Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ПОЯСНЮВАЛЬНА ЗАПИСКА

кваліфікаційної роботи магістра

галузь знань *12 Інформаційні технології*
(шифр і назва галузі знань)

спеціальність *125 Кібербезпека*
(код і назва спеціальності)

освітній ступень *магістр*

освітньо-наукова програма *Кібербезпека*
(назва освітньої програми)

на тему: «Система захисту на основі OSINT»

Виконавець: студент ІІ курсу, групи КБм-21

(підпис) **Денис КОРНЕЦЬКИЙ** (Ім'я, ПРІЗВИЩЕ)

	Ім'я, ПРІЗВИЩЕ	**Підпис**
Науковий керівник	Володимир НАКОНЕЧНИЙ	
Нормоконтроль	Олена БОГУСЛАВСЬКА	

Київ 2023

Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ЗАТВЕРДЖЕНО:
В.о. завідувача кафедри
кібербезпеки
та захисту інформації
_____ Сергій ТОЛЮПА
«24» жовтня 2022 р.

ЗАВДАННЯ
на виконання кваліфікаційної роботи

спеціальності *125 Кібербезпека*
(код і назва спеціальності)

освітній ступень *магістр*

Здобувача(ки) КБм-21 (група) Корнецького Дениса Станіславовича (прізвище ім'я по-батькові)

Тема кваліфікаційної роботи Система захисту на основі OSINT

1. ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Рішення засідання кафедри кібербезпеки та захисту інформації факультету інформаційних технологій протокол № 3 від 20.10.2022

2. МЕТА ТА ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Об'єкт досліджень	Процес визначення способу підвищення достовірності інформації отриманої за допомогою технологій OSINT.
Предмет досліджень	Технологія розвідки на основі відкритих джерел та способи підвищення достовірності інформації.
Мета	Досягнення підвищення достовірності інформації зібраної за допомогою інструментів розвідки на основі відкритих джерел.
Вихідні дані для проведення роботи	Методи виявлення ботів, технологія розвідки на основі відкритих джерел.

3. ОЧІКУВАНІ НАУКОВІ РЕЗУЛЬТАТИ

Наукова новизна удосконалення системи виявлення ботів серед інформації зібраної за допомогою розвідки на основі відкритих джерел.

Практична цінність підвищення достовірності інформації здобутої за допомогою технологій OSINT шляхом удосконалення системи виявлення ботів.

4. ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Робота виконана у повному обсязі відповідно до теми.

5. ЕТАПИ ВИКОНАННЯ РОБОТИ

Найменування етапів робіт	Строки виконання робіт (початок-кінець)
Розробка плану для досягнення мети роботи	24.10.2022 – 23.01.2023
Аналіз літературних джерел	24.01.2023 – 14.02.2023
Розробка пропозицій щодо підвищення достовірності інформації за допомогою технології розвідки на основі відкритих джерел	15.02.2023 – 24.04.2023
Оформлення і друк пояснювальної записки	25.04.2023 – 19.05.2023

6. РЕАЛІЗАЦІЯ РЕЗУЛЬТАТІВ ТА ЕФЕКТИВНІСТЬ

Економічний ефект Зниження збитків спричиненими ботами.

Соціальний ефект Підвищення ефективності виявлення ботів.

7. ДОДАТКОВІ ВИМОГИ

Завдання видав _____ Володимир НАКОНЕЧНИЙ
(підпис) (Ім’я, ПРІЗВИЩЕ)

Завдання прийняв до виконання _____ Денис КОРНЕЦЬКИЙ
(підпис) (Ім’я, ПРІЗВИЩЕ)

Дата видачі завдання: 24.10.2022 р.
Термін подання кваліфікаційної роботи до ЕК 19.05.2023 р.

УДК. 004.432.16

РЕФЕРАТ

Пояснювальна записка до кваліфікаційної роботи «Система захисту на основі OSINT»: 57 сторінок, 20 рисунків та 2 таблиці. 24 літературних джерела.

Актуальність теми: З урахуванням експансії російської федерації на території України стало надзвичайно актуальним питання отримання достовірної інформації з різних джерел, в тому числі і з відкритих. Інформація є дуже цінним ресурсом, тому можливість підвищити її достовірність під час використання інструментів розвідки на основі відкритих джерел є важливим в наші часи. Підвищення достовірності здобутої за допомогою технологій OSINT інформації буде мати позитивний вплив на інші сфери інформаційної розвідки.

Саме тому, актуальним науковим завданням, що має теоретичне та практичне значення є розробка рекомендацій щодо підвищення достовірності інформації отриманої за допомогою розвідки на основі відкритих джерел шляхом об’єднання двох API у систему виявлення ботів.

Об’єкт дослідження – процес визначення способу підвищення достовірності інформації отриманої за допомогою технологій OSINT.

Предмет дослідження – технологія розвідки на основі відкритих джерел та способи підвищення достовірності інформації.

Мета роботи – досягнення підвищення достовірності інформації зібраної за допомогою інструментів розвідки на основі відкритих джерел.

Методи дослідження – методи спостереження, аналізу, експерименту, порівняння об’єкту і предмету дослідження та дедукції.

У роботі проведено аналіз та досліджено базове поняття розвідки на основі відкритих джерел, розглянута структура та процес OSINT. Проведено аналіз переваг, недоліків та актуальних проблем дослідження розвідки на основі відкритих джерел.

Визначено та проаналізовано основні вимоги й загрози безпеки при використанні методу OSINT. Досліджено методи, якими підпорядковуються

інструменти інформаційної розвідки на основі відкритих джерел. Надано рекомендації щодо покращення достовірності інформації отриманої за допомогою розвідки на основі відкритих джерел шляхом об’єднання двох певних API у систему виявлення ботів.

Проведено експеримент в ході якого перевірено на наявність ботів тридцять IP-адрес взятих з різних відкритих чорних списків за допомогою API Focsec та API BotScout.

Здійснено розрахунок відсотку виявлених ботів на основі отриманих після перевірки даних. Проведено розрахунок ефективності запропонованого методу виявлення ботів в порівнянні з поодиноким використання розглянутих API.

Наукова новизна: удосконалено систему виявлення ботів серед інформації зібраної за допомогою розвідки на основі відкритих джерел. Дана методика з більшою ймовірністю виявляє бота серед інформації що перевіряється.

Ключові слова: розвідка, відкриті джерела, OSINT, виявлення ботів, достовірність.

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

API	–	Application Programming Interface
CMS	–	Content management system
CSV	–	Comma-Separated Values
DNS	–	Domain Name System
DoS	–	Denial of service
GeoIP	–	Geolocation Internet Protocol
HUMINT	–	Human intelligence
IMINT	–	Imagery intelligence
IoT	–	Internet of Things
IP	–	Internet Protocol
ISO	–	International Organization for Standardization
KML	–	Keyhole Markup Language
Mac OS	–	Macintosh Operating System
MASINT	–	Measurement and signature intelligence
OSD	–	Open source data
OSINF	–	Open source information
OSINT	–	Open source intelligence
OSINT-V	–	Validated OSINT
OVH	–	Online Virtual Hosting
PDF	–	Portable Document Format
RSS	–	Rich Site Summary
SIGINT	–	Signals intelligence
SQL	–	Structured Query Language
TECHINT	–	Technical Intelligence
VoIP	–	Voice over Internet Protocol
VPN	–	Virtual Private Network
АС	–	автоматизованої системи
ЕОМ	–	електронно-обчислювальна машина
ОС	–	операційна система
ШПЗ	–	шкідливе програмне забезпечення

ЗМІСТ

ВСТУП

З урахуванням експансії російської федерації на території України стало надзвичайно актуальним питання отримання достовірної інформації з різних джерел, в тому числі і з відкритих. Інформація є дуже цінним ресурсом, тому можливість підвищити її достовірність під час використання інструментів розвідки на основі відкритих джерел є важливим в наші часи. Підвищення достовірності здобутої за допомогою технологій OSINT інформації буде мати позитивний вплив на інші сфери інформаційної розвідки.

Саме тому, актуальним науковим завданням, що має теоретичне та практичне значення є розробка рекомендацій щодо підвищення достовірності інформації отриманої за допомогою розвідки на основі відкритих джерел шляхом об’єднання двох API у систему виявлення ботів.

Метою кваліфікаційної роботи є підвищення достовірності інформації зібраної за допомогою інструментів розвідки на основі відкритих джерел.

Для досягнення поставленої в кваліфікаційній роботі мети необхідно виконання конкретних завдань:

- провести аналіз та надати пропозиції щодо підвищення достовірності інформації отриманої за допомогою розвідки на основі відкритих джерел;
- здійснити пошук та провести відповідний аналіз відмінностей різних інтерфейсів прикладного програмування, їх переваг та недоліків;
- експериментально перевірити певну кількість IP-адрес взятих з різних відкритих чорних списків на наявність ботів;
- на основі отриманих у попередньому пункті даних здійснити розрахунок відсотку виявлених ботів;
- провести розрахунок ефективності запропонованого методу виявлення ботів у порівнянні з поодиноким використанням різних API.

Об’єктом дослідження – процес визначення способу підвищення достовірності інформації отриманої за допомогою технологій OSINT.

Предметом дослідження є технологія розвідки на основі відкритих джерел та способи підвищення достовірності інформації.

При вирішенні поставлених завдань у кваліфікаційній роботі використані методи: аналізу, спостереження, експерименту, порівняння об’єкту і предмету дослідження та дедукції.

Наукова новизна одержаних результатів:

- удосконалено систему виявлення ботів серед інформації зібраної за допомогою розвідки на основі відкритих джерел. Дана методика з більшою ймовірністю виявляє бота серед інформації що перевіряється.

Практична цінність роботи полягає в підвищенні достовірності інформації здобутої за допомогою технологій OSINT шляхом удосконалення системи виявлення ботів.

Основні наукові положення і результати роботи апробовані на VI Міжнародній науково-практичній конференції “Проблеми кібербезпеки інформаційно-телекомунікаційних систем” (PCSITS) (Київ, 2023).

РОЗДІЛ 1
АНАЛІЗ ПРОБЛЕМ КОПЦЕПЦІЇ ІНФОРМАЦІЙНОЇ РОЗВІДКИ НА ОСНОВІ ВІДКРИТИХ ДЖЕРЕЛ

1.1 Визначення технології OSINT

Як зазначали відомі класики: «Той хто володіє інформацією – володіє світом». І не просто так, бо інформація – це найцінніший ресурс, яким володіють люди, особливо в теперішні часи, коли наша країна вже більше року знаходиться в стані війни з російською федерацією. На сьогодні питання збору актуальної та несфальсифікованої ворогом інформації стоїть дуже гостро. Володіти достовірною інформацією під час воєнного стану дуже важливо для коректної координації своїх сил та контролю дій противника. І така актуальна й достовірна інформація потрібна постійно.

Особливо складно отримати достовірну інформацію з відкритих джерел, бо серед їх неосяжної кількості дуже важко виділити ту крихту надійних та цінних джерел. Кожен день мільйони людей в пошуках інформації стикаються з професійно спотвореними даними, які приймають за правду, що може призвести до непорозуміння або паніки, особливо під час війни.

Тому важливим і актуальним питанням залишається збір саме достовірних даних задля забезпечення контрдій проти сфальсифікованої інформації. Саме з цією метою і застосовується інформаційна розвідка.

Аналіз літературних джерел дає можливість побачити та проаналізувати існуючі методи інформаційної розвідки таблиця 1.1 [1].

В інформаційній розвідці, особливо в OSINT, напрям кібербезпеки грає не останню роль, так як зібрану даним методом інформацію можна порівняти з «двосічним мечем». Коли зібрана, розвідкою на основі відкритих джерел, інформація використовується в позитивному напрямку, то у даному випадку можна заздалегідь попереджувати загрози кібербезпеки та випадки кібертероризму в кіберпросторі. І це

не прості слова, бо згідно зі звітом відділу внутрішної розвідки США, використання інформації зібраної за допомогою OSINT позитивно вплинуло на загальну розвідку, завчасне попередження кіберінцидентів в кіберпростор та внутрішню боротьбу з тероризмом. Саме тому керування отриманою за допомогою розвідки на основі відкритих джерел інформацією дуже важливо для кібербезпеки [1].

