Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)
Кафедра кібербезпеки
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

бакалавр
(назва освітнього ступеня)

на тему: Використання технології OSINT для збору, узагальнення та аналізу інформації на основі різних соціальних мереж

Виконав: студент 4 курсу, групи СБ-41
спеціальності 125 Кібербезпека
(шифр і назва спеціальності)

(підпис) *Горбач М.М.* (прізвище та ініціали)

Керівник (підпис) *Деркач М.В.* (прізвище та ініціали)

Нормоконтроль (підпис) *Лобур Т.Б.* (прізвище та ініціали)

Завідувач кафедри (підпис) *Загородна Н.В.* (прізвище та ініціали)

Рецензент (підпис) *Гром'як Р.С.* (прізвище та ініціали)

Тернопіль
2023

Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)

Кафедра Кібербезпеки
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Загородна Н.В.
(підпис) (прізвище та ініціали)
«____» _____ 2023 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня Бакалавр
(назва освітнього ступеня)

за спеціальністю 125 Кібербезпека
(шифр і назва спеціальності)

Студенту Горбачу Максиму Миколайовичу
(прізвище, ім'я, по батькові)

1. Тема роботи Використання технології OSINT для збору, узагальнення та аналізу інформації на основі різних соціальних мереж

Керівник роботи к.т.н., доц. Деркач М.В.
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від «*03*» 04 2023 року № 4/7-349

2. Термін подання студентом завершеної роботи

3. Вихідні дані до роботи публічна інформація про OSINT розвідку; персональний комп'ютер; ПЗ для проведення OSINT розвідки; науково технічна література.

4. Зміст роботи (перелік питань, які потрібно розробити):

Опис використання технології OSINT
Аналіз прикладів використання OSINT
Пошук та вибір інструментів для проведення розвідки
Огляд популярних соціальний мереж
Розробка плану проведення розвідки
Створення інструменту для пошуку в соціальних мережах
Проводення OSINT розвідки за допомогою соціальних мереж
Безпека життєдіяльності, основи охорони праці
Висновки

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Безпека життєдіяльності, основи охорони праці	Пилипець М.І., доцент кафедри МТ		

7. Дата видачі завдання 04.04.2023 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1.	Ознайомлення з завданням до кваліфікаційної роботи	09.04 – 12.04	*Виконано*
2.	Підбір джерел про використання технології OSINT		
	в соціальний мережах	14.04 – 20.04	*Виконано*
3.	Опрацювання джерел про використання технології OSINT		
	в соціальний мережах	21.04 – 29.04	*Виконано*
4.	Розроблення програми і плану проведення розвідки	30.04 – 13.05	*Виконано*
	за допомогою соціальних мереж		
5.	Тестування програми і плану проведення розвідки		
	за допомогою соціальних мереж	14.05 – 20.05	*Виконано*
6.	Оформлення розділу «Аналіз використання технології		
	OSINT»	20.05 – 23.05	*Виконано*
7.	Оформлення розділу «Засоби реалізації»	23.05 – 28.05	*Виконано*
8.	Оформлення розділу «Практична реалізація»		
9.	Виконання завдання до підрозділу «Безпека	28.05 – 05.06	*Виконано*
	життєдіяльності, основи хорони праці»	05.06 – 07.06	*Виконано*
10.	Оформлення кваліфікаційної роботи	07.06 – 10.06	*Виконано*
11.	Нормоконтроль	11.06 – 14.06	*Виконано*
12.	Перевірка на плагіат	15.06 – 17.06	*Виконано*
13.	Захист кваліфікаційної роботи	20.06	

Студент _____ Горбач М.М.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Деркач М.В.
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Використання технології OSINT для збору, узагальнення та аналізу інформації на основі різних соціальних мереж. // Кваліфікаційна робота освітнього рівня «Бакалавр» // Горбач Максим Миколайович // Тернопільский національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра кібербезпеки, група СБ-41 // Тернопіль, 2023 // С. 60, рис. - 22 , табл – 0, додат. – 1, бібліогр. – 21.

Ключові слова: PYTHON, OSINT, АНАЛІЗ, СОЦІАЛЬНІ МЕРЕЖІ, ІНФОРМАЦІЯ, ВІДКРИТІ ДЖЕРЕЛА, РОЗВІДКА.

У кваліфікаційній роботі розроблено інструмент для пошуку користувачів та їх активності у соціальний мережах, а також створено і реалізовано план OSINT розвідки за допомогою соціальних мереж.

Інструмент було розроблено за допомогою мови програмування Python, За допомогою підключення API сервісу Social Searcher було створено функцію пошуку користувачів за введеною електронною адресою.

Проведення OSINT розвідки за допомогою соціальних мереж було реалізовано за допомогою соціальних мереж Facebook, Twitter, Instagram, LinkedIn, а також було використано такі інструменти, як Google Dorking, PimEyes, FaceCheck, Seon, Have I Been Pwned.

ANNOTATION

Using OSINT technology to collect, summarize and analyze information based on various social networks. // Qualification work of the educational level "Bachelor" // Horbach Maksym Mykolayovych // Ternopil Ivan Puluj National Technical University, Faculty of Computer Information Systems and Software Engineering, Cybersecurity Department, SB-41 group // Ternopil, 2023 // Pages - 60, figures - 22, tables - 0, addendump – 1, references – 21.

Keywords: PYTHON, OSINT, ANALYSIS, SOCIAL NETWORKS, INFORMATION, OPEN SOURCES, INTELLIGENCE.

In the qualification work, a tool for searching for users and their activity in social networks was developed, and an OSINT plan for social networks was created and implemented.

The tool was developed using the Python programming language. Using the API of the Social Searcher service, a user search function was created based on the entered email address.

Conducting OSINT intelligence using a social network was implemented using social networks Facebook, Twitter, Instagram, LinkedIn, and also were used tools such as Google Dorking, PimEyes, FaceCheck, Seon and Have I Been Pwned.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

OSINT – Open Source Intelligence

IP - Internet Protocol

API - Application Programming Interface

URL - Uniform Resource Locator

CSINT – Closed Source Intelligence

IT – Інформаційні технології

ЗМІСТ

ВСТУП

Сучасний стан використання та галузі застосування технології OSINT (Open Source Intelligence) ясно свідчить про її значну важливість у сфері інформаційної безпеки та розвідки. OSINT означає збір та аналіз публічно доступної інформації з використанням відкритих джерел даних, таких як соціальні мережі, веб-сайти, форуми, новинні джерела тощо.

Зараз технологія OSINT широко використовується в різних галузях. У сфері кібербезпеки вона допомагає виявляти загрози та вразливості шляхом моніторингу Інтернету на наявність інформації про потенційні атаки, зловмисні програми та інших кіберзагрози. Компанії можуть використовувати OSINT для конкурентного аналізу, це дає можливість зібрати інформацію про своїх конкурентів, включаючи дані про їх продукти, стратегію маркетингу, цінову політику, клієнтську базу та інше. Це допоможе компаніям зрозуміти ринок, ідентифікувати свої конкурентні переваги і розробити ефективні стратегії. Також таким чином вони можуть проводити моніторинг репутації. OSINT дозволяє компаніям відстежувати публічну думку про свій бренд, продукти і послуги. Вони можуть відстежувати відгуки клієнтів, коментарі в соціальних мережах, публікації у ЗМІ. Це дозволяє компаніям оперативно реагувати на негативну інформацію і забезпечувати задоволеність своїх клієнтів. Немаловажливим пунктом у використанні OSINT компаніями можна відзначити збір інформації про потенційні загрози безпеці, кібератаки, ризики та вразливості. Вони можуть відстежувати активність хакерських груп, зловживання своїми співробітниками, інформацію про вразливості програмного забезпечення та інше. Це допомагає компаніям вжити відповідних заходів безпеки та знизити ризики, адже відомо багато прикладів, де компанії дізнавались про хакерську атаку до її початку з різних форумів і інших відкритий джерел і таким чином встигали провести усі відповідні міри захисту.

У галузі розвідки та розслідувань OSINT є незамінимим інструментом для збору інформації про осіб, організації чи події. Служби безпеки, поліція та розвідувальні агентства можуть використовувати цю технологію для отримання важливих відкритих даних, які допомагають при прийнятті важливих рішень та попередженні злочинів.

Також OSINT має велике значення у сфері репутаційного менеджменту та моніторингу брендів. Компанії можуть відстежувати публічну думку про свою організацію, продукти або послуги, аналізувати відгуки та реакції клієнтів, таким чином визначати ринкові тенденції, що стосуються їх компанії для прийняття відповідних кроків для покращення свого бренду.

У наукових дослідженнях OSINT також знайшов своє використання. OSINT дозволяє дослідникам знайти і проаналізувати відкрито доступну літературу, наукові статті, тези конференцій та інші джерела інформації. Це допомагає встановити стан досліджень у певній області, ідентифікувати прогалини в знаннях і визначити потенційні напрями подальших досліджень. Також OSINT може бути використано для моніторингу новин, звітів, блогів та інших публікацій з метою отримання актуальної інформації про різні сфери науки. OSINT надає можливість використовувати відкриті дані, такі як картографічні дані, знімки з супутників, географічні теги у соціальних мережах тощо, для вивчення геопросторових явищ, наприклад, змін клімату, географічного розподілу та руху популяцій. Дослідники можуть використовувати цю інформацію для оновлення своїх знань, виявлення нових дослідницьких можливостей або стеження за розвитком конкретних тем.

Загалом, технологія OSINT має широкі застосування в сучасному світі і використовується в різних галузях, де доступ до відкритої інформації має велике значення. Використання OSINT дозволяє отримати цінні дані, які допомагають у прийнятті рішень, забезпеченні безпеки та підвищенні ефективності діяльності.

РОЗДІЛ 1. АНАЛІЗ ВИКОРИСТАННЯ ТЕХНОЛОГІЇ OSINT

1.1 Сучасний стан використання та галузі застосування технології OSINT

OSINT – це розвідувальні дані, зібрані з джерел, які є відкритими для громадськості. На відміну від більшості інших методів збору розвідувальних даних, ця форма не використовує інформацію, яка є прихованою, і, отже, не вимагає такого самого рівня скритності в процесі (хоча іноді потрібна певна скритність).

OSINT складається з різноманітних публічних джерел, таких як:

— Наукові публікації: наукові статті, публікації конференцій тощо.

— Джерела ЗМІ: газети, радіоканали, телебачення тощо.

— Веб-контент: веб-сайти, соціальні мережі тощо.

— Публічні дані: відкриті державні документи, оголошення публічних компаній тощо [1].

Деякі люди не звертають на це особливої уваги, але це знову і знову доводить свою важливість. У більшості випадків це дуже корисно для надання контексту розвідувальним даним, наданим з інших режимів, але це ще не все, у багатьох сценаріях він міг надавати розвідувальні дані, які можна безпосередньо використовувати для прийняття стратегічного рішення. На думку багатьох, якщо не більшості, це один із найпростіших і найлегших режимів, однак у нього є свої труднощі; одним із найбільших і унікальних з усіх є велика кількість даних. Там, де іншим формам розвідки не вистачає даних, OSINT має стільки даних, що найскладнішою частиною є їх фільтрація та перетворення в придатну для дії форму. OSINT вже давно використовується урядом, військовими, а також корпоративним світом, щоб стежити за конкуренцією та мати конкурентну перевагу над ними. Для OSINT існують різні публічні джерела, з яких можливо збирати розвідувальні дані, але в кваліфікаційній роботі розглядаються ті, що використовує лише Інтернет як

засіб масової інформації. Цей специфічний тип OSINT часто називають WEBINT. Може виглядати так, що, зосереджуючись на конкретному типі, втрачаємо величезну частину OSINT, що було б правильним кілька десятиліть тому, але сьогодні, коли більшість даних оцифровано, ця різниця повільно зменшується. Тому для розуміння будемо використовувати терміни WEBINT і OSINT як синоніми.

Технологія OSINT (Open Source Intelligence) здобуває все більшу популярність і використовується в різних галузях для збору, узагальнення та аналізу інформації з відкритих джерел. Її потужний потенціал виявляється у здатності надавати доступ до значної кількості даних, що можуть бути корисними для різних цілей, включаючи аналіз трендів, конкурентного середовища, репутації компаній, кібербезпеки та багато іншого.

За даними досліджень, обсяг інформації, доступної через відкриті джерела, постійно зростає. Від соціальних мереж і блогів до новинних сайтів та форумів - Інтернет просто переповнений даними, які можуть бути використані для отримання цінної інформації. Саме тому все більше організацій і фахівців використовують технологію OSINT для підтримки своїх потреб у зборі та аналізі даних [2].

Технологія OSINT знайшла застосування в різних галузях. У сфері кібербезпеки, наприклад, вона використовується для збору інформації про потенційні загрози, виявлення кібератак та моніторингу діяльності зловмисників в Інтернеті. Також OSINT може бути використана в правоохоронних органах для збору доказів, розслідування злочинів та виявлення злочинців. У сфері бізнесу технологія OSINT може бути використана для аналізу ринку, дослідження конкурентів, оцінки репутації бренду та сприяти прийняттю стратегічних рішень. Дослідження трендів у соціальних мережах та інших відкритих джерелах можуть допомогти підприємствам зрозуміти попит на продукти та послуги, прогнозувати ринкові тенденції та виявляти нові можливості. Також варто зазначити, що технологія

OSINT є важливим інструментом для журналістів та дослідників. Вона надає можливість збирати і перевіряти інформацію з різних джерел, що допомагає вести розслідування, виявляти правду та інформувати громадськість про важливі події.

Незважаючи на всі переваги, використання технології OSINT також супроводжується деякими викликами і обмеженнями. Одним з них є потреба управляти великим обсягом даних та використовувати ефективні інструменти для їх аналізу. Також важливо враховувати етичні аспекти та дотримуватися правових рамок під час збору та використання інформації з відкритих джерел.

Загалом, технологія OSINT є потужним інструментом, що відкриває безліч можливостей для збору, узагальнення та аналізу інформації з різних соціальних мереж та відкритих джерел. Вона знайшла своє застосування в різних галузях і продовжує розвиватися, стаючи невід'ємною частиною сучасного інформаційного простору.

1.2 Приклади застосування OSINT розвідки

OSINT розвідка займає окрему роль у розслідування кіберзлочинів і виявляє велику ефективність у їх розслідуванні. OSINT розвідка зіграє велику роль у знаходженні винуватців різних злочинів, для прикладу можна назвати декілька найпопулярніших випадків, а саме:

1) Один з таких прикладів - розслідування атаки WannaCry.

WannaCry була програмою вимагачем, яка поширилася у 2017 році, зашифрувавши дані на тисячах комп'ютерів у всьому світі. Розслідувачі використовували OSINT для відстеження поширення вірусу та виявлення зв'язків між злочинцями. Вони аналізували відкриті дані про доменні імена, використовані для комунікації зі зловмисниками, і знайшли ключові інформаційні сліди, що допомогли у виявленні злочинців.

2) Ще одним прикладом є розслідування атаки на Democratic National Committee (DNC) у 2016 році.

Хакерська група вкрала електронну пошту DNC та поширила скомпрометовану інформацію. Розслідувачі використовували OSINT для аналізу груп та форумів, пов'язаних з хакерством, з метою виявлення зв'язків між злочинцями та встановлення того, як вони здійснили доступ до систем DNC.

