтентифікації, використання антивірусних застосунків, постійне оновлення програмного забезпечення;

– впровадження систем моніторингу та аудиту внутрішніх систем;

– впровадження безпекових політик та регулярне навчання персоналу для підвищенні рівня обізнаності щодо розпізнавання атак соціальної інженерії та процедур реагування на такі атаки;

– використання парольних менеджерів для мінімізації вразливостей систем аутентифікацій;

– впровадження процедур поводження персоналу з файлами, якими з ними діляться колеги чи клієнти, під час роботи та поза нею тощо.

Усе це дозволяє значною мірою зменшити вплив атак соціальної інженерії на системи захисту компаній та мінімізувати негативні наслідки, що пов’язані з такими атаками.

Отже, мета кваліфікаційної роботи була досягнута.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] [Електронний ресурс] Режим доступу до ресурсу: https://phoenixnap.com/blog/social-engineering-examples

[2] Methods for Understanding and Reducing Social Engineering Attack [Електронний ресурс] Режим доступу до ресурсу: https://www.sans.org/white-papers/36972/

[3] Create a strong password & a more secure account [Електронний ресурс] Режим доступу до ресурсу: https://support.google.com/accounts/answer/32040?hl=en

[4] Vulnerability Disclosure Cheat Sheet [Електронний ресурс] Режим доступу до ресурсу: https://cheatsheetseries.owasp.org/cheatsheets/Vulnerability_Disclosure_Cheat_Sheet.html

[5] «ЗАХИСТ ІНФОРМАЦІЇ В КОМП'ЮТЕРНИХ СИСТЕМАХ ТА МЕРЕЖАХ» С.Г. СЕМЕНОВ, А.О.ПОДОРОЖНЯК, О.І.БАЛЕНКО, С.Ю.ГАВРИЛЕНКО, 2014 – 252 с.

[6] «ЗАХИСТ ІНФОРМАЦІЇ В КОМП'ЮТЕРНИХСИСТЕМАХ» В.Д. КОЗЮРА, В.О. ХОРОШКО, М.Є. ШЕЛЕСТ, Ю.М. ТКАЧ, О.О.БАЛЮНОВ, 2020 – 118 с.

[7] Ways to avoid social engineering attacks [Електронний ресурс] Режим доступу до ресурсу: https://www.kaspersky.com/resource-center/threats/how-to-avoid-social-engineering-attacks

[8] CIS Password Policy Guide [Електронний ресурс] Режим доступу до ресурсу: CIS_Benchmarks_Password_Policy_Guide_v21.12.pdf

[9] Florencio D., et al. (2007). Do Strong Web Passwords Accomplish Anything? [Електронний ресурс] Режим доступу до ресурсу: https://www.microsoft.com/en-us/research/wp-content/uploads/2016/02/tr-2007-64.pdf

[10] Grimes R. (2019, January 04). 6 reasons biometrics are bad authenticators (and 1 acceptable use) [Електронний ресурс] Режим доступу до ресурсу: https://www.csoonline.com/article/3330695/6-reasons-biometricsare-bad-authenticators-and-1-acceptable-use.html

[11] Walters, R. (2015, April 07). Insecure Passwords or Insecure People? [Електронний ресурс] Режим доступу до ресурсу: www.infosecurity-magazine.com/opinions/insecure-passwords-insecure-people/

[12] [Електронний ресурс] Режим доступу до ресурсу: https://www.openwall.com/john/doc/

[13] [Електронний ресурс] Режим доступу до ресурсу: https://www.kali.org/tools/hydra/

[14] Authentication vs. Authorization [Електронний ресурс] Режим доступу до ресурсу: https://auth0.com/docs/get-started/identity-fundamentals/authentication-and-authorization

[15] [Електронний ресурс] Режим доступу до ресурсу: https://cheatsheetseries.owasp.org/cheatsheets/Attack_Surface_Analysis_Cheat_Sheet.html

[16] [Електронний ресурс] Режим доступу до ресурсу: https://bitwarden.com/help/data-storage/#:~:text=Bitwarden%20processes%20and%20stores%20all,by%20the%20team%20at%20Microsoft.

[17] [Електронний ресурс] Режим доступу до ресурсу: https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2&hl=en

[18] [Електронний ресурс] Режим доступу до ресурсу: https://www.microsoft.com/en-us/security/mobile-authenticator-app

[19] [Електронний ресурс] Режим доступу до ресурсу: https://www.yubico.com/products/yubico-authenticator/

[20] [Електронний ресурс] Режим доступу до ресурсу: https://www.infosecinstitute.com/resources/phishing/ai-phishing-attacks/

[21] [Електронний ресурс] Режим доступу до ресурсу: https://www.stationx.net/social-engineer-toolkit/

[22] Full document on how to use SET [Електронний ресурс] Режим доступу до ресурсу: https://github.com/trustedsec/social-engineer-toolkit?tab=readme-ov-file#set-tutorial

[23] [Електронний ресурс] Режим доступу до ресурсу: https://www.maltego.com/blog/beginners-guide-to-maltego-charting-my-first-maltego-graph/

[24] [Електронний ресурс] Режим доступу до ресурсу: https://hackertarget.com/recon-ng-tutorial/

[25] Gmail Is Disabling Less Secure Apps on September 30, 2024 [Електронний ресурс] Режим доступу до ресурсу: https://wpmailsmtp.com/gmail-less-secure-apps/#Option_2_Use_an_App_Password

[26] [Електронний ресурс] Режим доступу до ресурсу: https://ztu.edu.ua/site/graduation-works-view?id=8149511

[27] Нова версія стандарту ISO/IEC 27001:2022. [Електронний ресурс] Режим доступу до ресурсу: https://ain.ua/2022/12/06/nova-versiya-standartu-iso-iec-270012022-chym-it-kompaniyam-korysnyj-czej-standart-ta-yak-jogo-vprovadyty/

[28] [Електронний ресурс] Режим доступу до ресурсу: https://www.varonis.com/blog/what-is-a-security-policy

[29] NIST Password Guidelines: 11 Rules to Follow (Latest Version Updated) [Електронний ресурс] Режим доступу до ресурсу: https://sprinto.com/blog/nist-password-guidelines/

[30] KeePass Password Safe [Електронний ресурс] Режим доступу до ресурсу: https://keepass.info/

[31] Microsoft Attack Simulator. Your First Campaign [Електронний ресурс] Режим доступу до ресурсу: https://keepass.info/