Таблиця 1.1

Методи інформаційної розвідки

Метод	Опис
OSINT (Open source intelligence)	Збирає розвіддані використовуючи відкриту інформацію та програмне забезпечення. До відкритої інформації відноситься та до якої можна отримати доступ у повсякденному житті через Інтернет, радіомовлення, газети та журнали.
HUMINT (Human intelligence)	Інформація зібрана людьми (агентами) під час шпигунства або іншої діяльності. Агенти поділяються на: Білий агент: може збирати відкриту інформацію, але шпигунство заборонено. Чорний агент: таємно викрадає конфіденційну інформацію.
TECHINT (Technical Intelligence)	Інформація збирається за допомогою технологічних та інформаційних ресурсів та поділяється на такі підвиди розвідки: Imagery intelligence (IMINT): Збирає інформацію за допомогою БПЛА, літаків-розвідників, супутників та ін. Signals intelligence (SIGINT): Збирає проаналізовану інформацію з радіохвиль та сигналів радарів. Measurement and signature intelligence (MASINT): для збору інформації використовуються пристрої, що відмінні від IMINT та SIGINT.

З іншого боку, як було сказано раніше, даний метод це «двосічний меч» і дана аналогія пов’язана з негативним аспектом використання OSINT для збору інформації.

Цим методом зловмисники можуть збирати необхідну їм інформацію задля реалізації таких кіберзлочинів, як спам, впровадження шкідливого програмного забезпечення (ШПЗ), злом, Denial of service (DoS), фішинг, порушення прав цифрової власності, порушення конфіденційності та розповсюдження сфальсифікованої інформації.

Зазвичай більшість таких кіберзлочинів спричиняються з метою збагачення, але є і випадки виникнення загроз національного рівня безпеки, наприклад, порушення мережевих операцій чи підняття хибних політичних питань шляхом поширення сфальсифікованої інформації. Саме тому використання даного методу має бути обмежено законною діяльністю, а також підтримуванням базових вимог безпеки задля мінімізації збитків у випадку, якщо зловмисники спробують зловживати зібраною інформацію [2].

З огляду на вищезазначене, дамо визначення терміну OSINT. Це найпростіший та найдешевший метод збору інформації, що є як його перевагою так і недоліком. Даний метод розвідки користується формою збору даних через відкриті джерела та їх обробкою задля того, щоб знайти відповідь на конкретне поставлене питання.

Використання відкритої інформації забезпечує певні переваги, наприклад, інформація збирається в режимі реального часу, доступ до даних простий, і їх збір не вимагає великих витрат. Однак актуальність та своєчасність зібраної інформації цим методом може бути нижча, ніж збір даних іншими методами збору інформації. Проте, збір даних саме цим методом може стати вирішальним в конкретні моменти часу доповнюючи інформацію зібрану іншими методами розвідки [3].

OSINT – це інформаційна розвідка на основі відкритих джерел. Дана технологія є частиною загального процесу під час якого будь-хто може збирати, аналізувати дані з відкритих джерел та перетворювати їх у необхідну для розвідки інформацію. Перш ніж досліджувати саму технологію OSINT необхідно визначити з чого вона складається [4]:

- Розвідка. Даний процес більшою мірою стосується зібраних, оброблених та зведених даних для отримання необхідної інформації.
- Дані з відкритих джерел або open source data (OSD). Складаються з необроблених загальних даних. Наприклад, зображення, фотографії, дані опитувань, аудіодані, метадані та набори даних, які можна отримати із загальнодоступної інформації.
- Інформація з відкритих джерел або open source information (OSINF). Відноситься до загальних даних, які були частково відфільтровані на основі вимог чи певних критеріїв. Наприклад, книги, статті та документи написані на певні теми і т.п. Ця інформація є результатом збору та обробки даних відповідно до призначення інструменту OSINT. Без інформації з відкритих джерел не існувало б і технології, тому це дуже важлива її частина.
- Розвідка на основі відкритих джерел або open source intelligence (OSINT). Дана частина технології стосується обробленої, через відкриті джерела, інформації. У деталях представляє собою результат задоволення певного запиту розвідки під час якого було зібрано, оброблено та скомпоновано інформацію з відкритих джерел. Отримана інформація безпосередньо використовується у всіх контекстах розвідки, а великий об’єм даних підсумовується, сортується та виводиться для інструментів OSINT.
- Підтверджений OSINT або validated OSINT (OSINT-V). Представляє собою OSINT з високим рівнем достовірності. Отримана інформація повинна бути перевірена за допомогою авторитетного джерела OSINT або того, що не входить до OSINT. Перевірка необхідна, тому що деякі зловмисники втручаються в аналіз, створюють неточну або недостовірну інформацію та розповсюджують її [4].

Процес розвідки на основі відкритих джерел складається зі збору, обробки, аналізу даних та створення звітів із корисною інформаціє відповідно до поставленого завдання. Оскільки вимоги до OSINT варіюються від однієї організації до іншої, тому кожна компанія має модифіковану структуру OSINT відповідно до своїх цілей та вимог.

Тим не менш базовий процес розвідки (рис. 1.1) на основі відкритих джерел складається з п’яти кроків, які можна побачити на рисунку 1.2 [1].

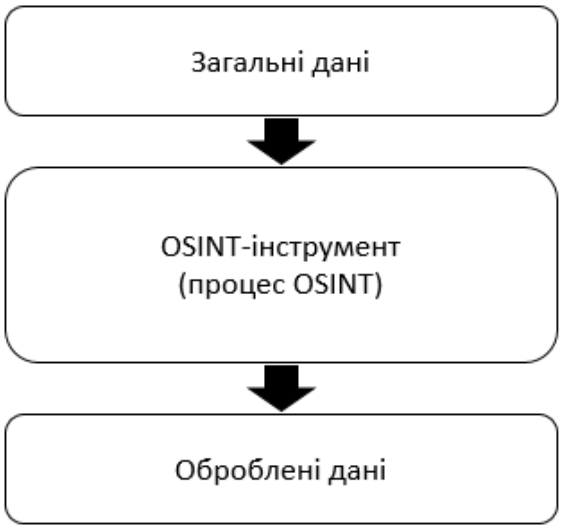

Рисунок 1.1 – Процес роботи OSINT

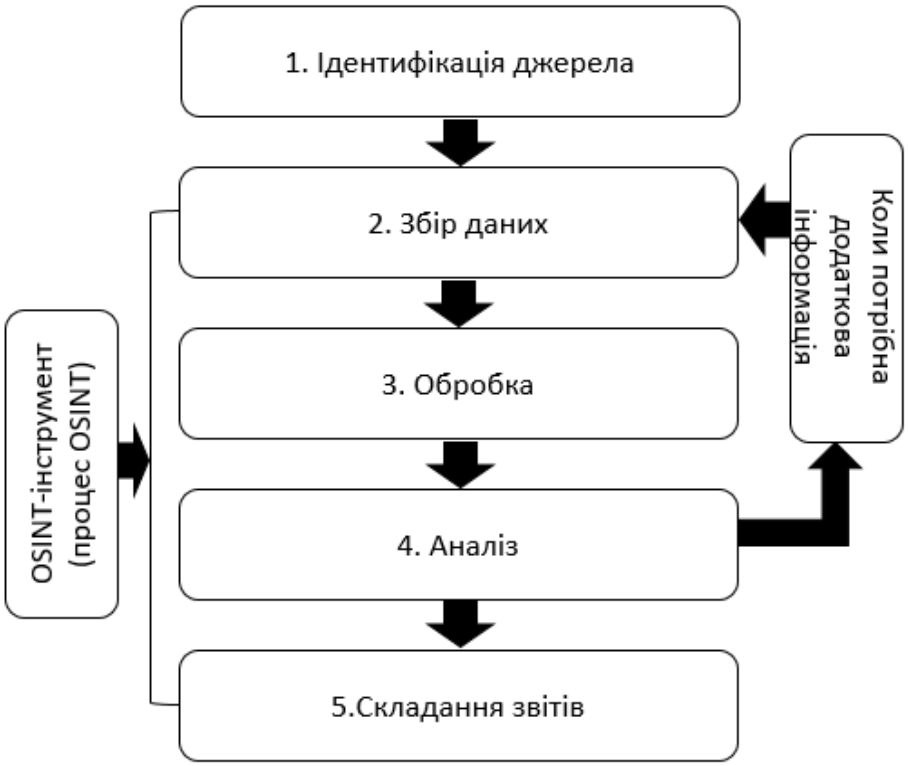

Рисунок 1.2 – Структура OSINT

Крок перший. *Ідентифікація джерела*. Визначення інформації, яку необхідно отримати, за допомогою розвідки на основі відкритих джерел, серед множини даних.

Крок другий. *Збір даних*. На даному етапі необхідно отримати інформацію з визначеного джерела. Збір даних поділяється на два типи, а саме пасивний та активний. Під час активного збору інформації використовуються програми та скрипти для пошуку необхідних даних. Пасивний збір інформації виконується за допомогою Google, Netcraft, Whois, Recon-NG, Shodan і т.д.

Крок третій. *Обробка*. На цьому етапі отримана інформація у другому кроці обробляється та уточнюється з метою виділення необхідних даних для відповіді на поставлене перед розвідкою питання. Так як на другому кроці отримується багато інформації, то на етапі обробки важливо профільтрувати ці дані. Окрім того, важливо враховувати зв'язок між інформацією, що є доволі складним завданням, яке потребує великого досвіду та необхідного образу мислення.

Крок четвертий. *Аналіз*. Дані, що уточнені на третьому етапі, обробляються відповідно до поставленого перед розвідкою питання. Тобто, якщо виникають сумніви щодо знайденої інформації, шукається додаткова інформація для їх спростування та пітвердження вірності оброблених даних. Тому в разі виникнення потреби у додатковій інформації на етапі аналізу, етапи збору та обробки даних постійно повторюються, щоб знайти зв'язок між інформацією для отримання необхідної для розвідки інформації.

Крок п’ятий. *Складання звітів*. Представляє собою процес підсумовування змісту четвертого кроку та запис його у формі звіту. В звітах знаходяться усі вихідні дані, які вказують на їх точність задля надання достовірності інформації. В результаті більшість загальних даних перетворюється в інформацію, що відповідна критеріям, які встановлені дослідником [1,5].

1.2 Аналіз переваг, недоліків та актуальних проблем дослідження технології OSINT

Переваги використання OSINT [6,7]:

- Швидкий збір інформації в режимі реального часу. За допомогою OSINT інформація швидко знаходиться та збирається з відкритих джерел з урахуванням постійних змін у режимі реального часу. Щоб отримати потрібні дані, користувач шукає їх покладаючись на різну інформацію з відкритих джерел, таку як пошук даних в Інтернеті, перегляд YouTube/TV та читання книг, а не збір інформації з одного місця. Перевага даного методу полягає у забезпеченні швидкого доступу до даних.
- Безпечний збір великої кількості даних. За допомогою агентурної розвідки (HUMINT) збирається небагато даних, тому що джерел інформації набагато менше ніж при використанні OSINT, а ризиків в рази більше. В свою чергу при використанні розвідки на основі відкритих джерел, відповіді на необхідні питання знаходяться безпечніше. Крім того, оскільки OSINF є доступним для всіх, він є законним. За рахунок цього з’являється перевага, що виражена низьким ризиком з точки зору безпеки для користувача даного методу розвідки.
- Достовірність джерел інформації. При застосуванні агентурної розвідки (HUMINT) достовірність отриманих даних сумнівна, оскільки джерело інформації через, яке отримує дані агент може визивати питання. В свою чергу інформація, що зібрана за допомогою OSINT забезпечує достовірність, оскільки ясність відкритих джерел гарантується процесом його перевірки на надійність.
- Зручність та простота доступу. Через те, що не кожен може легко отримати доступ до необхідної інформації, бо права доступу до неї можуть бути встановлені таким чином, що лише авторизовані користувачі можуть отримати доступ до конфіденційних та якісних даних. Перевага розвідки на основі відкритих джерел в тому, що будь-хто може легко отримати доступ до інформації, зібраної з допомогою OSINT та зручно використовувати дані відповідно до вимог користувача.
- Низька вартість. OSINT має перевагу отримання даних за низькою ціною порівняно з вартістю навчання агентів у HUMINT та вартістю збору даних з

використанням найновішого обладнання, такого як супутники та безпілотні літальні апарати, які використовуються у технічній розвідці (TECHINT).