3) OSINT також використовується для виявлення кібершпигунства.

В одному з прикладів, розслідувачі виявили, що російська кібершпигунська група Fancy Bear використовувала соціальні медіа та інші відкриті джерела для збору інформації про свої цілі та здійснення кібератак. Вони аналізували відкриті джерела для виявлення зв'язків та шаблонів, що допомогли виявити діяльність цієї кібершпигунської групи. Ці приклади демонструють важливість використання OSINT розвідки в кібербезпеці. Відкриті джерела інформації надають розслідувачам цінні відомості та докази, які можуть використовуватись для ідентифікації злочинців, встановлення зв'язків між ними та розкриття їхніх методів дії. OSINT стає незамінним інструментом для розслідування кіберзлочинів та забезпечення кібербезпеки.

1.3 Методи проведення OSINT

Існує багато методів та підходів до проведення OSINT, і їх вибір залежить від конкретної ситуації та типу даних, які необхідно отримати. Ось кілька основних методів проведення OSINT:

— Використання пошукових систем: використання пошукових систем, таких як Google, Bing, Yahoo, дозволяє знайти загальну інформацію про певну особу, організацію, подію або будь-який інший об'єкт. Використовуючи правильні ключові слова та оператори пошуку, можна знайти новини, статті, блоги, форуми, соціальні медіа тощо.

— Аналіз соціальних медіа: соціальні медіа є багатим джерелом інформації. Вивчення профілів осіб або організацій у популярних соціальних мережах, таких як Facebook, Twitter, Instagram, LinkedIn, може розкрити важливі дані про їхню діяльність, зв'язки, інтереси та інше.

— Моніторинг новин та медіа: слідкування за новинами, статтями та звітами відомих новинних агентств та медіа-ресурсів може допомогти отримати інформацію про події, кібератаки, злочинну діяльність, які сталися або ще відбуваються.

— Аналіз публічних баз даних: багато організацій та установ мають публічні бази даних, які містять інформацію про компанії, осіб, статистику, правові документи тощо. Доступ до цих баз даних може надати значну кількість важливої інформації.

— Аналіз відкритих джерел геопросторової інформації: використання картографічних сервісів, таких як Google Maps, може допомогти визначити місцезнаходження об'єктів, відслідковувати подорожі, знайти фотографії або відео з конкретного місця, а також здійснити аналіз географічних зон.

— Аналіз відкритих джерел коду: виявлення відкритих кодів, які використовуються в програмному забезпеченні або на веб-сайтах, може допомогти виявити вразливості, а також встановити зв'язки між різними проектами та розробниками.

Це лише кілька прикладів методів проведення OSINT. Комбінування різних методів та використання спеціалізованих інструментів може значно полегшити процес збору та аналізу інформації з відкритих джерел.

1.4 Постановка завдання

Мета кваліфікаційної роботи: розробка та імплементація інструменту для збору, узагальнення та аналізу інформації на основі різних соціальних

мереж з використанням технології OSINT, а також створення плану та проведення розвідки.

Об’єкт розробки: технології збору, узагальнення та аналізу даних з соціальних мереж з використанням технології OSINT.

Предмет розробки: дані, що розміщуються в соціальних мережах.

Для отримання поставленої мети, необхідно виконати низку наступних *задач:*

— провести аналіз технологій та інструментів, які працюють з застосування технології OSINT;

— провести пошук соціальний мереж, в яких надається можливість збору даних користувачів;

— реалізувати збір і аналіз даних за допомогою соціальних мереж;

— оцінити якість реалізованого пошуку.

Розроблений інструмент і план може бути використаний дослідниками, аналітиками, журналістами та іншими зацікавленими особами для проведення OSINT розвідки в соціальних мережах. Він дозволяє збирати, узагальнювати та аналізувати інформацію з різних джерел, що сприяє покращенню роботи з великим обсягом даних та забезпеченню більш точних та об'єктивних результатів аналізу.

Висновки до першого розділу

В першому розділі проведено загальний аналіз використання технології OSINT і досліджено його поточний стан і галузі застосування. Виявлено, що OSINT набуває все більшої популярності і широко використовується в різних сферах для збору, узагальнення та аналізу інформації з відкритих джерел. Використання OSINT може мати значний вплив на розвідку, бізнес-аналітику, кібербезпеку та інші сфери.

Було проаналізовано і описано, як OSINT застосовується в реальних ситуаціях. Наведено приклади успішного використання OSINT у кіберрозвідці компаній, де збір та аналіз відкритої інформації допомагав виявити загрози, виявити конкурентів та здійснити стратегічні рішення.

Також розглянуто основні методи, які використовуються в OSINT. Виявилося, що комбінація різних методів, таких як пошук в Інтернеті, аналіз соціальних мереж, перегляд публічної інформації та використання спеціалізованих інструментів, може значно полегшити процес збору та аналізу інформації. Використання цих методів дозволяє отримати глибоке розуміння ситуації і зробити обґрунтовані висновки на основі зібраної інформації.

Також в розділі визначено мету, об’єкт, предмет та основні задачі розробки.

РОЗДІЛ 2 ЗАСОБИ РЕАЛІЗАЦІЇ

2.1 Популярні інструменти технології OSINT

В сучасному світі соціальні мережі є незмінною складовою нашого повсякденного життя. Інформація, яку люди публікують у соціальних мережах, створює великий обсяг відкритих даних, які можуть бути використані для здійснення різних аналітичних та розвідувальних дій. Відкритий збір і аналіз інформації з соціальних мереж, відомий як OSINT, стає все більш важливим інструментом для отримання цінної інформації, яка може використовуватись в різних сферах, включаючи безпеку, розвідку, маркетинг та багато інших. Для OSINT розвідки важливо вибрати діючі інструменти, які проводять коректний пошук і дають якнайменше зайвої інформації, саме тому можна розглянути такі інструменти:

1) Maltego є потужним фреймворком OSINT, який дозволяє збирати, візуалізувати та аналізувати інформацію з різних джерел. Він дозволяє створювати графічні зображення, які відображають зв'язки між різними сутностями, такими як особи, організації, місцезнаходження та інші. Maltego може бути використаний для збору інформації з соціальних мереж, таких як LinkedIn, Facebook, Twitter, і допомагає розкривати зв'язки між користувачами та їх діяльністю.

2) Seon.io. Основні можливості SEON.io включають аналіз IP-адрес, перевірку електронних адрес, виявлення шаблонів шахрайської діяльності, аналіз ризиків, антифрод-рішення для операцій з платіжними картками, виявлення фальшивих акаунтів та багато іншого. Крім того, SEON.io надає можливість безкоштовно проводити пошуки з повним функціоналом при реєстрації нового користувача протягом 14 днів в повному обсязі.

3) PimEyes - це онлайн-інструмент для пошуку та виявлення зображень людей в Інтернеті. Використовуючи потужний алгоритм розпізнавання обличь, PimEyes дозволяє знайти подібні або ідентичні

фотографії, які містяться у веб-середовищі. PimEyes надає можливість виявити використання фотографій в Інтернеті без дозволу. Цей інструмент корисний для захисту приватності та контролю за використанням особистих зображень в мережі. Він може бути корисним для фотографів, блогерів, журналістів, а також для будь-кого, хто хоче відстежувати поширення зображень в Інтернеті. Інтерфейс PimEyes є простим і інтуїтивно зрозумілим. Користувач може завантажити фотографію або ввести URL-адресу зображення для пошуку. Після обробки запиту, PimEyes відображає результати, включаючи подібні або ідентичні зображення, де воно було знайдено та в яких контекстах воно використовувалося. Користувач може переглянути знайдені зображення і перейти до веб-сторінок, де вони були виявлені.

4) Shodan є спеціалізованою пошуковою системою, яка сканує Інтернет для виявлення підключених пристроїв. Він дозволяє отримувати інформацію про промислові системи, IoT-пристрої, веб-камери та багато іншого. Shodan може бути використаний для знаходження вразливих пристроїв або виконання аналізу інфраструктури, що може бути цінною для розвідувальних цілей.

5) Google Dorking. "Dork" - це пошуковий рядок, який використовує розширені оператори для знаходження відповідного результату [3]. Google Dorking використовує особливі пошукові запити для виявлення цікавої інформації, яка зазвичай не відображається в звичайних пошукових результатах. Використання спеціальних параметрів та операторів дозволяє знаходити конфіденційну інформацію, витоки даних, вразливості та інше. Google Dorking може бути використаний для пошуку важливих даних, які можуть бути корисними для OSINT-розвідки.

Кожен з цих інструментів має свої унікальні можливості та спеціалізовані функції, які можна використовувати для збору, аналізу та використання інформації з соціальних мереж. Їх комбінація в OSINT-інструменті може допомогти отримати точні і дійсні результати пошуку.

2.2 Робота з соціальними мережами

Кожна соціальна мережа надає унікальний доступ до інформації та функціональності, що дозволяє отримати різноманітні дані з різних джерел. Комбінація даних з різних соціальних мереж дозволяє отримати комплексну картину про об'єкт розвідки, збагачуючи інформацію та забезпечуючи більш точний аналіз. Крім того, вибір конкретних соціальних мереж для використання в OSINT-інструменті залежить від цілей і потреб. Кожна мережа має свою унікальну аудиторію, спрямованість та типи даних, які можна зібрати [4].

Соціальні мережі, такі як Reddit, LinkedIn, Instagram, Facebook та Twitter, є важливими джерелами інформації для проведення OSINT розвідки. Використання їх API дозволяє автоматизувати процес збору та аналізу даних. Це одні із найпопулярніших соцмереж, з яких є можливість зібрати велику кількість інформації про її користувачів, саме тому воно чудово підходять для збору інформації за певними критеріями. Також для наочності наведена різна статистика щодо відвідування і кількості активних користувачів на цих платформах, щоб показати їх актуальність [5].

2.2.1 Reddit

Reddit - це онлайн-платформа, де користувачі можуть ділитися контентом, спілкуватися та обговорювати різні теми. Вона створена у вигляді веб-сайту з багатим функціоналом, що дозволяє користувачам створювати підписки на конкретні тематичні "сабреддіти" (або просто "саби"), що є підрозділами платформи, присвяченими певним темам.

Reddit може бути корисною в OSINT розвідці з кількох причин:

— Інформаційні джерела: Reddit є великою спільнотою користувачів, яка активно обговорює різні теми. У різних сабреддітах можна знайти багато цінної інформації та досвіду, які можуть бути важливими для розвідки.

Наприклад, в сабреддіті, присвяченому кібербезпеці, можуть з'являтися повідомлення про нові загрози або вразливості, які можуть бути корисними для подальшого аналізу.

— Пошук свідків та інформаторів: Reddit може слугувати платформою для знаходження свідків подій або осіб, які мають доступ до певної інформації. Користувачі можуть розміщувати повідомлення про події, свідчення або запити на інформацію. Це може бути корисною можливістю для збору свідчень і знаходження джерел інформації з першоджерел.

— Аналіз громадської думки: Reddit є місцем, де люди вільно висловлюють свої думки та обговорюють різні питання. Аналіз громадської думки на певну тему може допомогти отримати інсайти, оцінити настрої, тенденції або реакції людей на певні події. Це може бути корисним для вивчення суспільно-політичних питань, дослідження думок і установок груп людей.

— Відстеження інформаційних потоків: Reddit може слугувати зручним інструментом для відстеження та моніторингу новин, трендів або подій у реальному часі. З підпискою на певні сабреддіти або використовуючи функцію пошуку, можна отримати доступ до широкого спектру інформації та оновлення з різних джерел та перевіряти їх автентичність.

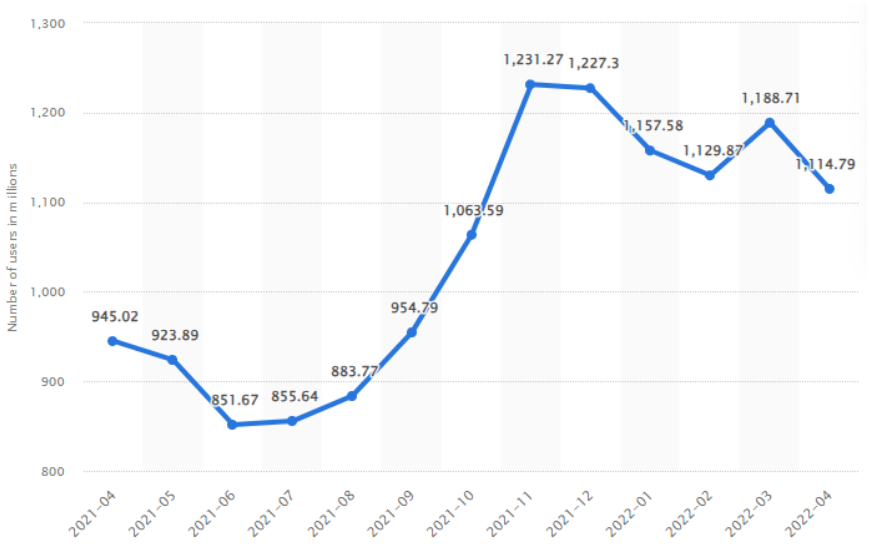


Рисунок 2.1 - Користувачі, які відвідували Reddit згідно з statista.com [6]

Звичайно, важливо зауважити, що інформація, отримана з Reddit, повинна бути перевірена та підтверджена в інших джерелах, оскільки вона базується на відкритих джерелах інформації та висловлюваннях користувачів, які можуть бути піддаються маніпуляції чи спотворенню. З рисунку 2.1 видно, що кількість активних користувачів платформи Reddit активно зростає.

2.2.2 LinkedIn

LinkedIn - це соціальна мережа, спеціалізована на професійних зв'язках та спілкуванні між фахівцями з різних галузей. Ця платформа дозволяє користувачам створювати профілі, в яких вони можуть представити свої професійні досягнення, досвід роботи, навички та освіту.

LinkedIn може бути корисною в OSINT розвідці з кількох причин:

— Професійна інформація: користувачі LinkedIn активно розміщують свої профілі, де вони подають детальну інформацію про свої професійні навички, робочі місця, освіту та інші важливі дані. Ця інформація може бути цінною для отримання даних про певну особу або компанію, їхні професійні зв'язки та експертизу.

— Зв'язки та мережа професійних контактів: LinkedIn дозволяє збирати інформацію про зв'язки між людьми та їхні професійні контакти. Це може допомогти виявити залежності, спільні проекти або партнерство між різними особами та компаніями.

— Робочі вакансії та рекрутинг: LinkedIn є популярною платформою для пошуку роботи, розміщення вакансій та професійного рекрутингу. Це означає, що на платформі можна знайти інформацію про робочі місця, здібності, навички та інші професійні деталі про різні організації та особи.

— Обговорення та спілкування: LinkedIn також надає можливість обговорювати професійні теми, приєднуватися до груп і спілкуватися з іншими фахівцями. Це може бути корисною можливістю для збору думок,

відгуків та інсайтів щодо конкретних сфер діяльності або професійних проблем.