Недоліки використання OSINT [6,7]:

- Дуже великий об’єм інформації. Чим більше інформації в користувача, тим складніше йому вишукувати достовірні дані за допомогою OSINT. В наші часи більша частина даних отримується з відкритих джерел, тому потрібен час та зусилля, щоб виявляти неправдиву інформацію та вибирати достовірну.
- Забобони спецслужб. В організаційній культурі спецслужб цінність даних, зібраних OSINT, недооцінюється, а їх важливість не враховується, тому що будь-хто може отримати доступ до даних та використати їх.
- Проблеми безпеки та технічні обмеження. Спецслужби використовують внутрішні комп'ютерні мережі через проблеми з безпекою, які обмежують використання даних з відкритих джерел (OSD) в Інтернеті. У результаті аналітики спецслужб виявляють пасивне ставлення до використання даних OSINT. Експерти з комп'ютерної безпеки намагаються підготувати методи вільного використання OSD під час вирішення проблем безпеки.
- Фундамент для кіберзлочинів у разі неправомірного використання. Фактор того, що будь-хто може отримати доступ до даних, зібраних методом OSINT, є як його перевагою так і великим недоліком. Цей недолік призводить до того, що дані, зібрані за допомогою OSINT, можуть стати основою для кіберзлочинів. Тому потрібні дослідження заходів безпеки та технологій, які можуть мінімізувати шкоду від кіберзлочинів, навіть якщо користувачі використовують дані OSINT у зловмисних цілях.

Актуальні проблеми досліджень технології OSINT [8, 9]:

- Проблеми з ефективною та надійною фільтрацією інформації. Для отримання даних, які потрібні користувачу від OSINT, необхідно збирати та ефективно обробляти велику кількість інформації. Залежно від обсягу даних розвідка на основі відкритих джерел споживає величезну кількість часу та людських ресурсів. Організації та користувачі використовують інструменти автоматизації для фільтрації даних для підвищення ефективного збору інформації щодо необхідних питань. Тим

не менш, точність і надійність отриманих даних, у разі наявності програмних дефектів у інструментів автоматизації, є сумнівними. Отже, важливо безперервно перевіряти інструмент автоматизації, який є стандартом для фільтрації даних, та необхідно дослідження перевірки вилучених даних. Це залишається проблемою для користувачів, які збирають та фільтрують дані за допомогою OSINT.

- Проблеми з достовірністю інформації. Надійність зібраних даних є критичною проблемою користувачів, які використовують дані OSINT. Зокрема, перевірка джерел на достовірність отриманих даних під час процесу OSINT значно підвищує надійність інформації. Однак у разі отримання даних OSINT незаконними засобами користувач може навмисно відмовитися або приховувати важливі джерела, проте не існує контрзаходів для OSINT. Важливо вести облік джерел на яких буде ґрунтуватися достовірність інформації отриманої з OSINT у майбутньому. Завдяки цьому користувачі зможуть ефективно забезпечити прозорість даних, але дослідження з цього приводу досі залишаються проблемою. Це також потребує інтеграції та співпраці багатьох інструментів OSINT для забезпечення надійності та прозорості даних.
- Відсутність перевірки процедур забезпечення конфіденційності. Багато компаній, таких як Facebook та Google, збирають багато даних користувачів для комерційної розвідки [8]. Дані, які були зібрані в Інтернеті, включають не лише загальні дані, що створені користувачами, а й конфіденційну інформацію, таку як імена, дні народження, адреси та номери паспортів. Багато компаній повідомляють, що вони збирають та забезпечують анонімізацію інформації, щоб виправдати збір даних, проте невідомо, чи правильно це робиться. Це схоже на проблему забезпечення конфіденційності, яка може виникнути під час збору даних в залежності від мети інструменту OSINT. Завжди будуть виникати сумніви щодо надійності обробки даних способами, що забезпечують анонімність задля збереження конфіденційності інформації. Таким чином, дослідження з перевірки процедур управління конфіденційністю в даних OSINT, як і раніше, залишаються проблемою. З юридичної точки зору, OSINT має використовувати дані звертаючи увагу на політику захисту інформації відповідно до закону [8,9].

1.3 Аналіз загальних вимог та загроз безпеки технології OSINT

Вимоги OSINT варіюються залежно від мети, організації та даних, які мають бути отримані за допомогою розвідки на основі відкритих джерел. Дані, оброблені інструментом OSINT використовуються, аналізуються та зберігаються в його базі даних.

До вимог OSINT відносяться аспекти збору/зберігання даних і отримання доступу та використання зібраних даних. Користувачі, які збирають та зберігають дані за допомогою інструментів OSINT, в основному повинні забезпечувати контроль даних, їх цілісність та надійність.

Контроль даних. В наш час даний процес є важливим елементом під час пошуку необхідної інформації серед необ'ємної кількості даних. Метою контролю даних є пошук інформації, забезпечення її якості та цінності задля повторного використання і збереження. У минулому даний процес забезпечувався лише збором інформації. В останні роки для підвищення якості інформації дані обробляються за допомогою їх глибокого аналізу та машинно навченого штучного інтелекту. Ця вимога важлива для користувачів OSINT, що збирають загальнодоступні дані та перетворюють їх у цінну інформацію.

Гарантія цілісності даних. Під час зберігання зібраних даних у сховищі інструменту OSINT має бути забезпечена цілісність даних. Під цілісністю тут розуміється забезпечення точності даних і те, що зібрана інформація не повинна бути модифікована ким-небудь без дозволу. Якщо хтось отримує доступ до даних та змінює їх у відкритому просторі, то надійність такої інформації може бути скомпрометована. Крім того, користувачі можуть отримувати та розповсюджувати фальшиву інформацію, яка є фундаментом для кіберзлочинів, таких як фальсифіковані новини. Таким чином, гарантія цілісності даних є важливою вимогою у процесі розвідки на основі відкритих джерел.

Гарантія надійності. Надійність даних є важливим елементом, коли користувачі використовують зібрану інформацію. Задля гарантії надійності інформації потрібно перевірити цілісність та достовірність джерела даних. Зазвичай

процес перевірки джерел виконувався за допомогою процесу OSINT, а забезпечення гарантії достовірності та цілісності відкритих джерел даних завжди були важливими вимогами підвищення надійності даних.

Нажаль більшість інструментів OSINT не враховують вимоги, необхідні для доступу до збережених даних та їх використання. З цього виходить, що зібрану інформацію може використовувати будь-хто. Саме тут випливає проблема інформаційної безпеки через те, що користувачі OSINT могли випадково розкрити конфіденційну інформацію в Інтернеті. У випадку, якщо конфіденційна інформація була розкрита, то будь-хто може отримати доступ до цих даних та використати їх, як передбачає саме поняття розвідки на основі відкритих джерел.

Тому важливо використовувати дані з етичної точки зору, що під собою розуміється дотримання правил, які визначають дозволені дії чи належну поведінку. Якщо казати простіше, то отримана за допомогою інформаційної розвідки на основі відкритих джерел інформація має використовуватися в законних, а не зловмисних цілях. Через те, що деякі користувачі не дотримуються етичного відношення щодо отриманої інформації, виникають підстави для скоєння різного роду кіберзлочинів [1,10,11].

Загрозу безпеки технології OSINT представляють розповсюдження інформації, порушення конфіденційності, фальсифікація та зміна даних, що призводить до виникнення кіберзлочинів. Ці загрози можуть призвести до виникнення таких кіберзлочинів, як злом, втрата даних, атака відмови в обслуговуванні, розповсюдження вірусів та сфальсифікованих новин. Оскільки кожен має доступ до інформації, то зловмисник може отримати доступ до збережених даних.

Отримана інформація може бути розповсюджена та стати фундаментом для поширення вірусів і т.п. Зловмисники також можуть сфальсифікувати дані, щоб надавати користувачам неточну інформацію або розповсюджувати підроблені новини для створення плутанини.

Крім того, великою проблемою є загроза безпеки пов'язана з відкритими джерелами, а саме занепокоєння користувачами порушенням конфіденційності їх інформації в епоху Інтернету. Щоденно люди використовують Інтернет для різних

цілей, включаючи збір даних, аналіз та спілкування тощо. Платформи соціальних мереж, такі як Facebook і Instagram, що також використовуються в цих цілях не можуть забезпечити необхідний рівень захисту від зловмисників. Дана ситуація призвела до зменшення суспільної довіри до збереження конфіденційності інформації. Проблема в тому, що компанії збирають конфіденційні дані користувачів, переважною мірою, без їх відома. Нажаль, конфіденційну інформацію збирати не перестануть, тому дуже важливим є покрашення її безпеки. А для покращення безпеки конфіденційних даних необхідно розуміти з якими загрозами безпеки треба боротись, а саме [1]:

- Розповсюдження інформації. У випадку, якщо не забезпечено конфіденційність інформації, то зловмисники можуть отримати доступ до неї та за її допомогою реалізувати різні загрози безпеки, такі як пошкодження або видалення даних. Зібрана за допомогою розвідки на основі відкритих джерел інформація може змінюватись залежно від організації та галузі застосування, і у разі її видалення може призвести до нестачі інформації, коли вона буде необхідна. У фінансовій галузі зловмисник може використовувати зібрані дані для отримання особистої, фінансової інформації. Все це може призвести до виникнення кіберзлочинів метою яких буде отримання грошових прибутків за рахунок крадіжки конфіденційної або фінансової інформації. Якщо інформація зібрана за допомогою розвідки на основі відкритих джерел є чутливою та важливою, то необхідно забезпечити її конфіденційність й цілісність, а також впровадити автентифікацію користувачів і контроль доступу до неї. Впровадження базового резервного копіювання та відновлення інформації зібраної за допомогою OSINT є обов’язковим.
- Порушення конфіденційності даних. У випадку, якщо зловмисник знайде особисті дані користувачів серед зібраної розвідкою на основі відкритих джерел інформації, то вони можуть стати фундаментом для безлічі різних загроз безпеки. Витік особистої інформації сам по собі призводить до збитків, однак завжди є можливість додаткової шкоди. Наприклад, зловмисник встановив цілі атаки на основі особистої інформації користувачів та атакував їх, розповсюджуючи віруси або шкідливі програми. Саме тому для поліпшення безпеки необхідні додаткові способи

її забезпечення. Гарним прикладом є анонімізація користувачів задля збереження конфіденційності інформації, що зібрана за допомогою розвідки на основі відкритих джерел.

- Фальсифікація та зміна інформації. В даному випадку зловмисниками підроблюється або змінюється зібрана за допомогою розвідки на основі відкритих джерел інформація. Неправомірна модифікація інформації може призвести до неправильного сприйняття видозмінених даних користувачами, що в свою чергу може призвести до непорозуміння. Яскравим прикладом цього є сфальсифіковані новини, які швидко розповсюджуються серед користувачів соціальних мереж. В результаті користувачі будуть збентежені достовірністю інформації через, що можуть виникнути сумніви щодо надійності джерела її розповсюдження. Саме тому необхідно забезпечити додаткові вимоги до безпеки задля збереження цілісності даних та гарантування достовірності джерел інформації, щоб швидко реагувати на фальсифікацію та зміну даних зібраних за допомогою розвідки на основі відкритих джерел.

Отже, враховуючи вищезазначене в OSINT необхідні додаткові вимоги безпеки для боротьби з кіберзлочинами та попередження інших загроз. Якщо зібрана за допомогою розвідки на основі відкритих джерел інформація має високу цінність, то впровадження системи автентифікації користувачів та забезпечення контролю доступу до неї може підвищити її безпеку. Впровадження даних вимог приведе до зменшення загроз безпеці інформації, що зібрана за допомогою OSINT. Таким чином зловмисники не зможуть викрадати, модифікувати та фальсифікувати дані непомітно [1, 12, 13].

Висновки до першого розділу

В даному розділі досліджено базове поняття розвідки на основі відкритих джерел, розглянута структура та процес OSINT. Проведений аналіз переваг, недоліків та актуальних проблем дослідження розвідки на основі відкритих джерел.

До переваг розвідки на основі відкритих джерел відносяться:

- швидкий збір інформації в режимі реального часу;

- безпечний збір великої кількості даних;
- достовірність джерел інформації;
- зручність та простота доступу;
- низька ціна.

До недоліків розвідки на основі відкритих джерел відносяться:

- достатньо великий об’єм інформації, що потребує для її обробки багато сил та ресурсів;
- скептичне ставлення відповідних спецслужб до отриманої даним методом інформації;
- проблеми безпеки та технічні обмеження;
- зібрана даним методом інформація може стати фундаментом для кіберзлочинів.

До актуальних проблем досліджень методу OSINT відносяться:

- проблеми з ефективною та надійною фільтрацією інформації;
- проблеми з достовірністю інформації;
- відсутність перевірки процедур забезпечення конфіденційності.

Крім того, в даному розділі визначені та проаналізовані основні вимоги та загрози безпеки при використанні методу OSINT.

РОЗДІЛ 2
ДОСЛІДЖЕННЯ МЕТОДІВ ТА ТЕХНОЛОГІЙ ІНФОРМАЦІЙНОЇ РОЗВІДКИ НА ОСНОВІ ВІДКРИТИХ ДЖЕРЕЛ

2.1 Дослідження методів та технологій OSINT

В сучасному інформаційному світі можна знайти відповідь на практично любе питання. Але яка достовірність і правдивість цієї інформації? Це питання було, є і буде актуальним поки існує людство. В необ'ємному просторі Інтернету циркулює величезний потік різноманітних даних, які можуть бути використанні при інформаційній розвідці на основі аналізу відкритих джерел для відповіді на поставлені питання. На основі обробки цих даних створено багато взаємопов'язаних методів збору інформації, які являються ключовою частиною роботи будь-якого інструменту OSINT.

До таких методів відносять пошук [9]:

- за реальним ім'ям;
- за електронною адресою;
- за ім'ям користувача веб-додатка;
- у соціальних мережах;
- за місцезнаходженням;
- за Internet Protocol (IP-адресою);
- за доменним ім'ям;
- використання сучасних пошукових систем.

Приклад взаємопов'язаності зазначених методів інформаційної розвідки на основі відкрити джерел можна побачити на рис.2.1-2.4 [9].