Важливо пам'ятати, що LinkedIn є платформою, де користувачі самостійно розміщують інформацію про себе, тому необхідно перевіряти достовірність інформації та підтверджувати її в інших джерелах, особливо при використанні її в розвідці або іншій професійній діяльності. З рисунку 2.2 видно статистику та відповідно до неї прогноз активних користувачів LinkedIn.

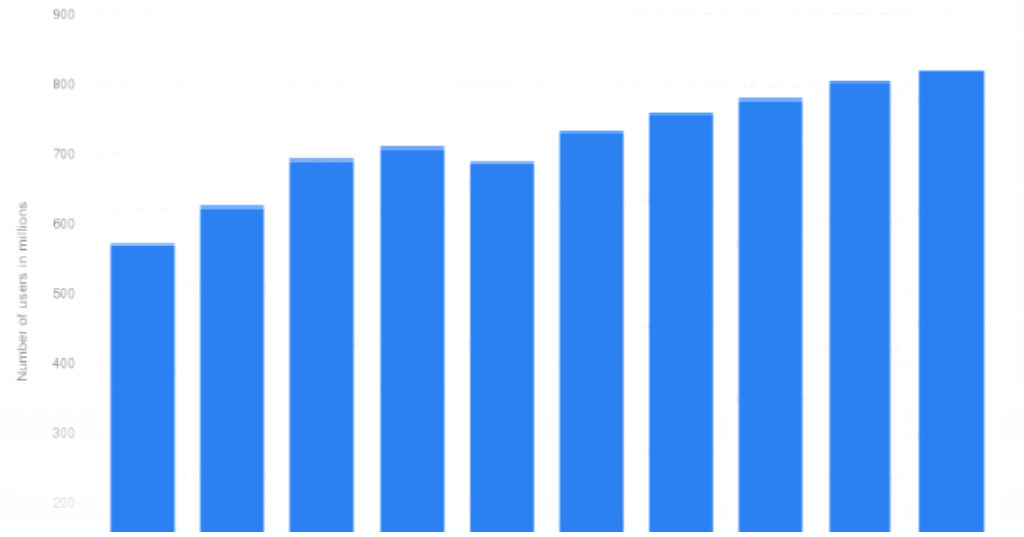


Рисунок 2.2 – Статистика та прогноз користувачів згідно з statista.com [7]

2.2.3 Instagram

Instagram - це популярна соціальна мережа, яка спеціалізується на обміні фотографіями та відео. Користувачі можуть створювати свої профілі, розміщувати зображення та відео, створювати сторіс (Stories) та обговорювати контент із своїми підписниками.

Instagram може бути корисною в OSINT розвідці з кількох причин:

— Візуальна інформація: Instagram є платформою, де користувачі активно діляться фотографіями та відео зі свого повсякденного життя, подорожей, подій та інших цікавих моментів. Це надає можливість отримати

візуальну інформацію про людей, місця, події або предмети, що може бути корисним для розвідки.

— Геолокація: Instagram дозволяє користувачам вказувати геолокацію своїх дописів, фотографій та історій. Це може допомогти визначити місце знаходження певної особи або події. Наприклад, вивчаючи геотеги або використовуючи інструменти пошуку за місцем, можна встановити, де знаходиться певна компанія, ресторан, пам'ятка чи інше місце інтересу.

— Інформація про інтереси та активності: Instagram дозволяє користувачам вказувати свої інтереси, використовувати хештеги, взаємодіяти зі спільнотою та обговорювати певні теми. Це може допомогти отримати уявлення про інтереси та активності конкретної особи або групи людей, що може бути важливим для розвідки та аналізу їхніх дій.

— Взаємодія з іншими користувачами: Instagram надає можливість взаємодіяти з іншими користувачами шляхом коментування, відмічання, підписки та приватного повідомлення. Це може стати корисним для встановлення зв'язків з потенційними джерелами інформації або знаходження інших осіб, пов'язаних з досліджуваними темами.

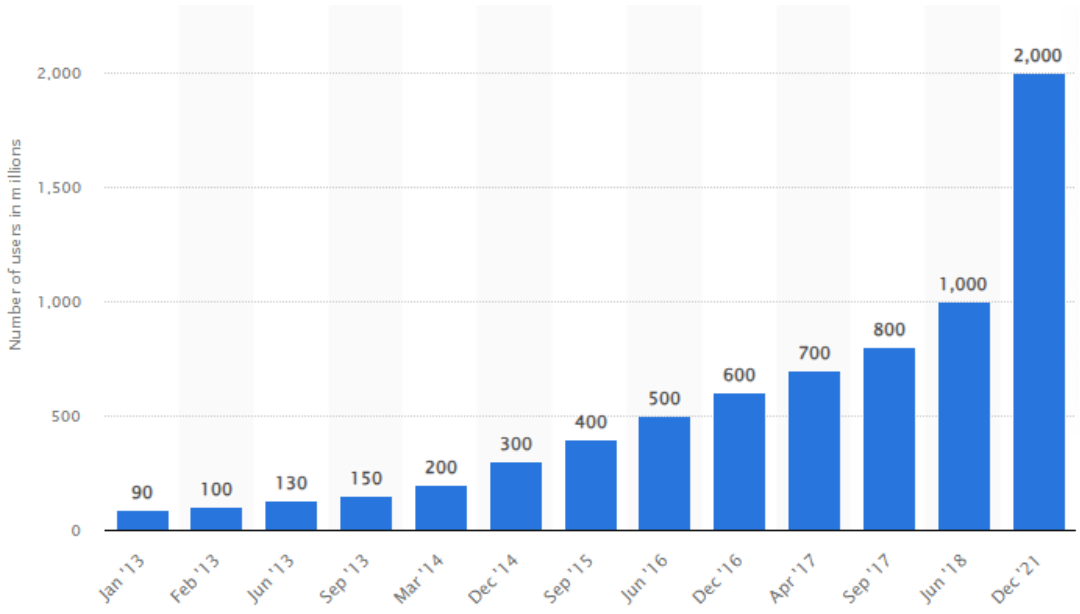


Рисунок 2.3 – Кількість активних користувачів Instagram згідно з statista.com [8]

Важливо враховувати, що Instagram - це особиста платформа, і доступ до багатьох функцій та інформації може бути обмеженим залежно від налаштувань конфіденційності користувачів. При використанні інформації з Instagram у розвідці необхідно дотримуватись етичних принципів та правил конфіденційності. З рисунку 2.3 видно зростаючу тенденцію активних користувачів Instagram.

2.2.4 Facebook

Facebook - це найпопулярніша соціальна мережа, яка дозволяє користувачам спілкуватися зі своїми друзями, родичами, колегами та іншими людьми з усього світу. Платформа надає можливість створювати особисті профілі, розміщувати повідомлення, фотографії та відео, приєднуватися до груп та сторінок, а також спілкуватися через приватні повідомлення.

Facebook може бути корисною в OSINT розвідці з кількох причин:

— Особиста інформація: користувачі Facebook розміщують в своїх профілях особисту інформацію, таку як місце проживання, освіта, робота, інтереси, статус стосунків тощо. Ця інформація може бути використана для отримання деталей про конкретну особу, її зв'язки, інтереси та ставлення до різних питань.

— Фотографії та відео: Facebook дозволяє користувачам завантажувати свої фотографії та відео, які можуть містити цінну візуальну інформацію. Це може стосуватися як особистих фотографій, де можуть бути виявлені люди, місця або події, так і фотографій з громадських подій, акцій, конференцій тощо.

— Групи та сторінки: на Facebook існують тисячі груп та сторінок, які об'єднують людей за спільними інтересами, хобі, професійними галузями та багатьма іншими темами. Досліджуючи такі групи та сторінки, можна

отримати інформацію про активності, думки та дії групи людей, що може бути корисною в розвідці.

— Взаємодія та комунікація: Facebook надає засоби для взаємодії та комунікації з іншими користувачами через коментарі, відмітки, приватні повідомлення тощо. Це може стати корисним для встановлення зв'язків з особами, виявлення залежностей та отримання додаткової інформації про конкретну особу чи групу людей.

Важливо зазначити, що Facebook має різні налаштування конфіденційності, і доступ до інформації може бути обмеженим залежно від налаштувань користувачів. Також потрібно дотримуватись етичних принципів та правил при використанні інформації з Facebook у розвідці та аналізі. З рисунку 2.4 видно стрімко зростаючу тенденцію активних користувачів мережі.

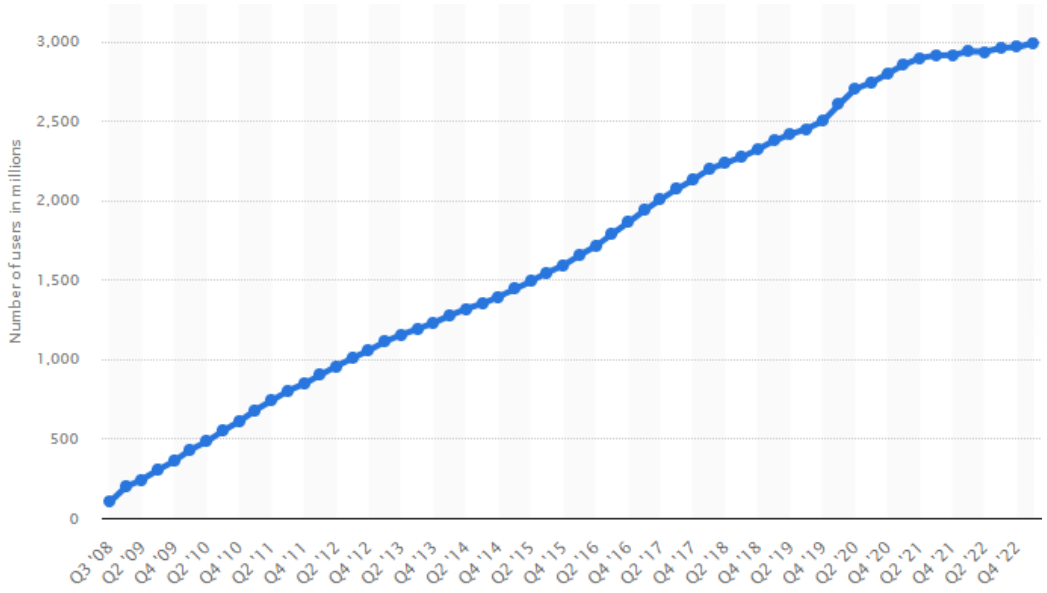


Рисунок 2.4 – Активні користувачі Facebook згідно з statista.com [9]

2.2.5 Twitter

Twitter - це соціальна мережа, яка дозволяє користувачам розміщувати повідомлення (твіти) обмеженої довжини (280 символів), які можуть включати

тексти, посилання, фотографії та відео. Користувачі можуть створювати свої профілі, підписуватися на інших користувачів, а також взаємодіяти з їхніми твітами шляхом лайків, ретвітів та коментарів.

Twitter може бути корисною в OSINT розвідці з кількох причин:

— Публічна інформація: Twitter є публічною платформою, де користувачі активно висловлюють свої думки, коментують події, розміщують новини та іншу інформацію. Твіти можуть містити цінну інформацію про події, тренди, погляди людей та інші важливі аспекти, що можуть бути використані для розвідки та аналізу.

— Теги та хештеги: Twitter використовує теги та хештеги для класифікації твітів та об'єднання пов'язаної інформації. Це дозволяє знайти та відстежувати тематичні обговорення, події, групи людей чи конкретні ключові слова, що може бути корисним для виявлення трендів, публічної думки та залучення до відповідних груп або спілкоти.

— Мережа взаємодії: Twitter дозволяє підписуватися на користувачів, створювати мережу зв'язків та взаємодіяти з ними шляхом коментарів, ретвітів та приватних повідомлень. Це може допомогти встановити зв'язки зі спеціалістами, експертами чи іншими особами, які мають цінну інформацію або відносяться до досліджуваної теми.

— Інформація про активності та настрої: Twitter дозволяє відстежувати активності користувачів, їхні настрої, ставлення до певних питань та подій. Це може бути важливою інформацією для виявлення трендів, аналізу громадської думки та оцінки ставлення до певної теми або події.

Варто пам'ятати, що Twitter є швидкозмінною платформою з великим потоком інформації, і це може бути викликом при зборі та аналізі даних. Важливо використовувати належні інструменти та методи для фільтрації, класифікації та відслідковування інформації з Twitter у розвідці. Згідно рисунку 2.5 видно, що кількість активних користувачів не падає, а тримається на одному і тому ж рівні, адже це досить стара соцмережа і зараз приплив

нових користувачів не такий великий, але вона все ж тримається в топі найпопулярніших соцмереж.

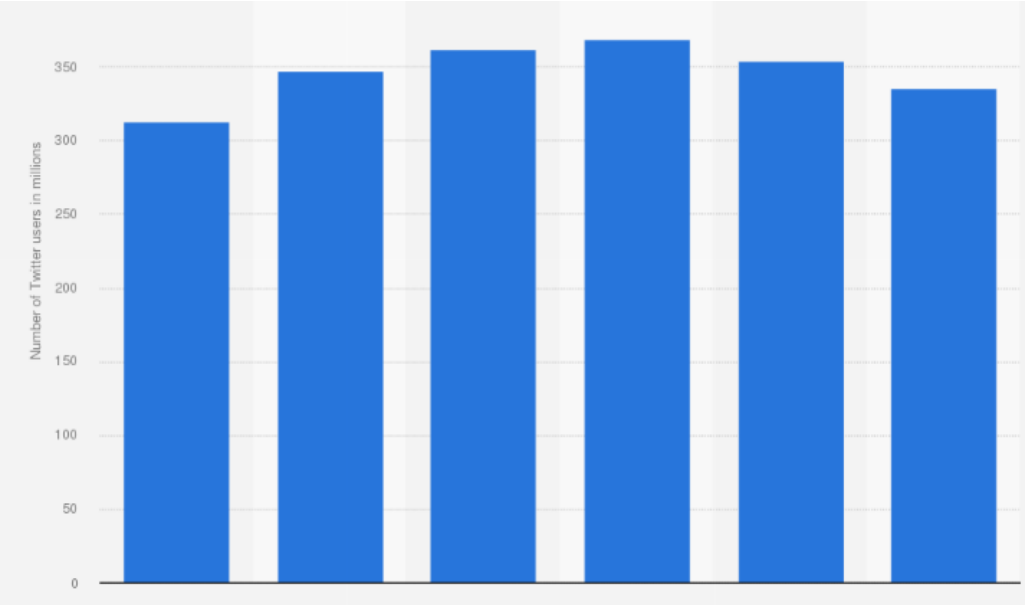


Рисунок 2.5 – Кількість активних користувачів Twitter згідно з statista.com [10]

Соціальні мережі, такі як Reddit, LinkedIn, Instagram, Facebook та Twitter, можуть бути надзвичайно корисними інструментами в OSINT розвідці. Вони надають доступ до широкого спектру інформації, що може бути використана для отримання важливих даних, аналізу трендів та публічної думки, встановлення зв'язків зі спеціалістами та експертами, а також виявлення цінних джерел інформації.

Проте, при використанні соціальних мереж у розвідці, важливо дотримуватись етичних принципів і правил конфіденційності. Доступ до інформації може бути обмежений залежно від налаштувань конфіденційності користувачів, тому важливо бути свідомим і розуміти обмеження та правила використання цих платформ [11].