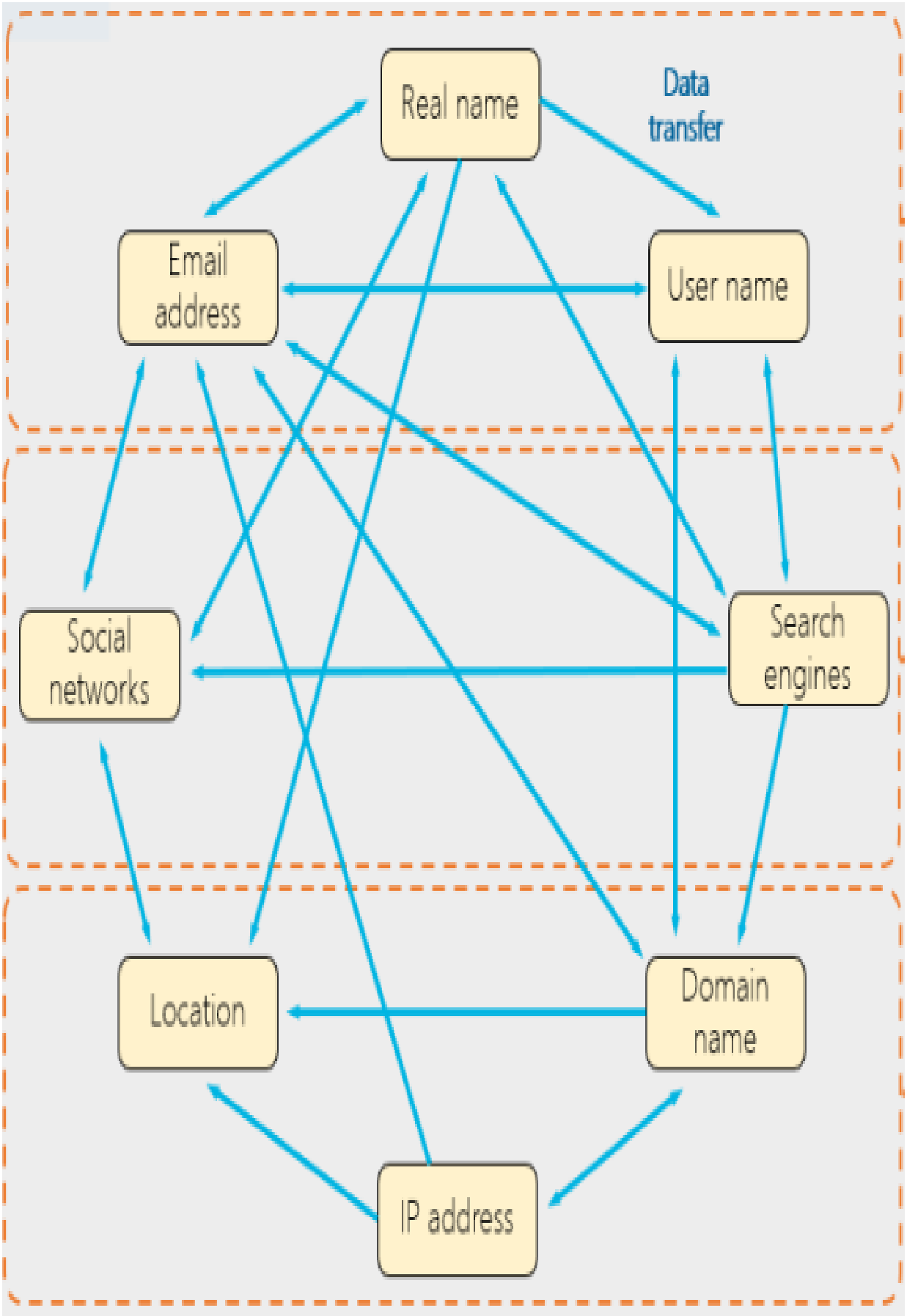

Рисунок 2.1 – Взаємозв’язок методів OSINT

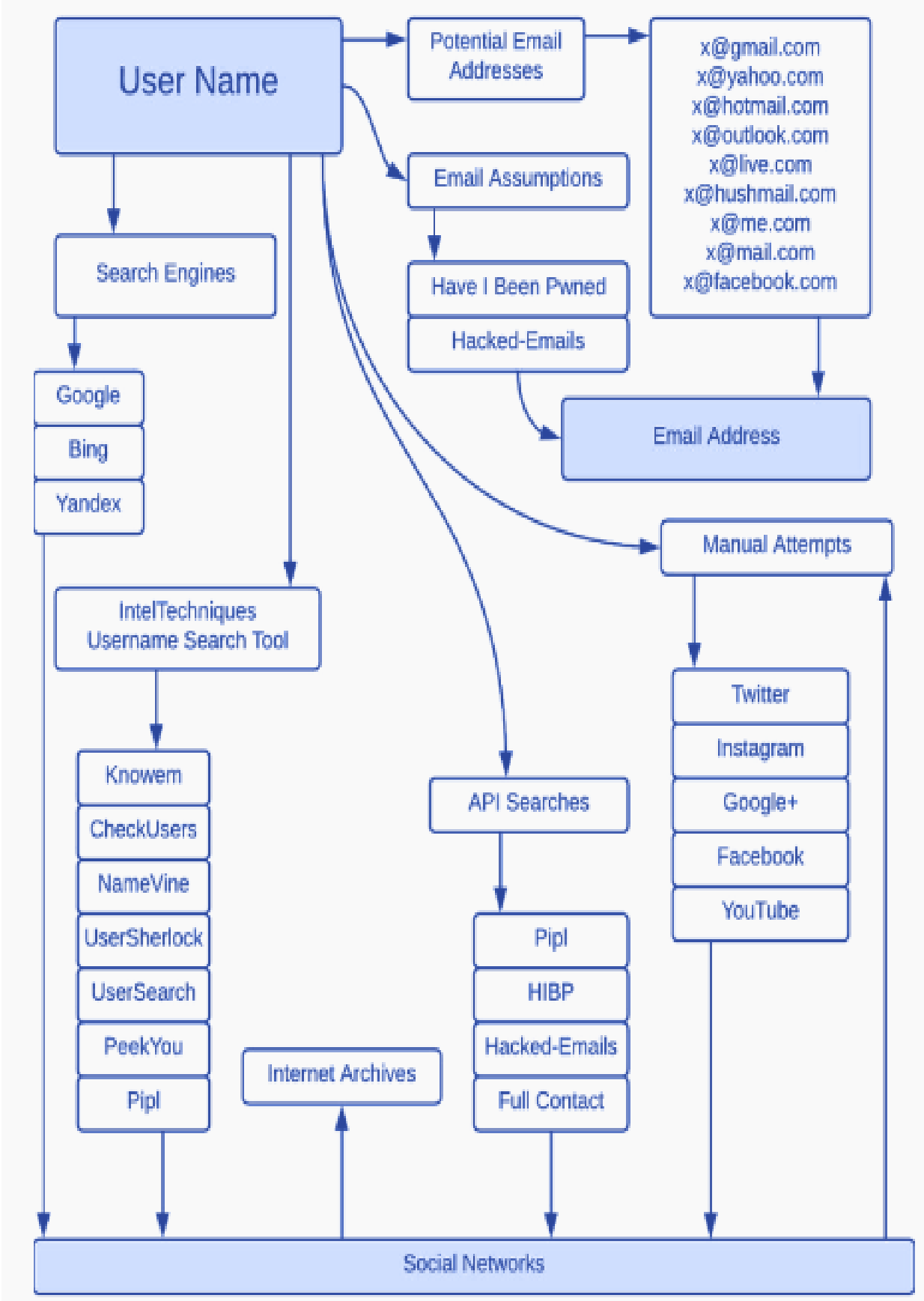

Рисунок 2.2 – Взаємозв’язок методів OSINT

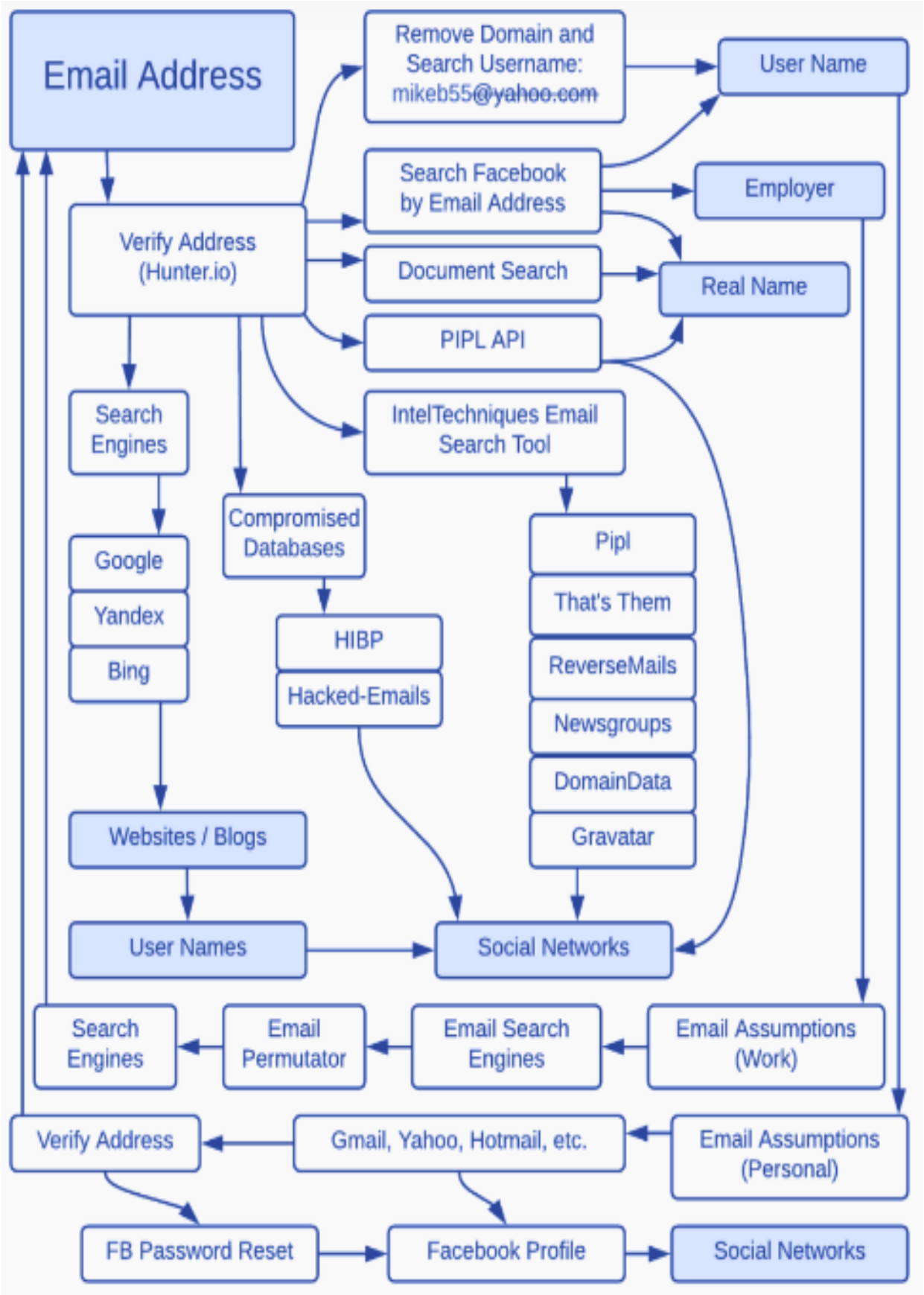

Рисунок 2.3 – Взаємозв’язок методів OSINT

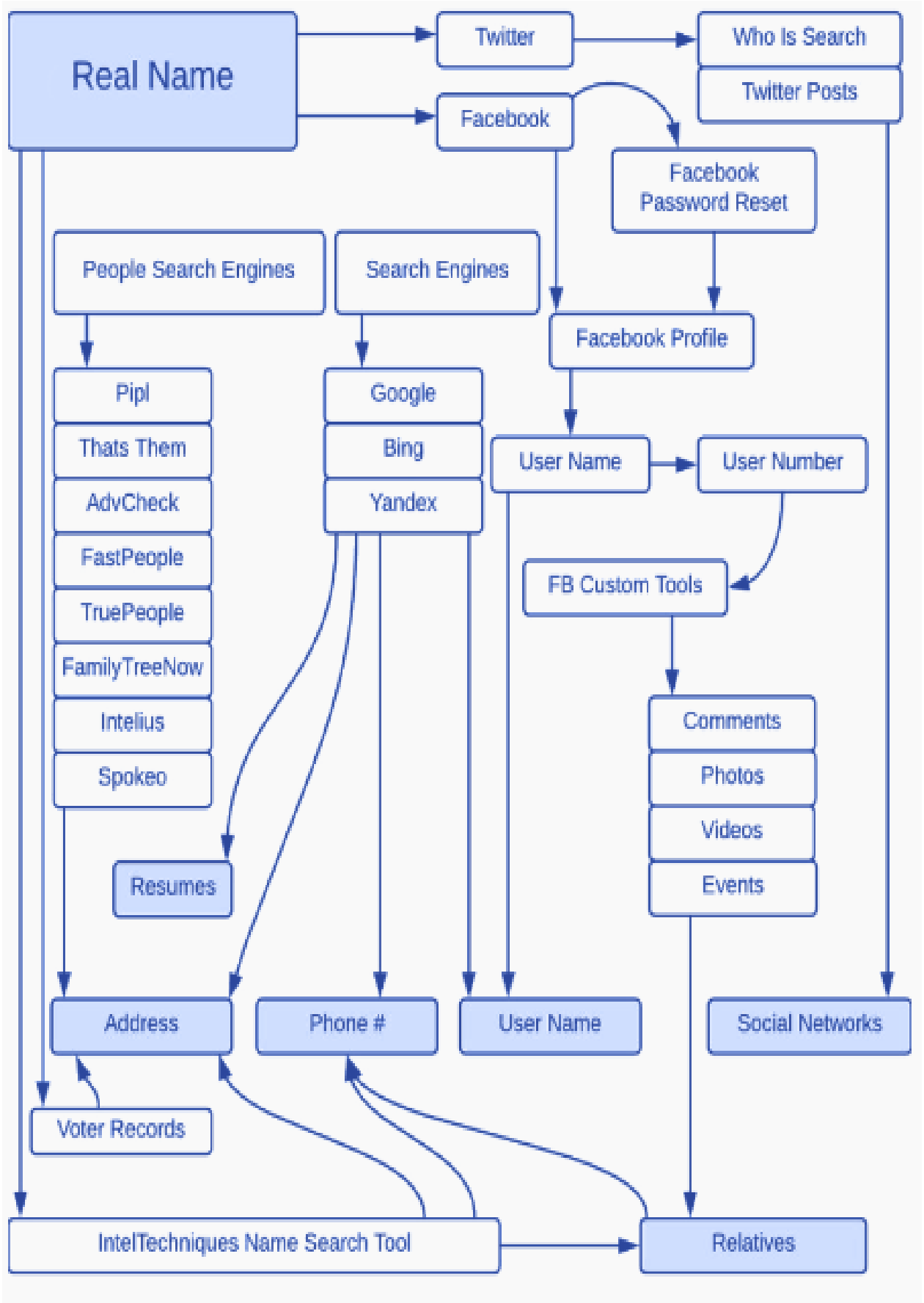

Рисунок 2.4 – Взаємозв’язок методів OSINT

При використанні даних методів інструментами розвідки на основі відкритих джерел отримуються такі дані [9]:

- Персональна інформація, а саме електронна адреса, реальне ім’я, ім’я користувача веб-додатку, вік, резюме, телефон, місто, країна, освіта, професійна кар’єра.
- Організаційна інформація, а саме доменне ім’я, місцезнаходження, файли, фотографії, GPS-координати, вейбсайт та дані про компанію.
- Мережева інформація, а саме субдомени, IP-адреси, ім’я хоста, Domain Name System (DNS) записи, регістраційна інфомація та дані операційної системи (ОС).

Завдяки інструментам OSINT при обороці знайдених даних можна потенційно знайти таку інформацію щодо об’єкта розвідки [9]:

- про економічну ситуацію;
- з політичним, сексуальним або релігійним контекстом;
- про родичів;
- щодо тенденції певних злочинів;
- деанонімізувати чиюсь інформацію;
- закешовану інформацію;
- докази злочинів;
- щодо активності у мережі;
- інформація щодо відвідуваних місць;
- інформацію про топологію мережів.

2.2 Дослідження провідних інструментів OSINT

Інструменти та методи OSINT є поширеними в кібербезпеці, де вони використовуються для ідентифікації зовнішніх потоків або для етичного злому та тестування на проникнення.

Правоохоронні органи, приватні детективи та журналісти також використовують ті самі методи, щоб дізнатися більше про злочин, підозрілу організацію чи зацікавлену особу.

Таким же чином рекрутери можуть шукати потенційних кандидатів, перевіряючи біографічні дані у каталогах з відкритих джерел.

Команди з маркетингу та продажу можуть використовувати інструменти OSINT, коли їм потрібно налаштувати націлювання для певного користувача або просто перевірити, чи є електронна адреса дійсною.

На жаль, слід також визнати, що шахраї та злочинці можуть використовувати однакові інструменти та методи для експлойтів. Наприклад, при створенні синтетичного ідентифікатора шахрай може поєднувати дані, отримані на торговій платформі в Darknet, і поєднувати їх з даними, отриманими з публічних записів [14].

З усього вищезазначеного можна стверджувати те, що інструменти інформаційної розвідки, на основі відритих джерел, значною мірою відрізняються за методами і цілями тривіальному збору інформації. Тим не менш серед великої кількості різноманітних інструментів є і такі, що виділяються своєю більшою популярністю серед розвідників інформаційних джерел. До них відносяться такі представники розвідки на основі відкритих джерел [14-20]:

1. Maltego – це додаток написаний на Java, який спрощує та прискорює розслідування завдяки доступу до баз даних та інструментів візуалізації.

Незалежно від того, чи перебуваєте ви в галузі довіри та безпеки, правоохоронних органів чи кібербезпеки, даний інструмент дозволяє проводити розслідування одним клацанням миші, які дають прості результати для розуміння.

Maltego дозволяє переглядати до 1 мільйона об'єктів на графіку з доступом до 58 джерел даних. Також можна підключити власні загальнодоступні бази даних та завантажувати джерела інформації вручну.

Як тільки вся інформація завантажується в програму, то можна обирати різні моделі візуалізації, такі як блоки, ієрархічні або кругові діаграми для налаштування графіків.

Переваги Maltego [14, 15]:

- чудовий інструмент візуалізації графіків;
- кілька варіантів візуалізації даних;
- створює мапу даних;
- ідеально підходить для відображення складних мереж та взаємозв’язків.

Недоліки Maltego [14]:

- додаток тільки для Java;
- застарілий інтерфейс.

Алгоритм роботи Maltego відображено на рисунку 2.5.

Рисунок 2.5 – Алгоритм роботи інструменту Maltego

2. SEON – інструмент для запобігання шахрайству, який перевіряє понад 50 соціальних та онлайн-сигналів. Ці перевірки базуються на електронній адресі, IP-адресі або номері телефону. Даною технологією зазвичай користуються при бажанні отримати більше інформації про людей не задаючи питання, що цікавлять напряму [14].

В наші часи підтвердження чужої особистості шляхом перевірки пов’язаних облікових записів соціальних мереж та онлайн-платформ є дуже популярним методом через те, що [14]:

- цей спосіб допомагає зібрати цифровий слід користувача;
- він може допомогти зробити уявлення про чужу соціально-економічну ситуацію навіть на ринках, де фінансової інформації недостатньо;
- соціальні мережі, що пов’язані з користувачем, також можуть більше розкрити його особистість.

Переваги SEON [14]:

- збирає інформацію в соціальних мережах;
- забезпечена масштабованість завдяки запитам Application Programming Interface (API);
- отримання результатів розвідки в режимі реального часу;
- доповнює дані на основі адреси електронної пошти, номера телефону або IP-адреси;
- додаткові перевірки швидкості, поведінки, видалення відбитків пристрою.

Недоліки SEON [14, 15]:

- він зосереджений на клієнті, тому йому не вистачає криміналістичних елементів;
- відсутній безкоштовний доступ до API.

3. Lampyre – це платна програма, розроблена спеціально для OSINT. Особливо корисна для розвідки кіберзагроз, аналізу злочинів та фінансової аналітики [16].

Ключова перевага Lampyre полягає в тому, що це програма за одним клацанням миші. Потрібно задати тільки вектор пошуку, такий як реєстраційний номер компанії, повне ім’я або номер телефону, і Lampyre проаналізує величезну кількість даних для отримання цікавої інформації для розвідника.

Lampyre автоматично обробляє більше 100 регулярно оновлених джерел даних, і, якщо необхідно, можна отримати доступ до них через програмне забезпечення або API.

При використанні даної технології важливо звернути увагу на те що, як і у випадку застосування інших інструментів OSINT необхідно перевірити, чи дійсно бази даних є справді джерелами з відкритою інформацією.

Lampyre може автоматизувати пошук, але розвіднику все одно доведеться подвоїти перевірку, звідки надходить інформація, а також, хто її надає.

Переваги Lampyre [14, 16]:

- відмінно підходить для кібербезпеки;
- збір даних з більш ніж 100 джерел;
- має доступ до більш ніж 100 постійно оновлюваних джерел;
- можливість отримати необхідну інформацію в один клік без реєстрації та додаткових витрат;
- можливість одночасно працювати з даними на карті, таблиці та графіку.

Недоліки Lampyre [14]:

- Lampyre – це не найінтуїтивніше програмне забезпечення для використання.

4. Google Dorks. Системи пошуку, такі як Google, Bing або DuckDuckGo, є досить поширеними безкоштовними інструментами OSINT, але тільки, якщо знати, як використовувати розширені фільтри.

Протягом багатьох років талановиті дослідники навчилися реконструювати пошукові системи. Цей метод називається Google Dorking або Hacking Google, і він використовує пошукові оператори або функції для розширення можливостей інструментів. Він також працює з іншими пошуковими системами, окрім Google.

Цей метод є суперечливим, оскільки він може виходити за рамки того, наскільки є «відкрита» інформація, що збирається.

Наприклад, можна знайти посилання на файл Portable Document Format (PDF), що містить список паролів, але його завантаження може призвести до судового переслідування.

Приклади пошукових операторів включають [15]:

- певні типи файлів;
- пошук термінів на певному сайті;

- пошук каналів Rich Site Summary (RSS) пов'язаних з терміном;
- пошук файлів, що створені між певними датами і т.д.

Прикладом використання Google може бути пошук файлів PDF, наприклад, на сайті «company.website.domain» можна зробити запит ввівши «site:company.website.domain filetype:pdf». Кількість документів у відкритому доступі викликає подив, якщо знати, як змусити Google отримати їх за розвідника.

Переваги Google [14, 15]:

- безкоштовний;
- обмежений об’єм результатів;
- гарний інструмент для розвідників-початківців;
- простий у використанні.

Недоліки Google [14, 15]:

- проблеми конфіденційності;
- обмеження пошукової системи Google;
- отримання певної інформації даним методом може спричинити порушення закону.

5. Платформа Recon-ng з відкритим кодом спочатку використовувався як безкоштовний скрипт з відкритим кодом для збору технічної інформації про веб-сайти. З моменту свого створення він перетворився в повноцінний фреймворк, до якого можна отримати доступ з інтерфейсу командного рядка в Kali Linux або як веб-додаток.

Його інтерфейс схожий на Metasploitable, інший проект комп'ютерної безпеки, розроблений для тестування на проникнення, і має подібні цілі: оцінювати та визначити веб-вразливості. Його функції включають, серед іншого, пошук Geolocation Internet Protocol (GeoIP), DNS та сканування порту [15].

Recon-ng може знайти конфіденційні файли, такі як robots.txt, визначити приховані субдомени, шукати Structured Query Language (SQL) помилки, IP-адреси та отримувати інформацію про Content management system (CMS) та Whois організації [15].