Крім того, соціальні мережі постійно змінюються, інформація швидко розповсюджується, і велика кількість даних потребує ефективного фільтрування та аналізу. Використовуючи відповідні інструменти та методи,

можна збирати цінну інформацію, встановлювати зв'язки та отримувати цілісне розуміння розглядуваної теми [12].

Загальною тенденцією є те, що соціальні мережі є важливими джерелами публічної інформації, яку можна використовувати в OSINT розвідці. Однак, необхідно бути обережними, маючи на увазі етичні аспекти та правила використання, і використовувати соціальні мережі як один із засобів у ширшому арсеналі розвідувальних методів [13].

2.3 Огляд OSINT Framework

Фреймворк (англ. framework) - це велика структура або платформа, яка надає основу для розробки програмного забезпечення. Він складається з набору бібліотек, інструментів, загальних правил, стандартів і компонентів, які допомагають розробникам швидко та ефективно створювати програми або веб-додатки. Основна мета фреймворка полягає в тому, щоб спростити розробку програмного забезпечення, забезпечити структуру і організацію проекту, а також забезпечити повторне використання коду і прискорити розробку за рахунок надання певного рівня абстракції. Фреймворк надає загальну архітектуру, шаблони проектування і інструменти для розробки, що дозволяє розробникам фокусуватися на бізнес-логікі своїх додатків, а не на низькорівневих деталях. Фреймворки грають важливу роль в OSINT: надають структуру і організацію для проведення OSINT розвідки, визначаючи правила і стандарти роботи. Це допомагає забезпечити систематизованість в процесі збору та аналізу інформації з відкритих джерел.

Однією з головних переваг фреймворків є їх готові компоненти та інструменти, які спрощують роботу розвідників. Вони дозволяють повторно використовувати код, надають шаблони проектування та інші ресурси, що прискорюють процес розвідки. Це дозволяє розвідникам зосередитися на більш важливих аспектах, наприклад, аналізі інформації замість написання

низькорівневого коду. Крім того, фреймворки полегшують інтеграцію з іншими інструментами та сервісами для збору інформації з різних джерел. Це дозволяє розвідникам використовувати різноманітні інструменти і платформи для збору інформації, розширюючи їх можливості. Окрім того, фреймворки допомагають автоматизувати деякі аспекти процесу OSINT розвідки. Вони надають інструменти для автоматичного збору, фільтрації та аналізу інформації, що дозволяє розвідникам ефективно виконувати завдання з меншими зусиллями і часом.

Не останнє місце посідає підтримка та спільнота, що супроводжує фреймворки. Багато фреймворків мають активні спільноти розробників, які надають підтримку, оновлення та нові функції. Це дозволяє користувачам отримувати допомогу, обмінюватися досвідом і використовувати покращені версії фреймворку для своїх потреб.

Взагалі фреймворки в OSINT розвідці є потужними інструментами, які допомагають організувати та стандартизувати процес збору та аналізу інформації з відкритих джерел. Вони спрощують роботу, забезпечують ефективність і дозволяють розвідникам сконцентруватися на важливих аспектах OSINT.

Один з найпопулярніших таких інструментів, це OSINT Framework - веб-сайт, створений звичайним ентузіастом Джастіном Нордінорм, що надає зручний перегляд та доступ до різних інструментів та ресурсів, які можуть бути корисними в процесі OSINT розвідки. Цей веб-сайт надає велику кількість категорій інструментів та джерел інформації, які покривають різні аспекти OSINT розвідки. До цих категорій належать соціальні мережі, пошукові системи, блоги, форуми, географічні ресурси, медіа-платформи, інструменти аналізу та інше. Кожна категорія містить посилання на відповідні інструменти, ресурси та сервіси, які можна використовувати для отримання інформації з цих джерел. Також OSINT Framework також надає корисні посилання на спеціалізовані інструменти для пошуку по електронній пошті,

IP-адресах, телефонних номерах, хеш-значеннях та інших важливих елементах OSINT розвідки. Він також містить посилання на інструменти для виявлення зображень, аналізу тексту, моніторингу соціальних мереж та багато іншого.

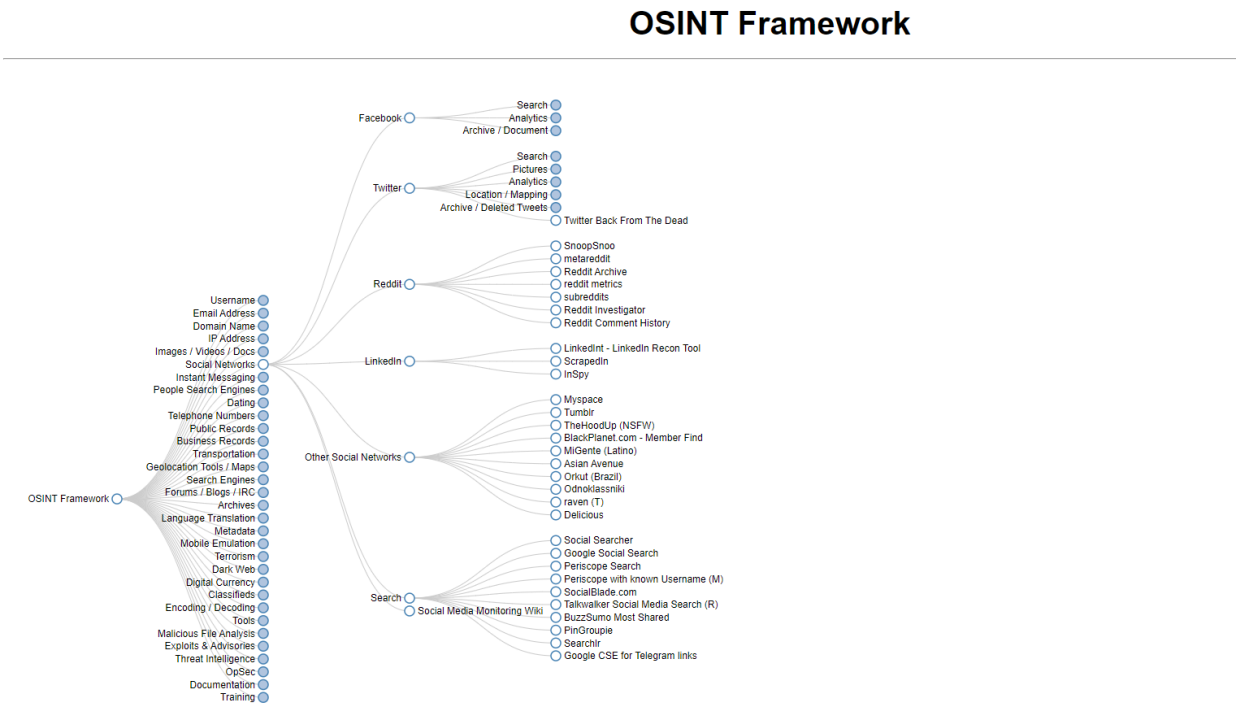


Рисунок 2.6 – Інструменти OSINT Framework

OSINT Framework виконує декілька важливих функцій, серед яких можна відзначити:

— Централізований доступ: він збирає разом різні інструменти та ресурси в одному місці, що дозволяє ефективно організувати та керувати процесом OSINT розвідки.

— Оновлення та розширення: OSINT Framework постійно оновлюється з новими інструментами та ресурсами, що відповідають змінюючимся потребам OSINT розвідки. Це дозволяє користувачам отримувати доступ до найновіших інструментів та методик.

— Систематизація інформації: він розподіляє інструменти та ресурси за категоріями, що допомагає користувачам зорієнтуватися та знайти потрібні інструменти швидко та легко.

— Ефективність: використання OSINT Framework дозволяє економити час та зусилля, оскільки користувачам не потрібно витрачати час на пошук окремих інструментів та ресурсів. Вони можуть швидко знайти все необхідне на одному веб-сайті.

OSINT Framework став популярним серед дослідників безпеки, кіберрозвідки, приватних детективів та інших спеціалістів, які займаються збором інформації з відкритих джерел. Його універсальність та зручність робить його цінним інструментом для виконання OSINT розвідки.

За допомогою цього фреймворку на прикладі пошуку по соціальним мережам можливо вибрати усі потрібні інструменти, які допоможуть провести ретельним пошук заданої теми.

2.4 Можливості пошукової системи Google

Довгий час OSINT асоціювався виключно з пошуком інформації через Google. Google є однією з найбільш відомих та широко використовуваних пошукових систем у світі. Завдяки своїм універсальним пошуковим можливостям, вона стала популярним інструментом у багатьох сферах, включаючи OSINT розвідку. Google є пошуковою системою, яка має колосальну базу даних проіндексованих веб-ресурсів, за якою можна здійснювати пошук [14].

Одна з найбільших баз Google-дорків доступна на сайті ExploitDB, головна сторінка якого показаний на рисунку 2.7.

В загальному більшість пошукових систем дозволяють використовувати команди в полі пошуку і ці команди насправді не є частиною пошукових термінів і називаються операторами. Зазвичай є дві частини оператори пошуку, і кожен розділений двокрапкою (:). З лівого боку розташовується вид оператора, наприклад site (веб-сайт) або ext (розширення файлу), а праворуч саме правило для оператора, для прикладу це може бути цільовий домен або

тип файлу [15]. Ці функції дозволяють здійснювати більш точний та ефективний пошук в рамках OSINT-розвідки.

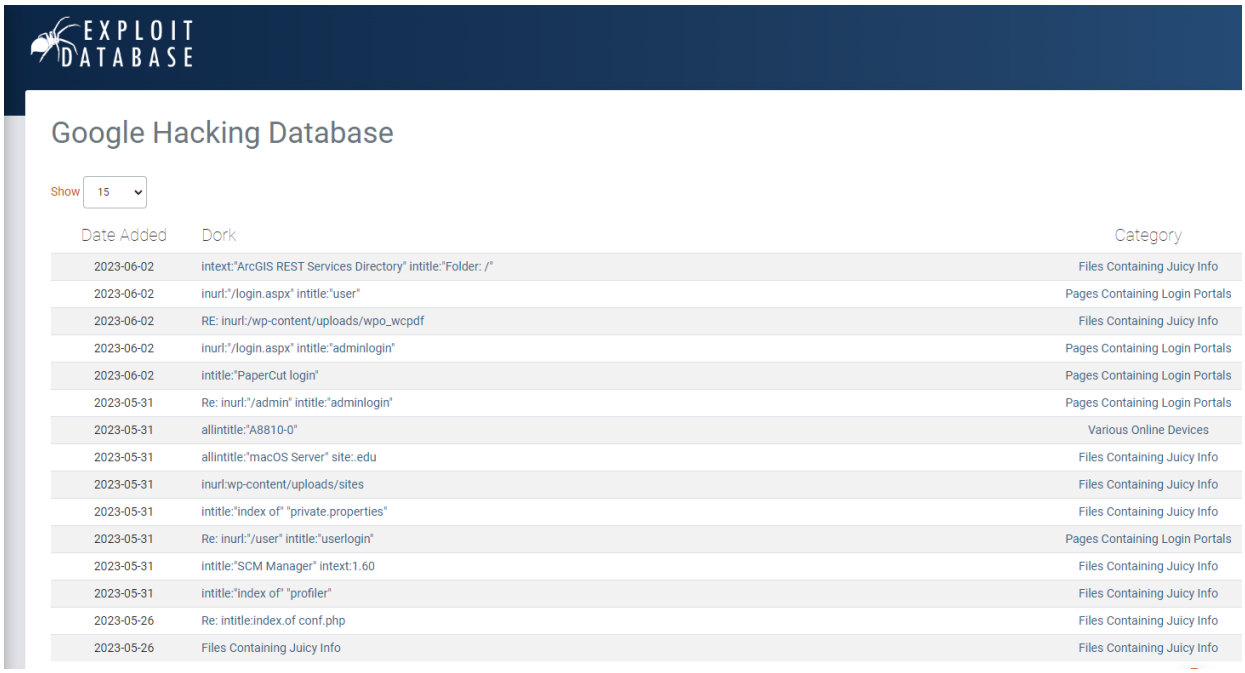


Рисунок 2.7 – Головна сторінка сайту Exploit Database

Також Google часто зберігає у своєму архіві (кеші) ті матеріали, які були видалені, що буває вкрай корисно при проведенні розслідувань.

Однією з ключових переваг Google є її обширний охоплюючий пошук. Google індексує мільярди сторінок в Інтернеті, що дозволяє здійснювати пошук і отримувати результати з різних джерел. Це надає можливість широкого аналізу доступної інформації та збирання великого обсягу даних.

Google також надає додаткові сервіси, такі як Google Maps, Google Images, Google News тощо, які можуть бути корисними в OSINT-дослідженнях. Завдяки цим додатковим ресурсам можна отримати географічну інформацію, зображення, новини та інші дані для аналізу та досліджень.

Крім того, Google надає можливість пошуку інформації в соціальних мережах. Це стає особливо корисним при проведенні OSINT розвідки, оскільки соціальні мережі є важливим джерелом публічної інформації.

Результати пошуку Google включають публічні профілі соціальних мереж, дописи, коментарі, фотографії тощо, що може дати розвідувачам додаткові відомості про особи, організації або події.

Прикладом застосування Google у пошуку інформації в соціальних мережах при OSINT розвідці є пошук публічних профілів осіб, пов'язаних з певною організацією або подією. Розвідувач може використовувати Google для пошуку інформації про ці особи, включаючи їхні профілі в соціальних мережах, дописи, коментарі, фотографії тощо. Це дозволяє зібрати додаткові дані та встановити зв'язки між особами, що сприяє побудові більш повної картини події або діяльності.

У додаток до своїх пошукових можливостей, Google також надає можливості моніторингу через функції, такі як Google Alerts. Ці інструменти надсилають повідомлення про нові результати пошуку або зміни в заданих критеріях, що дозволяє отримувати оновлену інформацію про обрані теми або ключові слова. Крім того, Google пропонує різноманітні спеціалізовані інструменти, які можуть бути корисними в OSINT-розвідці. Наприклад, Google Trends надає інформацію про популярність пошукових запитів в різних регіонах та часових періодах, Google Public Data Explorer дозволяє візуалізувати та аналізувати великі набори публічних даних, а Google Scholar спеціалізується на пошуку наукових публікацій та досліджень.

Загалом, Google є потужним інструментом для збору і аналізу відкритої інформації в рамках OSINT-розвідки. Її широкий охоплюючий пошук, розширені пошукові можливості, додаткові сервіси та спеціалізовані інструменти роблять її найкращим вибором для проведення OSINT-досліджень.

Висновки до другого розділу

Другий розділ кваліфікаційної роботи присвячений засобам реалізації OSINT розвідки. В ньому розглянуто найпопулярніші інструменти, які

використовуються в OSINT-дослідженнях, а також описано їх роботу з найпоширенішими соціальними мережами.

Один з найважливіших інструментів, який був оглянутий, це - OSINT Framework. Цей фреймворк забезпечує доступ до широкого спектру інструментів і ресурсів для збору і аналізу відкритої інформації. Він включає в себе різноманітні інструменти для пошуку даних, аналізу соціальних мереж, перевірки доменних імен, пошуку витоків даних та багато іншого. OSINT Framework є незамінним помічником у проведенні OSINT-розвідки.

Також розглянуто основну пошукову систему, яка є найпопулярнішою і найефективнішою для OSINT-розвідки, - Google. Вона володіє широкими можливостями пошуку, великою базою даних і розширеними функціями, що дозволяють здійснювати більш точний і ефективний пошук інформації з відкритих джерел. Використання Google у OSINT-дослідженнях дозволяє отримати доступ до різноманітної інформації та проводити глибокий аналіз даних.

РОЗДІЛ 3 РЕАЛІЗАЦІЯ ІНСТРУМЕНТУ НА ОСНОВІ ТЕХНОЛОГІЇ OSINT ДЛЯ СОЦІАЛЬНИХ МЕРЕЖ

3.1 Застосування API в OSINT розвідці

API (Application Programming Interface) - це інтерфейс, який програма надає іншим програмам, тобто певний посередник між програмами. Хоча API розроблені для роботи з іншими програмами, вони здебільшого призначені для розуміння та використання людьми, які пишуть інші програми. API — це блоки, які забезпечують взаємодію основних бізнес-платформ в Інтернеті [16].

Застосування API при розвідці OSINT може мати кілька корисних речей:

— Автоматизація збору даних: використання API дозволяє отримати доступ до різних джерел інформації з соціальних мереж та інших платформ. Замість ручного збору даних, API дозволяють автоматизувати процес і отримувати велику кількість даних швидко та ефективно.

— Розширення можливостей: API надають розробникам доступ до різноманітних функцій та даних, які не завжди доступні через загальнодоступні інтерфейси. Це дозволяє отримувати детальнішу інформацію, виконувати спеціалізовані запити та використовувати додаткові можливості платформи.

— Фільтрація та обробка даних: завдяки API можна отримувати дані у структурованому форматі, що спрощує фільтрацію та обробку інформації. API можуть надавати параметри пошуку, фільтри та сортування, що дозволяє точніше вибирати необхідні дані та пристосовувати їх до своїх потреб.

— Розширення джерел інформації: використання API дозволяє взаємодіяти з різними платформами та сервісами, які надають свої інтерфейси програмування. Це дозволяє отримувати інформацію з широкого спектру джерел, включаючи соціальні мережі, блоги, форуми, новинні сайти тощо.

Розширення джерел інформації сприяє отриманню більш повної та різноманітної картини.

— Посилена аналітика та візуалізація: використання API дозволяє об'єднувати дані з різних джерел і створювати більш комплексні аналітичні звіти. Можна застосовувати аналітичні методи та алгоритми для знаходження залежностей, виявлення шаблонів та розуміння контексту. Крім того, API дозволяють візуалізувати дані у зручний та зрозумілий спосіб, що полегшує аналіз та сприяє розробленню обґрунтованих висновків.

Застосування API значно полегшує та розширює можливості проведення OSINT розвідки, дозволяючи отримати більше даних, автоматизувати процес та забезпечити більш точний та ефективний аналіз.

3.2 Створення плану пошуку при OSINT розвідці

Створення плану при проведенні OSINT розвідки є дуже важливим, адже треба чітко розуміти план дій, щоб знайти усю корисну інформацію.

План проведення OSINT розвідки по соціальних мережах може включати наступні кроки:

— Визначення цілей. Спочатку потрібно чітко сформулювати мету розвідки. Це може бути збір інформації про певну особу, компанію, організацію або виявлення певної діяльності чи зв'язків.

— Вибір соціальних мереж. Визначте, які соціальні мережі потрібно дослідити в рамках вашої розвідки. Наприклад, Facebook, Twitter, Instagram, LinkedIn, YouTube тощо. Залежно від контексту, можливо, варто розглянути використання спеціалізованих платформ, таких як GitHub для розвідки серед розробників.

— Збір відкритої інформації. Почніть зі збору відкритої інформації на обраних соціальних мережах. Огляньте профілі особи або організації, розгляньте їх публічні повідомлення, фотографії, взаємодії з іншими

користувачами. Зверніть увагу на деталі профілю, такі як місце роботи, освіту, зацікавлення, зв'язки тощо. Запишіть будь-яку корисну інформацію.

— Дослідження зв'язків. Аналізуйте зв'язки між об'єктом розвідки та іншими користувачами. Перегляньте списки друзів, підписників, підписок та спільні групи. Це може дати уявлення про соціальну мережу особи, її вплив та зв'язки з іншими людьми.

— Дослідження активності. Вивчайте активність об'єкта розвідки на соціальних мережах. Ретельно огляньте його повідомлення, коментарі, вподобання та реакції на публікації інших користувачів. Це може розкрити думки, погляди, зацікавлення або потенційно небезпечну діяльність.

— Використання інструментів та пошукових запитів. Можна скористатись спеціалізованими інструментами для OSINT розвідки, такими як Maltego, Social-Searcher, Echosec, або провести розширений пошук, використовуючи спеціальні ключові слова та пошукові запити, щоб знайти більше інформації про об'єкт розвідки.

— Аналіз інформації. Після збору інформації проведіть аналіз і зробіть висновки. Спробуйте з'єднати крапки, виявити шаблони, визначити можливі ризики або перспективи. Запишіть висновки та підготуйте звіт.

Також важливо дотримуватись законодавства. Слід пам'ятати, що під час проведення OSINT розвідки потрібно дотримуватися законодавства та правил конфіденційності. Не використовувати отриману інформацію для незаконних чи шкідливих дій. Це варто врахувати при створенні плану розвідки і під час її проведення, адже наслідки можуть бути дуже серйозними [17].

Це загальний план, який можна використовувати для проведення OSINT розвідки по соціальних мережах. Зауважте, що кожен випадок може мати свої унікальні особливості та вимоги, тому план може змінюватися в залежності від контексту та потреб розвідки.

3.3 Створення інструменту для пошуку у соціальних мережах

Для написання інструменту було вибрано мову програмування Python, яка є дуже зручною для написання програм з використанням API з кількох причин. Python має дуже зрозумілий та простий синтаксис, що дозволяє швидко та легко писати код. Це зменшує час, необхідний для розробки програми з використанням API, і полегшує розуміння коду іншими розробниками. Також у Python є широкий вибір бібліотек для роботи з API. Бібліотеки, такі як Requests, PyCurl, Tweepy, Google API Python Client та багато інших, надають зручний інтерфейс для взаємодії з різними API. Також варто відмітити, що Python має вбудовану підтримку для серіалізації та десеріалізації даних у форматах, таких як JSON та XML. Це особливо корисно, оскільки багато API повертають дані у цих форматах, і Python надає зручні засоби для роботи з ними. Обробка та аналіз отриманих даних стають простішими та зручнішими завдяки цим можливостям, Python підтримує модульну структуру коду, що дозволяє організовувати програму в окремі модулі та пакети. Це сприяє підтримці чистого, організованого та зрозумілого коду. Крім того, Python також має можливості для розширення за допомогою модулів, написаних на C або інших мовах програмування, що дозволяє використовувати спеціалізовані бібліотеки для роботи з API. Python має велику та добре документовану спільноту розробників. Багато API надають документацію та приклади коду на Python, що значно спрощує розуміння та використання API. Завдяки активній спільноті, можливо легко знайти рішення для своїх питань або проблем, пов'язаних з використанням API у Python. Всі ці переваги роблять мову Python дуже зручною для написання програм з використанням API. Вона дозволяє розробникам ефективно працювати з API, зосереджуючись на функціональності програми та взаємодії з зовнішніми сервісами, замість деталей низькорівневої роботи з мережею або серіалізації даних.

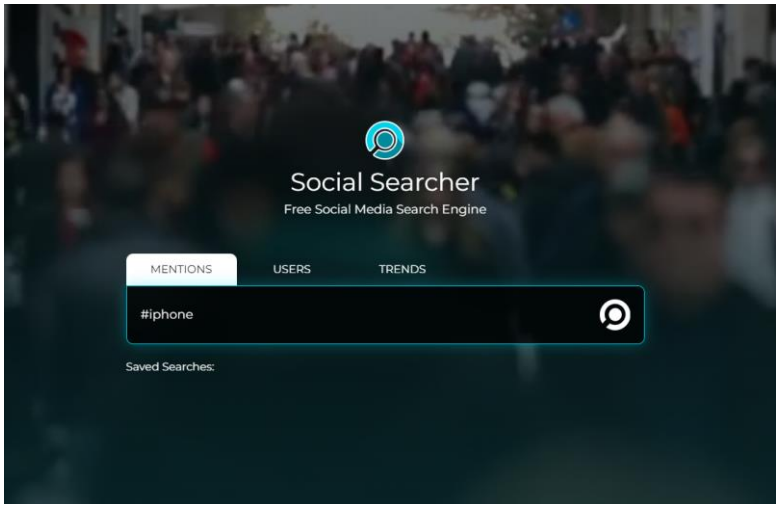


Рисунок 3.1 – Інтерфейс сервісу Social Searcher

Також було обрано сервіс Social Searcher, який є безкоштовним інструментом для проведення пошуку в соціальних мережах, інтерфейс якого зображено на рисунку 3.1. На головній сторінці бачимо, що за допомогою цього інструменту можливо проводити пошук по згадках, користувачах і різних трендах. Розглянемо пошук за користувачем, який проводить пошук у таких соціальних мережах, як Facebook, Instagram, Dailynotion і LinkedIn

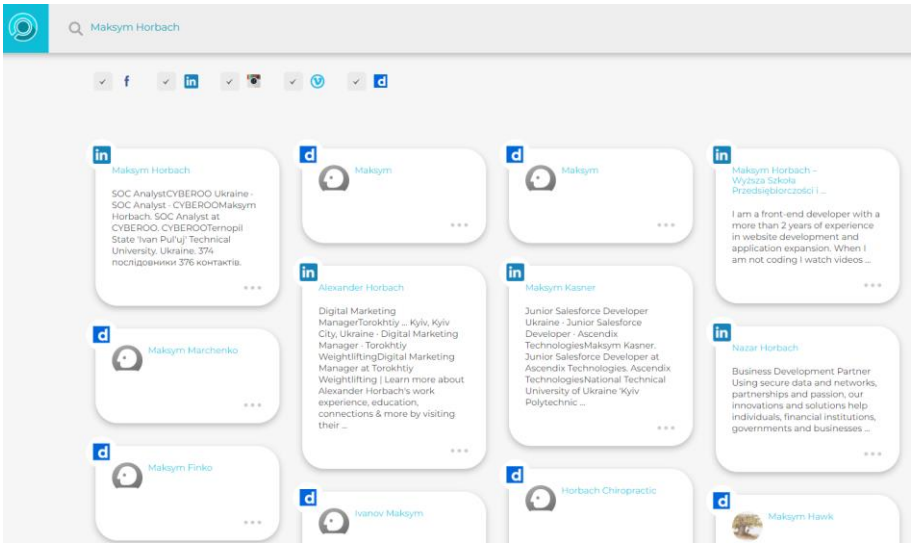
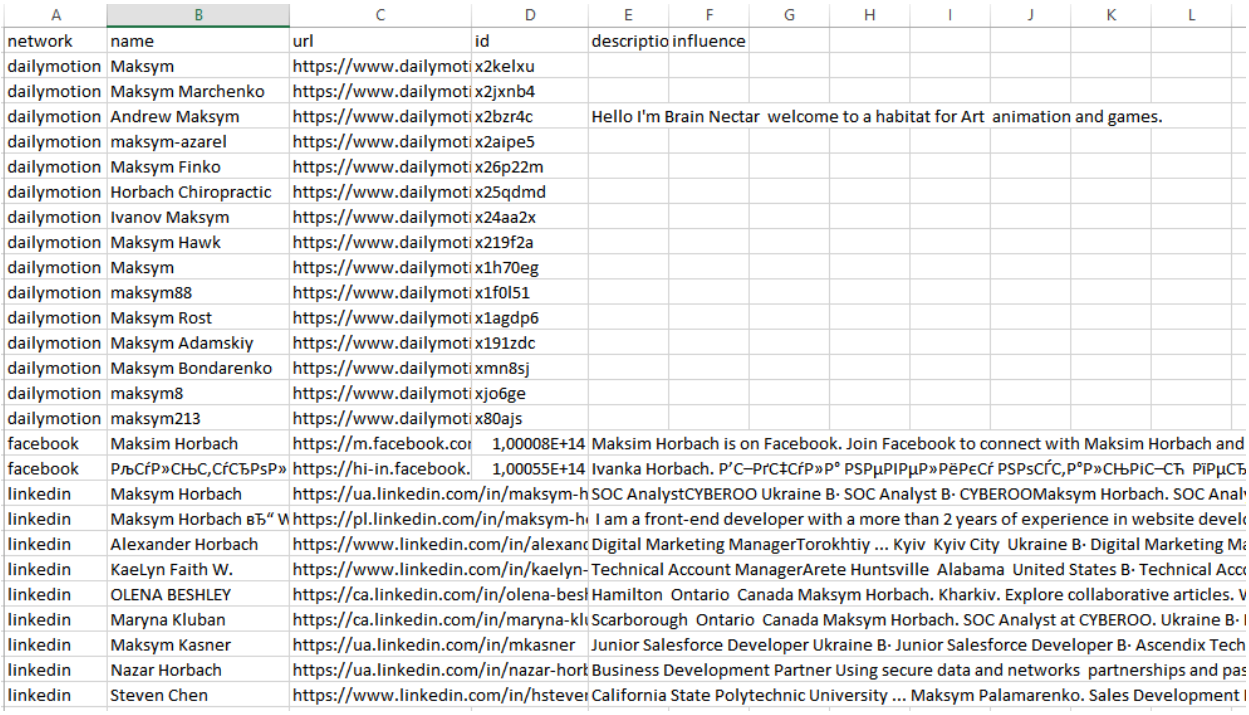


Рисунок 3.2 – Результат пошуку за користувачем

Після проведеного пошуку також маємо можливість зробити експорт інформації у Excel-файл. Що може бути корисно при аналізі даних, а також у

випадках, коли створюємо інструмент на API сервісі і хочемо отримувати результати пошуку в певну папку, або файл. Приклад експорту зображений на рисунку 3.3.