Переваги Recon-ng [13, 15]:

- безкоштовно та з відкритим кодом;
- гарний користувацький інтерфейс;
- може легко знайти обхідні шляхи в коді веб-додатків та веб-сайтів;
- чудово підходить для кібербезпеки.

Недоліки Recon-ng [14]:

- інтерфейс у вигляді командного рядка;
- не підходить для менш технічно обізнаних розвідників.

6. Spiderfoot – це інструмент OSINT, розроблений спеціально для спеціалістів з розслідування інцидентів. Він популярний серед експертів з кібербезпеки, яким потрібно регулярно виявляти можливі цілі кібератак і поверхнево моніторити можливі атаки.

Інструмент може отримати доступ до сотень відкритих джерел даних та відстежувати результати в режимі реального часу. Однак ключова відмінність від інших інструментів OSINT полягає в тому, як можна використовувати Spiderfoot.

А саме, можна незалежно використовувати версію з відкритим кодом в межах власної електронно-обчислювальна машина (ЕОМ) або придбати версію хостом якої є Spiderfoot.

Останній спосіб має багато переваг. Наприклад, більш висока ефективність та можливість побачити співвідношення у своєму розслідуванні.

Переваги Spiderfoot [14, 18]:

- наявна версія з відкритим кодом;
- вибір більшості спеціалістів з розвідки;
- простий інтерфейс;
- повністю безкоштовний доступ до інструменту.

Недоліки Spiderfoot [14, 18]:

- вимагає деякого часу навчання для роботи з інструментом;
- відсутня версія для Macintosh Operating System (Mac OS).

7. HIBP або «Have I Been Pwned?» – це сайт для швидкого пошуку електронних адрес, які з’являються у витоках даних. Витік даних з електронної пошти може

допомогти при перевірці користувача. На основі отриманих даних можна зробити висновок, наскільки підозріла адреса, залежно від виявленої інформації.

Переваги HIBP [14, 15]:

- дає уявлення про те, скільки років електронній адресі;
- допомагає знайти інформацію про витік даних;
- надає можливість масового пошуку цілих доменів;
- безкоштовно для ручної перевірки.

Недоліки HIBP [14]:

- є обмеження щодо перевірки телефонів та електронних адрес.

8. PhoneInfoga. Незважаючи на свої вимоги до технічної обізнаності при використанні PhoneInfoga, важко знайти ліпшу технологію з відкритим кодом для розвідки на основі відкритих джерел з метою пошуку телефонних номерів.

Інструмент обробляє величезний об’єм інформації з номера телефону і працює в будь-якій точці світу.

Переваги PhoneInfoga [14, 15]:

- безкоштовно;
- гарний інструмент для розвідників-початківців;
- покриття по всьому світу.

Недоліки PhoneInfoga [14]:

- вимагає деякого часу навчання для роботи з інструментом.

Алгоритм роботи PhoneInfoga представлено на рисунку 2.6.

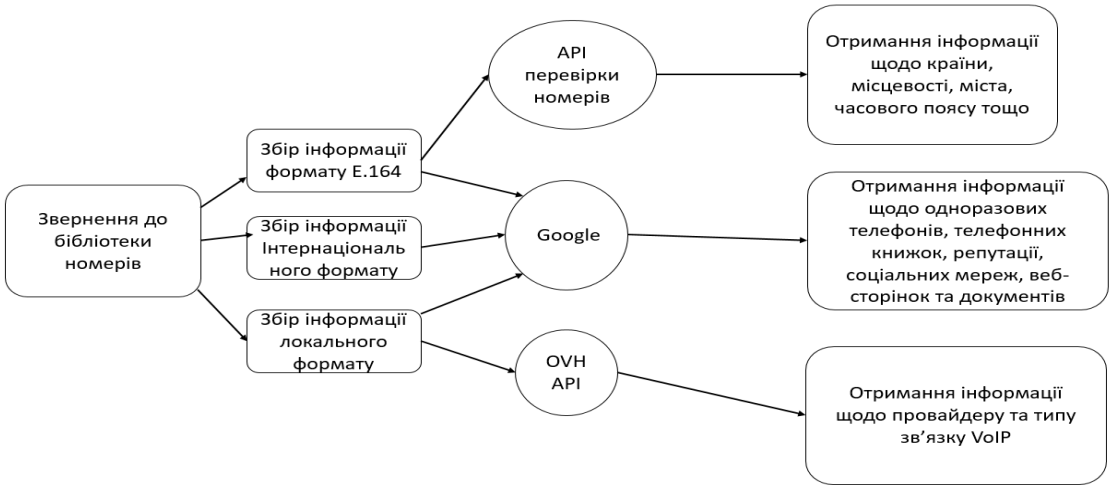

Рисунок 2.6 – Алгоритм роботи методу PhoneInfoga

9. Shodan. Google - це найпоширеніша пошукова система для всіх, тоді як Shodan - це фантастичне та золоте ядро для хакерів, що дозволяє переглядати відкриті активи.

Порівняно з іншими пошуковими системами, Shodan надає аналітику результати, які мають більше сенсу та пов'язані з фахівцями з безпеки. В основному це інформація, пов'язана з активами, підключеними до мережі, наприклад, ноутбуки, світлофори, комп’ютери та інші пристроїв Internet of Things (IoT). Цей інструмент з відкритим кодом, головним чином, допомагає аналітику безпеки визначити мету та перевірити її на різні вразливості, паролі, послуги, порти тощо.

Головним недоліком даного інструменту є його доступність хакерам. Shodan можна використовувати для пошуку вразливостей у пристроях, підключених до мережі, але також можна використовувати для експлуатації цих вразливостей. Це означає, що хакери та інші зловмисники можуть використовувати Shodan для визначення цілей кібератак [19].

Переваги Shodan [18]:

- дуже зручний, навіть для технічно не підкованих користувачів;
- гарний інтерфейс користувача, відображає метрики разом з географічною картою;
- можна експортувати результати та створювати звіти всередині інструменту.

Недоліки Shodan [18]:

- це платний інструмент;
- Shodan пропонується в якості послуги, як і Google, тому не має можливості працювати з його внутрішньою складовою.

10. NexVision – це технологія OSINT, що заснована на штучному інтелекті, яка надає інформацію в режимі реального часу з усієї мережі (Clear Web, Dark Web та Social Networks). Вона забезпечує безпрецедентний доступ до пошуку Darknet через звичайні браузери, такі як Chrome та Safari, без використання анонімного браузера The Onion Routing project (TOR).

Якщо є необхідність перевірити біографічні дані на відповідність вимогам клієнта, зібрати інформацію про організацію та кіберзагрози або навіть вивчити адреси криптовалют із програм-вимагачів, то NexVision забезпечить надання точної відповіді на ці питання у режимі реального часу.

Дана технологія працює так як це показано на рисунку 2.7.

Рисунок 2.7 – Алгоритм роботи методу NexVision

На першому етапі його механізм, заснований на штучному інтелекті, постійно збирає дані, аналізує їх та класифікує, створюючи найбільше комерційно доступне озеро даних.

На другому етапі пошукова система використовує машинне навчання, щоб зменшити кількість помилкових робіт та забезпечити високу точність та контекстуалізовані результати. Це значно зменшує кількість людських годин та час, необхідний для досліджень, а також зменшує втому аналітиків при роботі з великими обсягами невідповідних даних.

На останньому етапі всі результати відображаються на інформаційній панелі, де користувачі можуть легко візуалізувати та приймати розумні рішення.

Панель інструментів дозволяє користувачам встановлювати сповіщення за ключовими словами для відстеження цілей у режимі реального часу, проведення розслідувань та аналізу результатів, зберігаючи анонімність.

Перевагою цього програмного забезпечення є простий інтерфейс, призначений для початкових аналітиків. Аналітики можуть отримати доступ та використовувати комплексну інформацію розвідки не покладаючись на скрипти і не написавши жодного рядка коду.

До недоліків можна віднести те, що інструмент є платним.

Його модуль соціальних мереж відстежує дані з Meta, Instagram, LinkedIn, Discord, Twitter, YouTube, Telegram тощо і оснащений технологією геолокації для визначення джерела та місця розподілу інформації [19].

11. Creepy – це інструмент геолокації з відкритим кодом. Він збирає інформацію про геолокацію, використовуючи різні платформи соціальних мереж та послуг розміщення зображень, які вже були опубліковані десь. Creepy надає звіти на карті за допомогою пошукового фільтра на основі точного місця та дати. Ці звіти доступні у форматі Comma-Separated Values (CSV) або Keyhole Markup Language (KML) для експорту для додаткового аналізу.

Основна функціональність у Creepy поділяється на дві основні вкладки, а саме «Ціль» та «Переглянути карту». З цього і випливає його перевага, що виявляється у простоті використання та недолік в якості малого функціоналу.

Creepy написаний на Python, а також постачається з упакованим двійковим файлом для розподілів Linux, таких як Debian, Backtrack, Ubuntu та Microsoft Windows [19].

12. TheHarvester – дуже простий, але ефективний інструмент, призначений для використання на ранніх етапах тестування на проникнення. Використовується для збору інформації з відкритих джерел та допомагає у визначенні загроз.

TheHarvester має можливість отримати величезну кількість інформації, якщо розвідник з'єднає безліч джерел пошуку, які він підтримує.

Алгоритм роботи TheHarvester на прикладі роботи у середовищі Kali Linux можна побачити на рисунку 2.8.

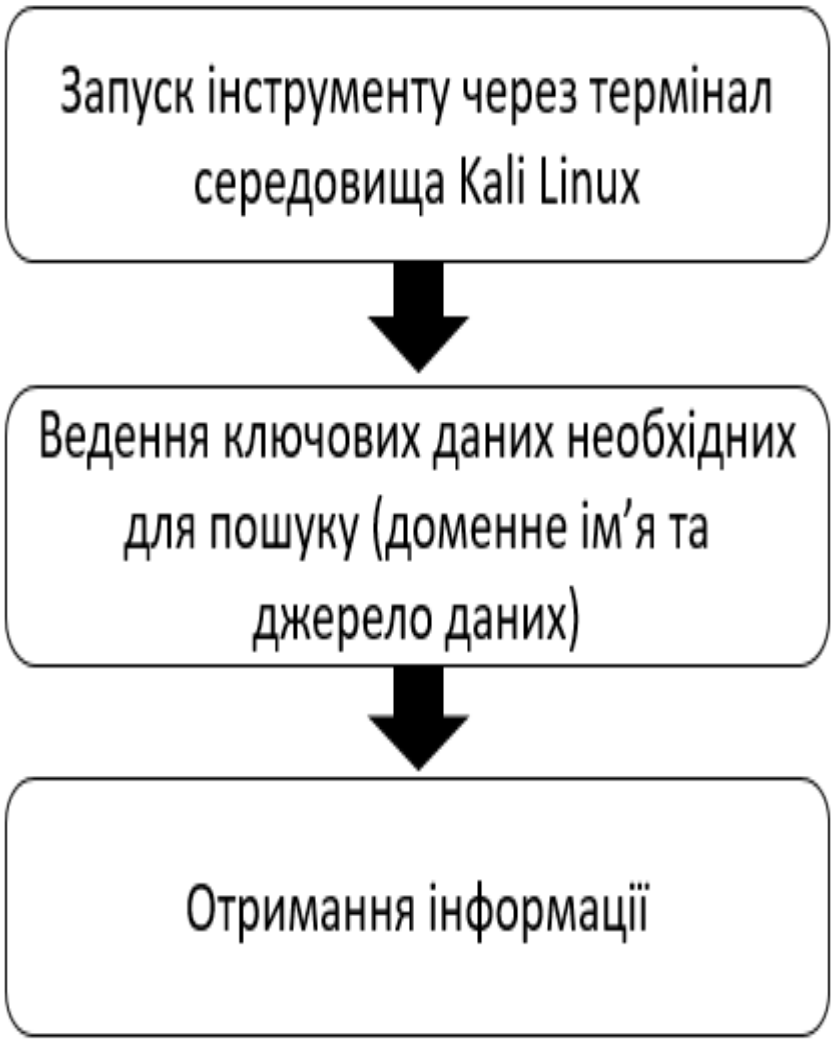

Рисунок 2.8 – Алгоритм роботи методу NexVision

Ось яку інформацію можна отримати за його допомогою в розвідці на основі відкритих джерел [20]:

- електронні адреси;
- субдомени;
- віртуальні хости;
- сканування портів;
- інформація з IP-адрес.

Переваги TheHarvester [18]:

- безкоштовний;
- підтримується великою кількістю людей.

Недоліки TheHarvester [18]:

- не візуалізує дані.