network	name	url	id	descriptio	influence
dailymotion	Maksym	https://www.dailymoti	x2kelxu		
dailymotion	Maksym Marchenko	https://www.dailymoti	x2jxnb4		
dailymotion	Andrew Maksym	https://www.dailymoti	x2bzr4c	Hello I'm Brain Nectar welcome to a habitat for Art animation and games.	
dailymotion	maksym-azarel	https://www.dailymoti	x2aipe5		
dailymotion	Maksym Finko	https://www.dailymoti	x26p22m		
dailymotion	Horbach Chiropractic	https://www.dailymoti	x25qdmd		
dailymotion	Ivanov Maksym	https://www.dailymoti	x24aa2x		
dailymotion	Maksym Hawk	https://www.dailymoti	x219f2a		
dailymotion	Maksym	https://www.dailymoti	x1h70eg		
dailymotion	maksym88	https://www.dailymoti	x1f0l51		
dailymotion	Maksym Rost	https://www.dailymoti	x1agdp6		
dailymotion	Maksym Adamskiy	https://www.dailymoti	x191zdc		
dailymotion	Maksym Bondarenko	https://www.dailymoti	xmn8sj		
dailymotion	maksym8	https://www.dailymoti	xjo6ge		
dailymotion	maksym213	https://www.dailymoti	x80ajs		
facebook	Maksim Horbach	https://m.facebook.co	1,00008E+14	Maksim Horbach is on Facebook. Join Facebook to connect with Maksim Horbach and	
facebook	РљСѓР»СЊС‚СЂСЂР»	https://hi-in.facebook.	1,00055E+14	Ivanka Horbach. Р'С–РґС‡СѓР»Р° PSPµPIPµР»РёРєСѓ PSPsСЃС‚Р°Р»СЊРіС–СЂ РїРµСЂ	
linkedin	Maksym Horbach	https://ua.linkedin.com/in/maksym-h		SOC AnalystCYBEROO Ukraine В· SOC Analyst В· CYBEROOMaksym Horbach. SOC Anal	
linkedin	Maksym Horbach вЂ“ W	https://pl.linkedin.com/in/maksym-h		I am a front-end developer with a more than 2 years of experience in website develo	
linkedin	Alexander Horbach	https://www.linkedin.com/in/alexanc		Digital Marketing ManagerTorokhtiy ... Kyiv Kyiv City Ukraine В· Digital Marketing Ma	
linkedin	KaeLyn Faith W.	https://www.linkedin.com/in/kaelyn-		Technical Account ManagerArete Huntsville Alabama United States В· Technical Acc	
linkedin	OLENA BESHLEY	https://ca.linkedin.com/in/olena-besl		Hamilton Ontario Canada Maksym Horbach. Kharkiv. Explore collaborative articles. V	
linkedin	Maryna Kluban	https://ca.linkedin.com/in/maryna-kl		Scarborough Ontario Canada Maksym Horbach. SOC Analyst at CYBEROO. Ukraine В·	
linkedin	Maksym Kasner	https://ua.linkedin.com/in/mkasner		Junior Salesforce Developer Ukraine В· Junior Salesforce Developer В· Ascendix Tech	
linkedin	Nazar Horbach	https://ua.linkedin.com/in/nazar-hort		Business Development Partner Using secure data and networks partnerships and pas	
linkedin	Steven Chen	https://www.linkedin.com/in/hstever		California State Polytechnic University ... Maksym Palamarenko. Sales Development	

Рисунок 3.3 – Експортований результат пошуку у Excel-файл

Великою перевагою цього інструменту – безкоштовне використання API для автоматизації проведення пошуку.

Для реалізації інструменту було написано функцію загального пошуку по сайту з лімітом в топ 10 результатів.

Приклад API-запиту:

```
https://api.social-
searcher.com/v2/search?q={email}&key={social_searcher_api_key}&l
imit=10
```

Наведений нижче лістинг 3.1 є частиною додатку А.

```
def search_social_searcher_by_email(email):
    try:
        # Виконання запиту до Social Searcher API
```

```
            url = f"https://api.social-searcher.com/v2/search?q={email}&key={social_searcher_api_key}&limit=10"
            response = requests.get(url)
```

Лістинг 3.1 – Функція пошуку

Після запуску програми бачимо на рисунку 3.4 результат пошуку, який видав 10 найрелевантніших результатів з різних соціальних мереж.

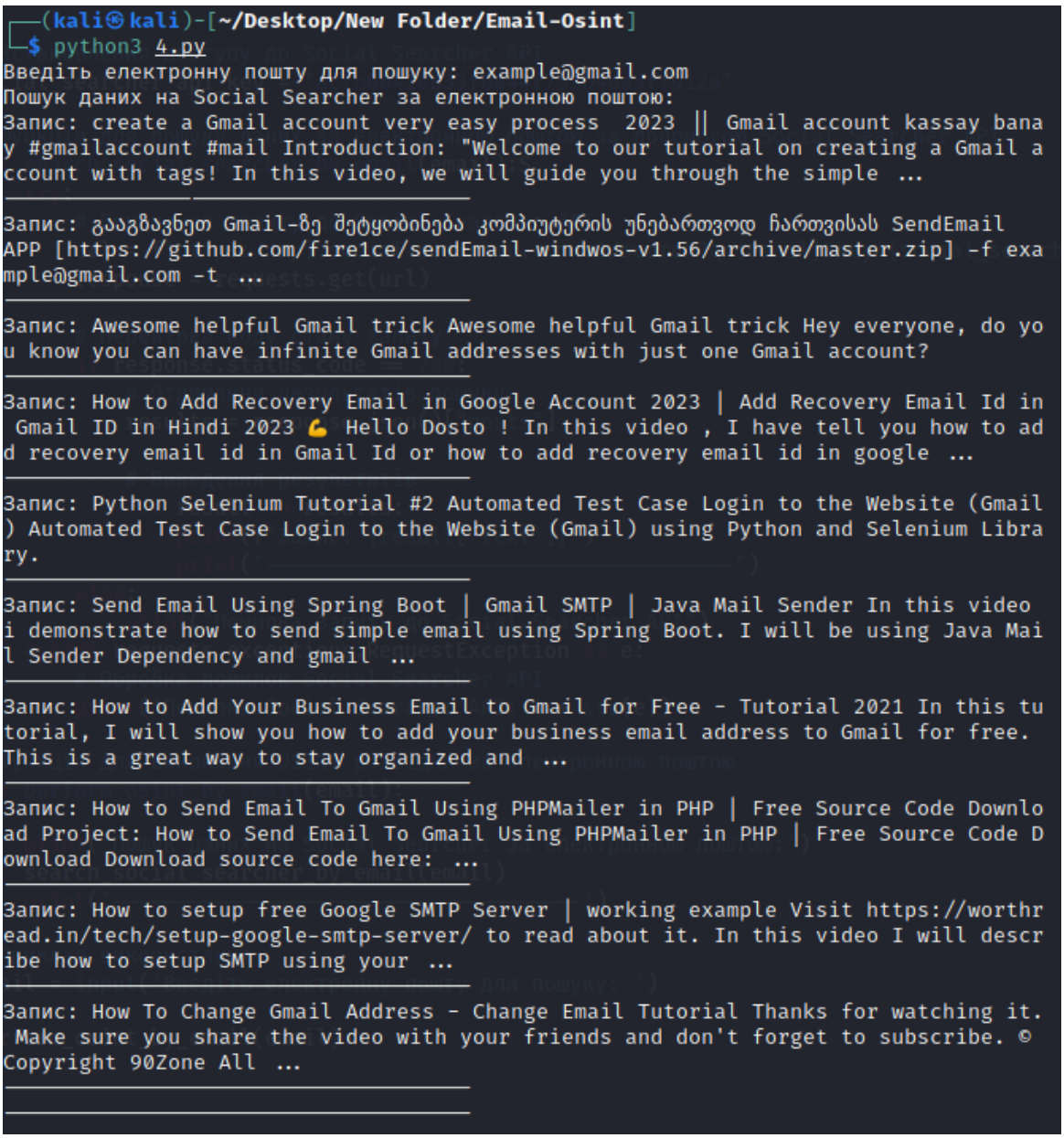


Рисунок 3.4 – Результати пошуку

3.4 Проведення OSINT розвідки для соціальних мереж

На самому початку розвідки потрібно буде провести пошук по усій доступній інформації по цілі, яка у нас є. Для початку рекомендується провести загальний пошук в пошукових системах, для прикладу Google, використовуючи інструмент Google Dorking, який було описано вище і провести пошуки з різними операторами, серед який “site:”, включивши туди домени різних соціальних мереж, як показано на рисунках 3.5 і 3.6.

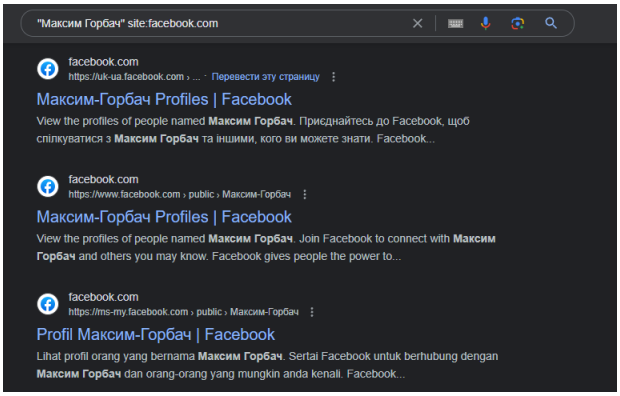


Рисунок 3.5 – Пошук за допомогою оператора site

Також варто пам’ятати, що при пошуку варто використовувати різні мови, для прикладу при пошуку по імені, можна писати його як на англійській, так і на українській мовах.

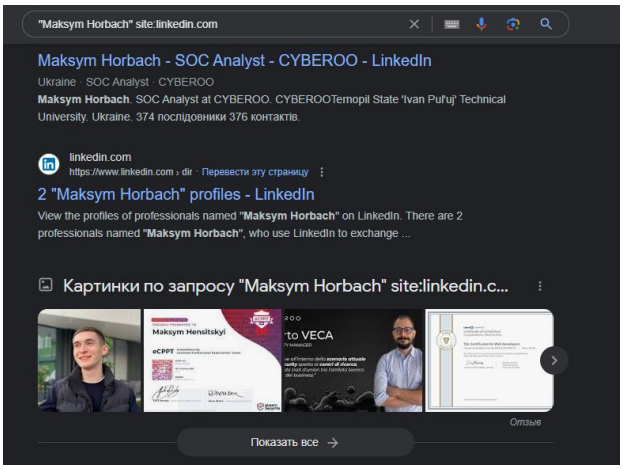


Рисунок 3.6 - Пошук за допомогою оператора site

З пошуку на рисунку 3.6 вилно, що вдалось знайти відповідний профіль на LinkedIn, спробуємо дістати з нього корисну інформацію. LinkedIn – сайт, на якому зазвичай готові розглядати нові вакансії і тому часто додають персональну інформацію для контактів, наприклад номер телефону, або ж електронну адресу, як у наведеному випадку, що зображено на рисунку 3.7.

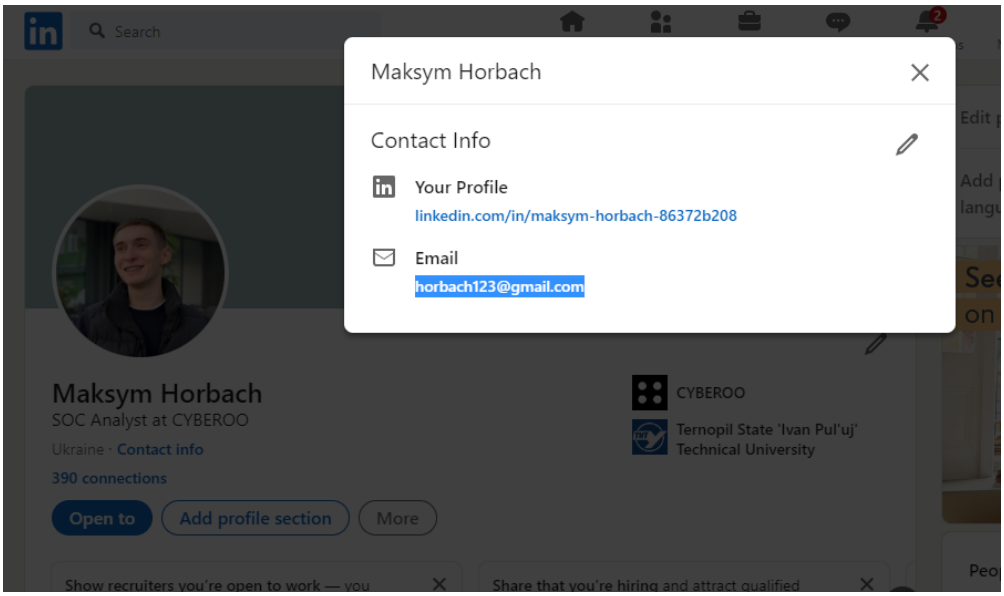


Рисунок 3.7 – Контактна інформація профіля з сайту LinkedIn

Після того, як вдалось дізнатись електронну адресу користувача, можливо спробувати дістати з неї додаткову інформацію. Для початку можна перевірити, чи задіяно її в якомусь з дата брічів, це можна зробити за допомогою ресурсу HIBP, як зображено на рисунку 3.8. Змогли дізнатися, що ця електронна адреса була задіяна в Cit0day дата бріч (у листопаді 2020 року колекція з понад 23 000 ймовірно зламаних веб-сайтів, відомих як Cit0day, була доступна для завантаження на кількох хакерських форумах. Дані складалися з 226 мільйонів унікальних адрес електронної пошти разом із парами паролів, часто представлених як хешами паролів, так і зламаними версіями простого тексту), за допомогою CSINT (closed source intelligence, що означає процес збору інформації з закритих джерел або інформації, яка не доступна загальному публічному доступу).

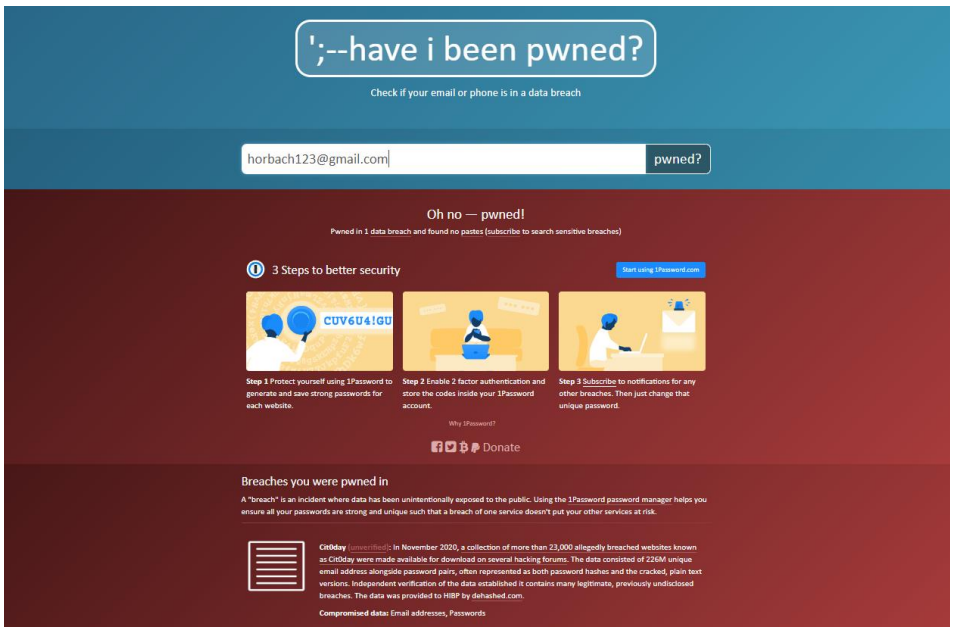


Рисунок 3.8 – Ресурс HIBP (Have I Been Pwned)

На ресурсі seon.io, про яких згадувалось в попередніх розділах можна перевірити, до яких саме сайтів і соціальних мереж прив’язана задана електронна пошта, як показано на рисунку 3.9.