2.3 Аналіз існуючих проблем інструментів інформаційної розвідки на основі відкритих джерел

У всього є свої проблеми і інструменти інформаційної розвідки на основі відкритих джерел не виключення. На основі проведеного опитування незалежним міжнародним колективом дослідників, слідчих та громадянських журналістів «Беллінгкет» [21] та опитування автора цієї роботи на платформі Reddit серед користувачів OSINT, люди, що користуються різноманітними інструментами інформаційної розвідки на основі відкритих джерел стикаються з такими проблемами пов’язаними як з самими інструментами так із процесом роботи з ними:

- достовірність інформації;
- актуальність джерел;
- обробка великого об’єму даних;
- вибір потрібного інструмента;
- структуризація зібраної інформації;
- нестача навичок написання кодів;
- нестача часу;
- сфальсифікована інформація;
- нестача досвіду у сфері досліджень та розвідки;
- аналіз інформації;
- нестача інформації щодо спрощення пошуку потрібної інформації;
- обмежений доступ до інформації через її вартість або конфіденційність;
- аналіз мереж;

- обмежений доступ до різноманітних інструментів інформаційної розвідки на основі відкритих джерел;
- забезпечення власної безпеки під час розвідки;
- виявлення ботів;
- конфіденційність отриманої інформації.

Під час дослідження цього питання автором роботи визначено, що користувачі інструментів з інформаційної розвідки на основі відкритих джерел частіше за все стикаються з проблемами виявлення ботів, застарілими даними, достовірністю інформації та великим об’ємом інформації, яку потрібно обробити.

Висновки до другого розділу

В даному розділі досліджено методи, якими підпорядковуються інструменти інформаційної розвідки на основі відкритих джерел. Проведено аналіз існуючих інструментів OSINT та запропоновано дванадцять найпопулярніших з них.

На основі опитування автора цієї роботи на платформі Reddit та даних з інтернет-видання «Беллінгкет» визначено найактуальніші проблеми з інструментами інформаційної розвідки на основі відкритих джерел та їх використання.

Показані переваги та недоліки кожного розглянутого інструмента OSINT і поставлено завдання щодо покращення ефективності виявлення ботів та достовірності інформації зібраної за допомогою розвідки на основі відкритих джерел.

РОЗДІЛ 3
ПРОПОЗИЦІЇ ЩОДО ПІДВИЩЕННЯ ДОСТОВІРНОСТІ ЗІБРАНОЇ ІНФОРМАЦІЇ ЗА ДОПОМОГОЮ ТЕХНОЛОГІЇ РОЗВІДКИ НА ОСНОВІ ВІДКРИТИХ ДЖЕРЕЛ

3.1 Інструменти виявлення ботів

Однією з основних проблем при використанні інструментів призначених для інформаційної розвідки на основі відкритих джерел є виявлення ботів, тому за мету даної роботи поставлено завдання підвищення достовірності зібраних даних за допомогою технологій OSINT.

Підвищення достовірності зібраної інформації реалізується шляхом перевірки даних за допомогою певних інтерфейсів прикладного програмування, які орієнтовані на виявлення ботів в IP-адресах та електронній пошті.

Згідно до проведеного у другому розділі дослідження інформація з відкритих джерел взаємопов’язана між собою, тому підвищуючи достовірність однієї можна забезпечити отримання більш правдивих даних за допомогою різноманітних інструментів OSINT.

Саме тому, основну увагу в даному дослідженні, приділено двом наведеним нижче API, що призначені для виявлення ботів серед отриманих за допомогою інструментів розвідки на основі відкритих джерел IP-адрес.

Перше API аналізу загроз від організації Focsec, яке спрощує пошук IP-адрес злоякісних ботів. Дане API працює цілодобово та надає високоякісну актуальну інформацію щодо загроз пов’язаних з IP-адресами за для вчасного виявлення та знешкодження ботів.

Дане API не користується статичними чорними списками так як запатентовані вузли збору даних Focsec постійно відслідковують мережу Інтернет та надають актуальну інформацію щодо виявлення ботів.

Інформація отримана з допомогою даного API гарно фільтрується, що зменшує ймовірність помилкового спрацювання.

Зазначене API дуже легко пристосувати до потреб користувача так як воно працює з Python, Ruby, Node та через команду «curl».

Нижче на рисунках 3.1-3.4 наведено способи застосування даного API в зручній для користувача формі [22]:

```python
import requests
headers = {'Authorization': 'your-api-key-here'}
rsp = requests.get('https://api.focsec.com/v1/ip/46.5.143.218', headers=headers)
print(rsp.json())
```

Рисунок 3.1 – Використання API з допомогою мови програмування Python

```ruby
require 'httparty'

headers = {
  "Authorization"  => "your-api-key-here",
}
rsp = HTTParty.get(
  "https://api.focsec.com/v1/ip/46.5.143.218",
  :headers => headers
)
puts rsp
```

Рисунок 3.2 – Використання API з допомогою мови програмування Ruby

```javascript
const axios = require('axios').default;

axios.get('https://api.focsec.com/v1/ip/46.5.143.218', {
    headers: {Authorization: 'b4ew4FfgbEg3ib2gemowbo69al3'}
}).then(function (response) {
    console.log(response.data);
}).catch(function (error) {
    console.log(error.response.data);
})
```

Рисунок 3.3 – Використання API з допомогою Node

```
curl -X GET "https://api.focsec.com/v1/ip/46.5.143.218" \
     -H "Authorization: your-api-key-here"
```

Рисунок 3.4 – Використання API з допомогою команди «curl»

Після виконання функції даного API може бути отримана інформація, що представлена на рисунку 3.5.

Result

Code: 200


```
{
    "ip": "204.32.106.40",
    "is_proxy": false,
    "is_vpn": false,
    "is_tor": false,
    "is_bot": false,
    "is_datacenter": false,
    "city": null,
    "country": "United States",
    "iso_code": "us",
    "is_in_european_union": false,
    "flag": "us",
    "autonomous_system_number": null,
    "autonomous_system_organization": null
```


Рисунок 3.5 – Приклад використання API Focsec

Згідно з представлених на рисунку 3.5 даних можна отримати таку інформацію [22]:

- IP яке проходить перевірку;
- результат перевірки на запити з проксі-мережі;
- результат перевірки на запити з мережі Virtual Private Network (VPN);

- результат перевірки на запити з мережі TOR;
- результат перевірки на бота;
- вказує, чи належить IP центру обробки даних, хмарі чи хостинговій компанії;
- приблизне місцезнаходження IP-адреси;
- країна IP-адреси;
- двозначний код країни визначений International Organization for Standardization (ISO) 3166;
- результат того чи є країна частиною Євросоюзу;
- прапор країни;
- номер автоматизованої системи (АС), яка керує даною IP-адресою;
- назва АС організації, що керує даною IP-адресою.

Тобто дане API не тільки виконує свою функцію щодо виявлення злоякісних ботів, а також виступає поверхневим інструментом інформаційної розвідки на основі відкритих джерел, яке працює з IP-адресами [20].

Наступне API, яке має застосовуватися для виявлення ботів разом з тим, що надає Focsec, працює взагалі за іншим принципом.

BotScout – це служба, яка допомагає боротися з автоматизованими веб-скриптами, також відомими як «боти» [23].

Боти переміщуються по мережі Інтернету розповсюджуючи спам, поширюючи шкідливі посилання, а при отриманні доступу до сайту вони користуються ним як плацдармом для подальшого виконання своїх функцій.

Результатом цього є фіктивні реєстрації на форумах, забруднення ретельно розробленої бази даних, спам з образливими посиланнями та безліч інших проблем.

Крім того BotScout відстежує імена, IP-адреси та адреси електронної пошти, які використовують боти, а потім реєструє їх для майбутнього порівняння.

BotScout надає простий API, який можна використовувати для виявлення ботів. Проста перевірка по створеній базі даних BotScout виявляє більшість ботів. База даних BotScout містить «сигнатури» ботів. Підпис складається з унікальної комбінації імені, яке бот використовував при спробі зареєструватися, адреси електронної пошти

бота та його IP-адреси. Ці три елементи використовуються окремо для ідентифікації ботів щоразу, коли вони використовують вже відоме ім'я, адресу електронної пошти або IP-адресу.

На відміну від інших баз даних ботів, які стверджують, що містять сотні тисяч сигнатур ботів, але при перевірці виявляється, що більшість їх даних є дубльованими записами.

База даних BotScout регулярно очищається шляхом прибирання однакових сигнатур, щоб переконатися, що вона містить лише унікальні підписи [23].

Дане API може також використовуватися в якості модуля такого відомого інструменту розвідки на основі відкритих джерел як Spiderfoot [24].

Користуватися даним API дуже просто, достатньо відправити URL-запит з інформацією, яка має пройти перевірку на наявність ботів.

BotScout має п’ять команд для перевірки до яких відносяться [23]:

- перевірка електронної пошти – http://botscout.com/test/?mail=youremail;
- перевірка IP-адреси – http://botscout.com/test/?ip=yourip;
- перевірка імені – http://botscout.com/test/?name=yourname;
- перевірка всього на предмет невизначеного об’єкту – http://botscout.com//test/?all=yourobject;
- мульти-перевірка по всім параметрам – http://botscout.com/test/?multi&name=yourname&mail=youremail&ip=yourip.

В результаті виконання запиту до API BotScout зазвичай з’являється три значення, що розділені вертикальною полосою (рис.3.6).

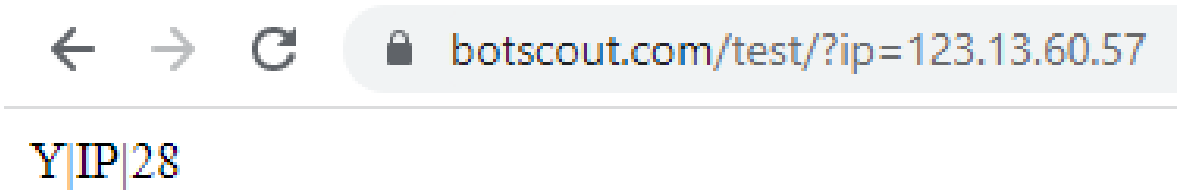

Рисунок 3.6 – Приклад роботи API BotScout

Параметр «Y» вказує на те, що є збіги інформації, яка перевіряється з наявною у базі BotScout.

Параметр «N» вказує на відсутність збігів інформації, яка перевіряється з наявною у базі BotScout.

Параметр «число» вказує на кількість збігів інформації, яка перевіряється з наявною у базі даних BotScout.

Параметр «IP/MAIL/NAME/ALL/MULTI» вказує на тип перевірки інформації.

На реальному прикладі представленому на рисунку 3.6 показано результат роботи даного API. Тобто після перевірки IP-адреси «123.13.60.57» маємо 28 збігів з «сигнатурою» злоякісного бота [23].

3.2 Рекомендації щодо поліпшення достовірності інформації

З метою покращення достовірності отриманої за допомогою інструментів розвідки на основі відкритих джерел інформації щодо IP-адрес пропонується попарно використовувати вище вказані API Focsec та API BotScout.

Дані API працюють за зовсім різними принципами, в той час коли Focsec перевіряє на ботів IP-адреси за своєю запатентованою методологією в режимі реального часу.

BotScout порівнює інформацію зі своєю базою даних «сигнатур» ботів, що постійно оновлюється. Саме тому, якщо використовувати ці API в парі можна досягти майже стопроцентного рівня ймовірності виявлення злоякісного бота. Це в свою чергу підвищить достовірність отриманої інформації, хоча і за рахунок витраченого часу на саму перевірку.

Остання обставина свідчить про те, що у даної системи перевірки інформації зібраної з допомогою OSINT є також недолік який виявляється в збільшенні кількості необхідного часу для отримання шуканої інформації.

Попри те, що зазначений недолік виникає у разі застосування запропонованої системи виявлення ботів серед інформації добутої за допомогою технологій розвідки на основі відкритих джерел тільки у разі виконання ручної перевірки.

Для підтвердження представленої теорії того, що попарне використання даних API збільшить ймовірність виявлення бота серед IP-адрес було проведено експериментальне дослідження під час якого здійснено перевірку тридцяти IP-адрес взятих з різних відкритих чорних списків, що можна побачити у таблиці 3.1.

Приклади результатів проведеного експерименту по виявленню ботів можна побачити на рисунках 3.7-3.10.