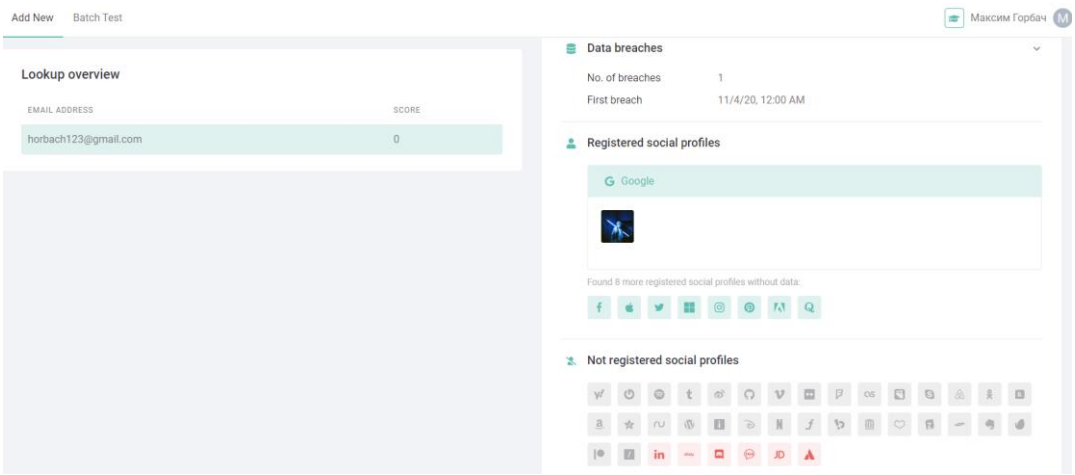


Рисунок 3.9 – Ресурс seon.io

Після цього можна спробувати проводити відновлення паролю за допомогою знайденої електронної адреси, як показано на рисунку 3.10, де червоним кольором виділена форма відновлення паролю у Google, чорним – Apple ID і синім – Facebook. Після таких дій дізнались, що номер цього

користувача закінчується на 76, що може бути корисним при звірці даних, якщо наприклад знайдемо номер телефону користувача на інших ресурсах чи витоках даних.

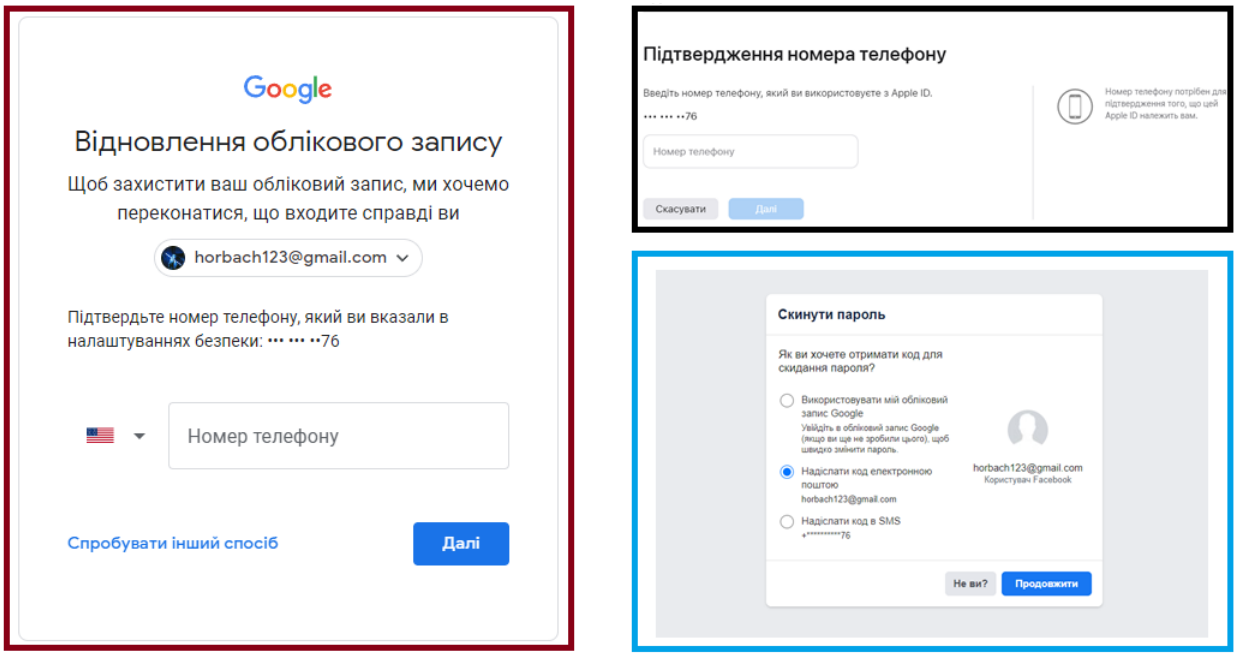


Рисунок 3.10 – Приклади форм відновлення паролю Google, Apple ID і Facebook

Є багато інструментів, які допомагають проводити пошук за зображеннями, для прикладу це може бути FaceCheck.ID, Pim Eyes або ж пошук за зображенням у Google. На рисунку 3.11 бачимо пошук по зображенню користувача, який знайшли на сторінці LinkedIn, а на рисунку 3.12 провели пошук по одному з знайдених зображень. Таким чином знайшли ще фотографії цієї людини і бачимо, що ці фотографії знайдені на сайті https://shkola-licej6.te.ua/, який належить Тернопільському навчально-виховний комплексу "Школа-ліцей №6 ім. Н.Яремчука". Цим змогли дізнатись, що дана людина навчалась в школі №6 у м. Тернопіль. Також варто зазначити, що це результати PimEyes, які були знайдені за допомогою безкоштовного пошуку, на цьому сайті також є можливість купити підписку,

яка дасть можливість проводити поглиблений пошук і отримувати безпосередньо посилання на фото, на якому знайдено ціль пошуку.

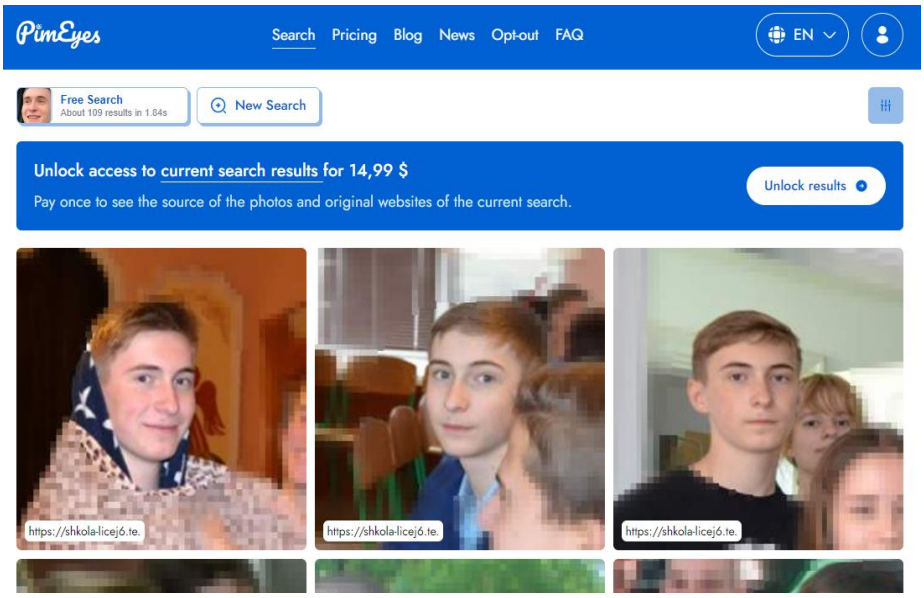


Рисунок 3.11 – Результат пошуку PimEyes

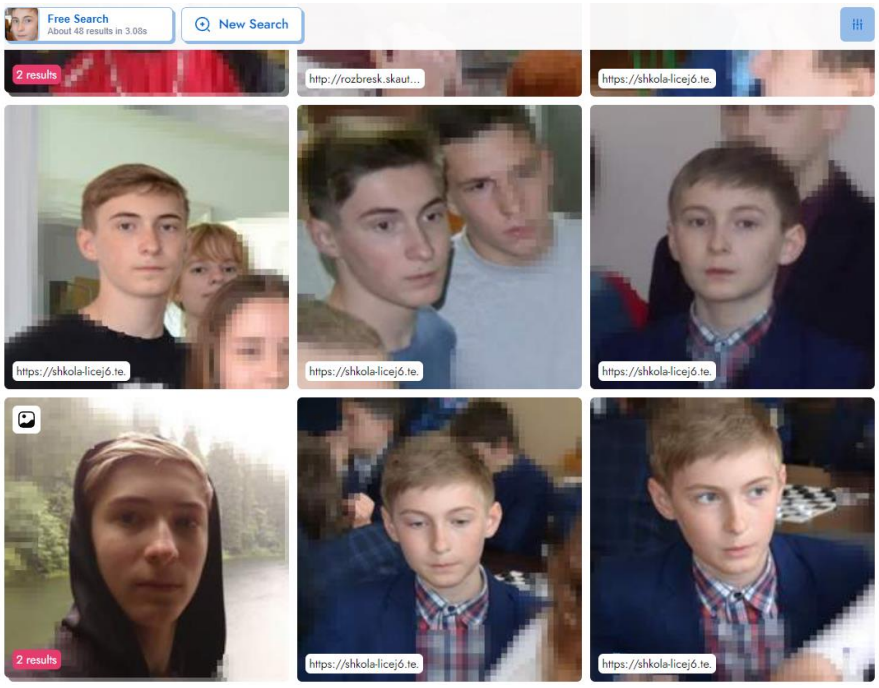


Рисунок 3.12 – Результат пошуку по зображенню

Також спробували провести пошук на FaceCheck.ID, але там отримали лише профіль з LinkedIn.

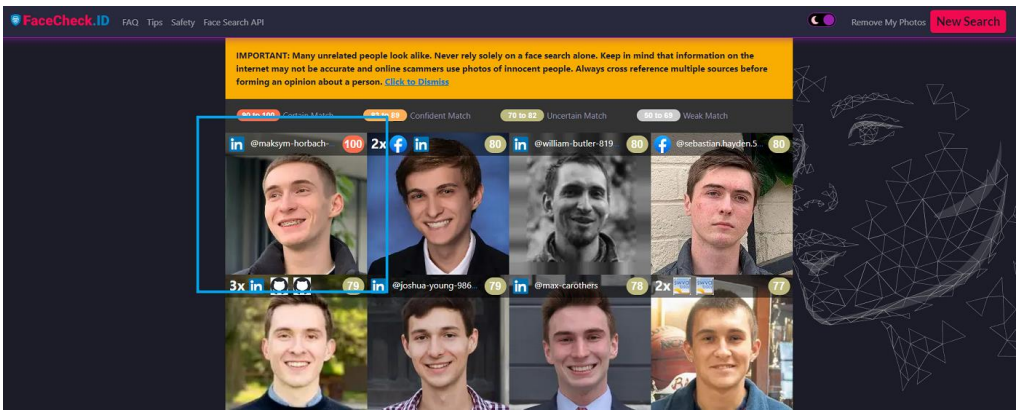


Рисунок 3.13 – Результат пошуку FaceCheck.ID

Також для поглибленого пошуку можна спробувати безкоштовні ресурси для знаходженню паролів, для прикладу це може бути телеграм-бот @PasswordSearchBot, який видав один із потенційних паролів користувача.

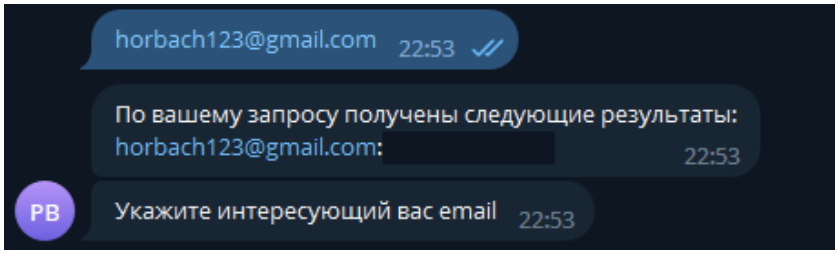


Рисунок 3.14 – Пошук в телеграм-боті PasswordSearchBot

Також важливо повторювати початкові етапи пошуку, якщо знайшли ще якісь деталі окрім тих, які мали з самого початку, для прикладу після отримання електронної адреси користувача знову можемо скористатися інструментом Google Dorking і провести пошук по різних типах файлів, адже часто електронні адреси можуть бути знайдені у різних документах у відкритому доступі, резюме, тощо. Важливо пам’ятати, що є сайти по типу pastebin.com, які можуть використовуватись користувачами для різних цілей і часто такі сайти можуть містити конфіденційну інформацію, яка ненавмисно залишена користувачем. Приклади таких пошуків зображені на рисунку 3.15.

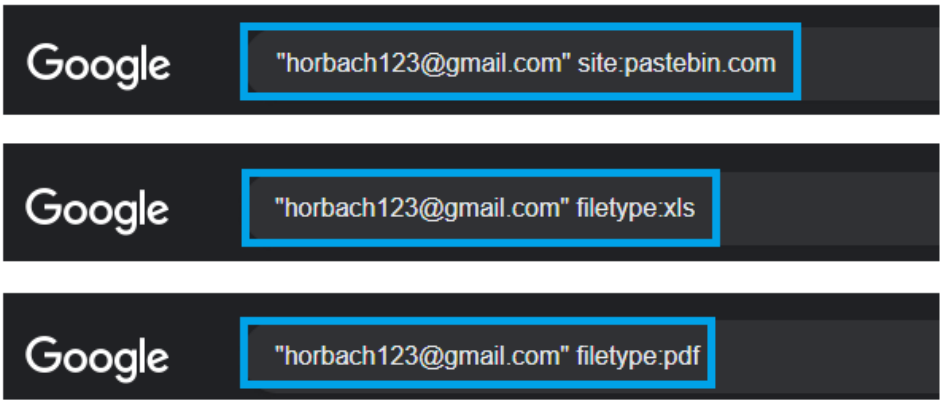


Рисунок 3.15 – Пошук за допомогою Google Dorking

Висновки до третього розділу

У цьому розділі була проведена практична реалізація використання технології OSINT для збору, узагальнення та аналізу інформації з використанням різних соціальних мереж.

По-перше, було детально розглянуто застосування API в OSINT розвідці. Була створено інструмент, який використовує API одного з ресурсів та проводить відповідний пошук інформації. Це дозволяє отримувати доступ до певних даних, які розміщені на цьому ресурсі, і використовувати їх для подальшого аналізу.

По-друге, був розроблений план пошуку при OSINT розвідці, який включав в себе використання соціальних мереж. За допомогою цього плану був проведений пошук на конкретній цілі. Під час такого пошуку вдалося знайти значну кількість інформації, яка містилась як у відкритих джерелах, так і безпосередньо в соціальних мережах.

Соціальні мережі виявилися надзвичайно важливим джерелом інформації під час OSINT розвідки. Вони дозволяють отримати доступ до персональних профілів, публічних постів, фото- та відеоматеріалів користувачів, а також коментарів та взаємодій між ними. Ця інформація може бути цінною для аналізу і розуміння певних подій, осіб або організацій.

Використання соціальних мереж у OSINT розвідці може допомогти

виявити зв'язки між особами, встановити їхні місця перебування, інтереси, думки та активності. Це може бути корисно для розслідування злочинів, виявлення шпигунської діяльності, оцінки громадської думки та викриття фейкової інформації.

Тому, соціальні мережі виконують важливу роль у процесі збору інформації при використанні методів OSINT. Вони дозволяють отримати доступ до великої кількості відкритої інформації, яка може бути використана для розуміння і прогнозування різних ситуацій, а також для забезпечення безпеки та захисту суспільства.

РОЗДІЛ 4 БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ, ОСНОВИ ОХОРОНИ ПРАЦІ

4.1 Поведінкові реакції населення у надзвичайних ситуаціях

Для того, щоб дізнатись поведінкові реакції населення у надзвичайних ситуаціях, потрібно визначитись із терміном надзвичайної ситуації. Надзвичайна ситуація техногенного та природного характеру - порушення нормальних умов життя і діяльності людей на окремій території чи об'єкті на ній або на водному об'єкті, спричинене аварією, катастрофою, стихійним лихом або іншою небезпечною подією, в тому числі епідемією, епізоотією, епіфітотією, пожежею, яке призвело (може призвести) до неможливості проживання населення на території чи об'єкті, ведення там господарської діяльності, загибелі людей та/або значних матеріальних втрат. Зона надзвичайної ситуації - окрема територія, де склалася надзвичайна ситуація техногенного та природного характеру [18].

Питання поведінки людей у різних надзвичайних ситуаціях мають велике значення для підготовки керівників, рятувальників і громадськості до дій у разі екстремальних подій. Особлива увага приділяється психології страху, оскільки люди стикаються з небезпеками, що створюють страхові реакції у вигляді емоційного стану, викликаного реальною або уявною загрозою.

Страх слугує сигналом тривоги, що активує захисні реакції людини. Хоча страх є негативним відчуттям, він також спонукає до індивідуальних або колективних захисних дій, оскільки головна мета полягає у збереженні власного життя та продовженні існування.

Важливо враховувати, що в умовах небезпеки люди часто реагують необдумано і несвідомо. Існують різні фактори, які можуть спричинити загрозу життю людини через агресивний вплив, такі як екстремальні

температури, хімічні речовини, фізичні сили, біологічні фактори та іонізуюче випромінювання.

Готовність людини до надзвичайних ситуацій вимагає високої емоційної стійкості, рішучості та витримки. Такі події можуть викликати значну емоційну збудженість, вимагаючи допомоги постраждалим і рятуванню матеріальних цінностей.

У таких обставинах може бути порушений процес нормального мислення, втрачений контроль над собою та діями, що може мати непередбачувані наслідки. Подолання страху, зазвичай, залежить від почуття власної відповідальності та усвідомлення значимості виконуваної дії.

Незахищені психологічно та необізнані люди відчувають страх і намагаються покинути небезпечні місця. Вони можуть зазнати психологічного шоку, який супроводжується заціпенінням м'язів. В такі моменти порушується процес нормального мислення, втрачається контроль над почуттями та волею.

Реакція нервової системи на страх може проявлятися по-різному, включаючи розширення зіниць, підвищення пульсу, зміни дихання, потовиділення, спазми кровоносних судин, втрату мови та зміни голосу. У деяких випадках раптовий страх може призвести до серйозних проблем зі здоров'ям серцево-судинної системи, навіть смерті.

Цей стан може тривати від кількох годин до декількох днів. Часто при ліквідації наслідків надзвичайних ситуацій спостерігаються люди, які перебувають у стані глибокої депресії, блукають безцільно серед руїн протягом тривалого періоду.

Причини такої поведінки людей у надзвичайних ситуаціях можуть включати слабку морально-психологічну підготовку, неочікуване виникнення небезпеки, відсутність знань про характер та наслідки таких ситуацій, незнання правил поведінки в них, а також відсутність навичок та досвіду в боротьбі з ними [19].

4.2 Заходи, що забезпечують оптимальні метеорологічні умови в санітарно-побутових приміщеннях

Один з способів взаємодії організму людини з оточуючим середовищем - це обмін теплом. Організм людини віддає тепло, переважно, за допомогою конвекції, випаровування та випромінювання. Тип і рівень тепловіддачі залежать від фізичного навантаження і погодних умов оточуючого середовища.

Організм людини може адаптуватися до цих умов і підтримувати постійну температуру. Це властивість організму, відома як терморегуляція. Проте можливості терморегуляції обмежені. При високій температурі повітря віддача тепла відбувається переважно через випаровування, а при низькій - через конвекцію. Тривале перебування людини в умовах з високою температурою повітря може призвести до теплового удару, а при низькій - до переохолодження.

Висока і низька температура оточуючого середовища створює загрозу для організму людини, спричиняючи гострі і хронічні захворювання. При відносній вологості повітря менше 20%, слизові оболонки дихальних шляхів висихають; при відносній вологості понад 85%, теплообмін через випаровування сповільнюється [20].

Навколишнє середовище з високими значеннями температури і відносною вологості повітря є особливо небезпечним для людини. Збільшення швидкості повітря підсилює процеси тепловіддачі. Для комфортного теплового стану людини важливо поєднання температури, відносної вологості та швидкості руху повітря. Тепловий стан організму людини значно впливає на теплове випромінювання від Сонця та технологічних пристроїв.

Визначають оптимальні та припустимі мікрокліматичні умови:

- оптимальні мікрокліматичні умови - це поєднання показників мікроклімату, які за тривалий і систематичний вплив на людину забезпечують

збереження нормального теплового стану організму без напруження механізмів терморегуляції. Вони забезпечують відчуття теплового комфорту і сприяють високій продуктивності праці.

- припустимі мікрокліматичні умови - це поєднання показників мікроклімату, які при тривалому і систематичному впливі на людину можуть змінити тепловий стан її організму, але швидко нормалізуються. Ці умови вимагають напруження механізмів терморегуляції, але не перевищують фізіологічні можливості адаптації. Хоча стан здоров'я не порушується, можуть виникати незручні відчуття тепла, погіршення самопочуття і зниження продуктивності.

Робочою зоною вважається простір, обмежений по висоті 2 метри над рівнем підлоги або площадки, де знаходяться працівники. У холодний період року середня добова температура зовнішнього повітря становить +10°С і нижче, а у теплий період - вище +10°С [20].

"ДСТУ-Н Б А.3.2-1:2007 Система стандартів безпеки праці. Настанова щодо визначення небезпечних і шкідливих факторів та захисту від їх впливу при виробництві будівельних матеріалів і виробів та їх використанні в процесі зведення та експлуатації об`єктів будівництва" є нормативним документом, який надає настанови та вимоги щодо визначення небезпечних та шкідливих факторів, а також заходів захисту від їх впливу на підприємствах, що займаються виробництвом будівельних матеріалів та використанням їх у процесі будівництва і експлуатації об'єктів будівництва. Керівники підприємств повинні користуватись цим стандартом для забезпечення безпеки праці, дотримання вимог щодо захисту працівників від небезпечних факторів, а також для виконання нормативних вимог та забезпечення якості будівельних матеріалів і виробів" [21].

Забезпечення оптимальних метеорологічних умов в санітарно-побутових приміщеннях є важливим аспектом забезпечення комфорту, здоров'я та безпеки проживання людей. Правильна організація вентиляції,

оптимальний рівень температури, вологості та освітлення сприяють створенню здорового та приємного середовища, де люди можуть працювати, відпочивати і займатися побутовими потребами.

Основні заходи, які допомагають забезпечити оптимальні метеорологічні умови в санітарно-побутових приміщеннях, включають:

- вентиляція: ефективна система вентиляції є важливою для забезпечення свіжого повітря та видалення забрудненого повітря з приміщення. Це може бути досягнуто шляхом використання природної вентиляції через вікна, двері, вентиляційні отвори, або за допомогою механічної вентиляції, такої як системи кондиціонування повітря з обмінниками тепла та фільтрами для очищення повітря від шкідливих речовин.
- температура: підтримка комфортної температури в приміщенні є важливою для забезпечення здоров'я та благополуччя людей. Рекомендована температура залежить від функціонального призначення приміщення, проте загальною рекомендацією є збереження температури в діапазоні 24°C.
- вологість: оптимальний рівень вологості також впливає на комфорт та здоров'я. Занадто сухе повітря може спричиняти висихання шкіри, дратувати дихальні шляхи та сприяти поширенню пилу. Занадто вологе повітря може сприяти росту плісняви та інших шкідливих організмів. Рекомендований діапазон вологості зазвичай становить від 40% до 60%.
- освітлення: правильне освітлення є важливим фактором для комфорту та безпеки в приміщенні. Натуральне освітлення, через вікна, є бажаним, але також необхідно забезпечити належне штучне освітлення в тих місцях, де недостатня кількість природного світла. Використання енергоефективних джерел світла та регульованої освітленості дозволяє підтримувати оптимальні умови.
- контроль якості повітря: санітарна оцінка якості повітря є важливою для виявлення наявності шкідливих речовин, таких як хімічні

забруднювачі, волокна, пил, грибки та бактерії. Регулярне проведення аналізу повітря та очищення його від шкідливих речовин сприяє забезпеченню здорового середовища.

Загальною метою цих заходів є створення оптимального мікроклімату в санітарно-побутових приміщеннях, який сприяє збереженню здоров'я та благополуччя людей. Правильна вентиляція, контроль температури, вологості та освітлення є ключовими елементами для досягнення цієї мети і варто надавати їм належну увагу при проектуванні та облаштуванні санітарно-побутових приміщень.

ВИСНОВКИ

В кваліфікаційній роботі було вивчено та досліджено використання технології OSINT для збору, узагальнення та аналізу інформації, зокрема на основі різних соціальних мереж. Основним завданням роботи було висвітлення проблематики, пов'язаної з важливістю соціальних мереж у процесі OSINT розвідки.

Під час виконання кваліфікаційної роботи було проведено докладне дослідження сучасного стану використання технології OSINT. Були розглянуті та опрацьовані популярні інструменти, що використовуються для збору та аналізу інформації в рамках OSINT розвідки, а також розроблений план проведення такої розвідки.

Для досягнення поставлених цілей, в рамках кваліфікаційної роботи було створено власний інструмент на мові програмування Python. Цей інструмент використовував API одного з відкритих сервісів для збору необхідної інформації. Також була проведена повноцінна OSINT розвідка, використовуючи популярні соціальні мережі та інші відкриті джерела, що дозволило отримати значну кількість цінної інформації.

Важливість теми використання технології OSINT для збору, узагальнення та аналізу інформації на основі соціальних мереж не може бути недооцінена. У сучасному цифровому світі, де соціальні мережі є неодмінною частиною життя багатьох людей, вони стають важливим джерелом відкритої інформації. Вони можуть надати унікальну інформацію та допомогти розуміти поведінку, інтереси та думки різних людей. Майбутнє у цій сфері виглядає дуже перспективним. З ростом кількості та розширенням функціоналу соціальних мереж з'являються нові можливості для збору та аналізу інформації. Вдосконалення алгоритмів та методів обробки даних, розвиток штучного інтелекту та машинного навчання дозволять зробити OSINT розвідку більш точною, швидкою і ефективною.

Таким чином, використання технології OSINT для збору, узагальнення та аналізу інформації на основі соціальних мереж має великий потенціал у багатьох сферах, включаючи безпеку, розвідку, бізнес-аналітику та громадську діяльність. Неперервний розвиток цієї технології та її поєднання з іншими інноваційними підходами відкривають шлях до нових можливостей і досягнень у майбутньому.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Sudhanshu Chauhan, Nutan Kumar Panda. Hacking Web Intelligence. 2015. c. 23

2. Sally Rumsey How to Find Information. A guide for researchers. SE. Open University Press. England. 2008. c. 223.

3. Vinny Troia. A Hacker’s Guide to Online Intelligence Gathering Tools and Techniques. 2020. c. 48

4. Michael Sankey. "The Manual to Online Public Records: The Researcher's Tool to Online Resources of Public Records and Public Information." 2016. c. 109

5. Robert David Steele. "The Open-Source Everything Manifesto: Transparency, Truth, and Trust." 2012. c. 59

6. Statista. Users worldwide visiting Reddit.com from April 2021 to April 2022. URL: https://www.statista.com/statistics/1310710/redditcom-monthly-users/

7. Statista. Forecast of the number of LinkedIn users in the World from 2017 to 2025. URL: https://www.statista.com/forecasts/1147197/linkedin-users-in-the-world

8. Statista. Number of monthly active Instagram users from 2013 to 2021. URL: https://www.statista.com/statistics/253577/number-of-monthly-active-instagram-users

9. Statista. Number of monthly active Facebook users worldwide as of 1st quarter 2023. URL: https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide

10. Statista. Number of Twitter users worldwide from 2019 to 2024. URL: https://www.statista.com/statistics/303681/twitter-users-worldwide/

11. Michael Bazzell. "Hiding from the Internet: Eliminating Personal Online Information." 2016. c. 23

12. Steve Weber. "The Success of Open Source." 2004. c. 89

13. Michael Bazzell. "Open Source Intelligence Techniques: Resources for Searching and Analyzing Online Information." 2020. с. 53

14. С.Б.Могильний. Методи та інструменти ділової розвідки в Internet. 2010. с. 197.

15. Michael Bazzell. Open Source Intelligence Techniques. Resources for Searching and Analyzing. Sixth Edition. 2018. с. 58

16. Brenda Jin, Saurabh Sahni, Amir Shevat. Designing Web APIs. 2018. с. 2

17. Babak Akhgar, P. Saskia Bayerl, Fraser Sampson. "Open Source Intelligence Investigation: From Strategy to Implementation." 2019. с. 25

18. Закон України «Про затвердження Порядку класифікації надзвичайних ситуацій за їх рівнями»

19. Зеркалов Д. В. Безпека життєдіяльності. Навчальний посібник. 2011. с. 263

20. Метеорологічні умови в приміщеннях URL: https://buklib.net/books/35226/

21. Національний стандарт України «ДСТУ-Н Б А.3.2.1:2007»

ДОДАТОК А

Лістинг функції пошуку даних за електронною поштою

```
import tweepy
import requests


# Встановлення доступу до Social Searcher API
social_searcher_api_key = '***'

# Функція для пошуку даних за електронною поштою за допомогою
Social Searcher API
def search_social_searcher_by_email(email):
    try:
        # Виконання запиту до Social Searcher API
        url                =                f"https://api.social-
searcher.com/v2/search?q={email}&key={social_searcher_api_key}&l
imit=10"
        response = requests.get(url)

        # Перевірка коду стану запиту
        if response.status_code == 200:
            # Отримання результатів пошуку
            results = response.json()["posts"]

            # Виведення результатів
            for result in results:
                print(f"Запис: {result['text']}")
                print("-------------------------------------")
        else:
            print("Помилка запиту до Social Searcher API")
    except requests.exceptions.RequestException as e:
        # Обробка помилок Social Searcher API
        print('Помилка Social Searcher API: ' + str(e))

# Функція для виконання OSINT розвідки за електронною поштою
def perform_osint_by_email(email):

    print('Пошук даних на Social Searcher за електронною поштою:')
    search_social_searcher_by_email(email)
    print('-------------------------------------')

# Приклад використання
email = input('Введіть електронну пошту для пошуку: ')

perform_osint_by_email(email)
```