Рисунок 3.7 – Приклад невдалого виявлення бота за допомогою API BotScout

Рисунок 3.8 – Приклад вдалого виявлення бота за допомогою API BotScout

Рисунок 3.9 – Приклад вдалого виявлення бота за допомогою API Focsec

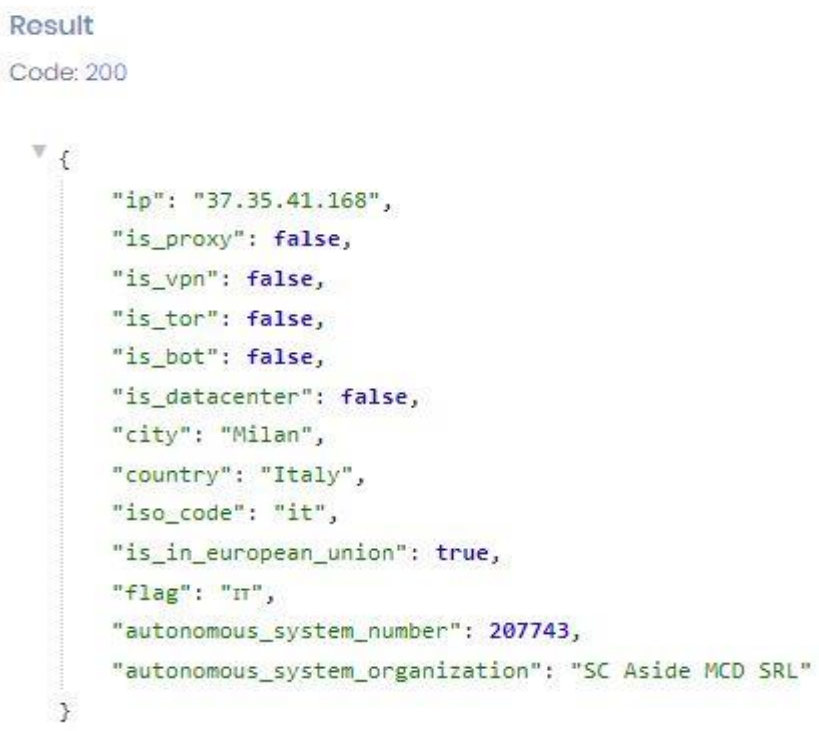

Рисунок 3.10 – Приклад невдалого виявлення бота за допомогою API Focsec

Після аналізу отриманих результатів проведено розрахунок того на скільки відсотків отримана система виявлення ботів працює краще ніж у випадку поодинокого використання вище представлених API.

Після отримання цих даних проведено розрахунок відсотку виявлених ботів за формулою 3.1:

$$X = \frac{A \times 100}{B} \tag{3.1}$$

де X – відсоток виявлених ботів;

A – кількість виявлених збігів;

B – загальна кількість IP-адрес.

Після виконання розрахунків за формулою 3.1 маємо такі результати:

- відсоток виявлених ботів за допомогою API Focsec складає 70%;
- відсоток виявлених ботів за допомогою API BotScout складає 60%;
- відсоток виявлених ботів за допомогою попарного використання представлених вище API складає 90%.

Таблиця 3.1

Результати процесу виявлення ботів за допомогою API Focsec та API BotScout

IP-адреси з відкритих чорних списків	Виявлення бота через API Focsec	Виявлення бота через API BotScout
196.240.254	+	+
123.13.62.181	+	+
113.11.69.103	+	+
172.81.129.246	+	–
17.241.75.176	+	–
104.238.4.79	–	+
195.146.6.73	–	+
17.241.219.151	–	–
23.94.2.250	+	+
191.96.181.145	+	+
69.58.7.18	–	+
5.255.231.158	+	–
17.241.219.6	+	–
163.53.183.68	+	–
41.101.186.145	–	–
121.184.19.115	+	+
2.56.117.145	+	+
165.231.182.146	+	+
58.136.1.136	+	+
220.248.70.237	+	+
64.124.8.57	+	–
197.247.192.159	+	–
45.117.60.99	+	–
103.88.24.3	–	–
37.35.41.168	–	+
91.199.3.220	–	+
154.85.124.67	–	+
193.39.245.34	+	+
23.229.12.118	+	+
168.119.65.116	+	–

Для визначення на скільки відсотків більше виявляється ботів за допомогою запропонованого методу проведено розрахунки за формулою 3.2:

$$V = \frac{C \times 100}{M} - 100 \quad (3.2)$$

де V – відсоток різниці між двома ймовірностями;

C – відсоток виявлених ботів за допомогою запропонованого методу;

M – відсоток виявлених ботів за допомогою одного з розглянутих API.

В результаті маємо такі дані. Попарне використання представлених API ефективніше на 28,57% і 50%, ніж поодиноке використання API Focsec та API BotScout відповідно. Тобто у випадку, якщо раніше для виявлення ботів серед інформації зібраної з відкритих джерел використовувалося тільки API Focsec, то при додаванні до системи перевірки API BotScout ефективність збільшиться на 28,57%.

З іншого боку, якщо для виявлення ботів серед інформації зібраної за допомогою інструментів OSINT застосовувалося тільки API BotScout, то при додаванні до системи перевірки API Focsec ефективність збільшиться на 50%.

Висновки до третього розділу

В даному розділі досліджено API Focsec та API BotScout, що призначені для виявлення ботів.

Проведено аналіз відмінностей даних інтерфейсів прикладного програмування.

Надано рекомендації щодо покращення достовірності інформації отриманої за допомогою розвідки на основі відкритих джерел шляхом об’єднання двох представлених API у систему виявлення ботів.

Перевірено на наявність ботів тридцять IP-адрес взятих з різних відкритих чорних списків за допомогою API Focsec та API BotScout.

Здійснено розрахунок відсотку виявлених ботів на основі отриманих після перевірки даних.

Проведено розрахунок ефективності запропонованого методу виявлення ботів в порівнянні з поодиноким використання розглянутих API.

Визначено, що при одночасному використанні обох API процент виявлених ботів дорівнює 90%, що на 28,57% більше ніж при окремому використанні API Focsec та на 50% більше ніж при окремому застосуванні API BotScout.

ВИСНОВКИ

В роботі проведений аналіз та досліджено базове поняття розвідки на основі відкритих джерел, розглянута структура та процес OSINT. Проведений аналіз переваг, недоліків та актуальних проблем дослідження розвідки на основі відкритих джерел.

До переваг розвідки на основі відкритих джерел відносяться:

- швидкий збір інформації в режимі реального часу;
- безпечний збір великої кількості даних;
- достовірність джерел інформації;
- зручність та простота доступу;
- низька ціна.

До недоліків розвідки на основі відкритих джерел відносяться:

- достатньо великий об’єм інформації, що потребує для її обробки багато зусиль та значних ресурсів;
- скептичне ставлення відповідних спецслужб до отриманої даним методом інформації;
- проблеми безпеки та технічні обмеження;
- зібрана даним методом інформація може стати фундаментом для кіберзлочинів.

До актуальних проблем досліджень методу OSINT відносяться:

- проблеми з ефективною та надійною фільтрацією інформації;
- проблеми з достовірністю інформації;
- відсутність перевірки процедур забезпечення конфіденційності.

Визначені та проаналізовані основні вимоги й загрози безпеки при використанні методу OSINT.

Досліджено методи, якими підпорядковуються інструменти інформаційної розвідки на основі відкритих джерел.

Проведено аналіз існуючих інструментів OSINT та запропоновано дванадцять найпопулярніших з них.

Автором цієї роботи на основі опитування на платформі Reddit та даних з інтернет-видання «Беллінгкет» визначено найактуальніші проблеми з інструментами інформаційної розвідки на основі відкритих джерел та їх використання.

Показані переваги та недоліки кожного розглянутого інструмента OSINT і поставлено завдання щодо покращення ефективності виявлення ботів та достовірності інформації зібраної за допомогою розвідки на основі відкритих джерел.

Досліджено API Focsec та API BotScout, що призначені для виявлення ботів.

Проведено аналіз відмінностей даних інтерфейсів прикладного програмування.

Надано рекомендації щодо покращення достовірності інформації отриманої за допомогою розвідки на основі відкритих джерел шляхом об’єднання двох представлених API у систему виявлення ботів.

Проведено експеримент в ході якого перевірено на наявність ботів тридцять IP-адрес взятих з різних відкритих чорних списків за допомогою API Focsec та API BotScout.

Здійснено розрахунок відсотку виявлених ботів на основі отриманих після перевірки даних.

Проведено розрахунок ефективності запропонованого методу виявлення ботів в порівнянні з поодиноким використання розглянутих API.

Визначено, що при одночасному використанні обох API процент виявлених ботів дорівнює 90%, що на 28,57% більше ніж при окремому використанні API Focsec та на 50% більше ніж при окремому застосуванні API BotScout.

У результаті виконання даної кваліфікаційної роботи всі поставлені завдання виконані, мета роботи досягнута.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Yong-Woon H. Current Status and Security Trend of OSINT / Hwang Yong-Woon. // Wireless Communications and Mobile Computing. – 2022. – С. 1–14.

2. World of Cyber Security and Cybercrime / R.Buch, D. Ganda, P. Kalola, N. Borad. // STM Journals 2017. – 2017. – №4. – С. 18–23.

3. Lee W. H. Intelligence in the internet Era: understanding OSINT and case analysis / Lee. // Korean Security Journal. – 2013. – №34. – С. 259–278.

4. Miller B. H. Open source intelligence (OSINT): an oxymoron? / Miller. // International Journal of Intelligence & Counter Intelligence. – 2018. – №31. – С. 702–719.

5. Kanta A. A survey exploring open source Intelligence for smarter password cracking / Kanta. // Forensic Science International: Digital Investigation. – 2020.

6. Dokman T. Open source intelligence (OSINT) issues and trends / T. Dokman, T. Ivanjko // INFuture 2019: knowledge in the digital age, / T. Dokman, T. Ivanjko., 2020.

7. Chun W. Open source intelligence in the information age / Chun. // Journal of National Intelligence Studies. – 2008. – С. 151.

8. Hassan N. A. Open Source Intelligence Methods and Tools / N. A. Hassan, R. Hijazi // The evolution of open source intelligence / N. A. Hassan, R. Hijazi. – USA, 2018.

9. Pastor-Galindo J. The not yet exploited goldmine of OSINT: opportunities, open challenges and future trends / Pastor-Galindo. //– 2020. – №8. – С. 10282–10304.

10. Alkhudhayr F. Information security: a review of information security issues and techniques / Alkhudhayr. // IEEE. – 2019. – С. 1–6.

11. Wells D. OSINT in the context of cybersecurity / Wells // Open Source Intelligence Investigation: From Strategy to Implementation / Wells, 2016. – С. 213–231.

12. Yeboah-Ofori A. Cyber intelligence and OSINT: developing mitigation techniques against cybercrime threats on social media / A. Yeboah-Ofori, A. Brimicombe. // International Journal of Cyber-Security and Digital Forensics. – 2018. – №7. – С. 87–98.

13. Siddula M. Privacy-enhancing preferential lbs query for mobile social network users / M. Siddula, Z. Tian. – 2020. – С. 1–13.

14. Top 10 OSINT (Open Source Intelligence) Software Tools [Електронний ресурс]. – 2023. – Режим доступу до ресурсу: https://seon.io/resources/comparisons/osint-software-tools/.

15. Hitesh J. Top 10 Best Open Source Intelligence Tools – OSINT – (Pros and Cons) [Електронний ресурс] / Jethva Hitesh // Cloud Infrastructure Services Ltd – Режим доступу до ресурсу: https://cloudinfrastructureservices.co.uk/top-10-best-open-source-intelligence-tools-osint/.

16. Lampyrise data [Електронний ресурс] – Режим доступу до ресурсу: https://lampyre.io/.

17. Recon-ng Information gathering tool in Kali Linux [Електронний ресурс] // GeeksforGeek. – 2021. – Режим доступу до ресурсу: https://www.geeksforgeeks.org/recon-ng-installation-on-kali-linux/.

18. Wilson M. OSINT Tools & Software for Passive & Active Recon & Security! [Електронний ресурс] / Marc Wilson // PC & Network Downloads. – 2022. – Режим доступу до ресурсу: https://www.pcwdld.com/osint-tools-and-software#wbounce-modal.

19. Anjaneyulu N. 9 Open Source Intelligence (OSINT) Tools for Penetration Testing [Електронний ресурс] / Naini Anjaneyulu. – 2022. – Режим доступу до ресурсу: https://geekflare.com/osint-tools/.

20. theHarvester Best OSINT tool [Електронний ресурс]. – 2020. – Режим доступу до ресурсу: https://ethicaltools.gitbook.io/subdomainfinder/theharvester-best-osint-tool.

21. Wild J. These are the Tools Open Source Researchers Say They Need [Електронний ресурс] / Johanna Wild // Bellingcat. – 2022. – Режим доступу до ресурсу: https://www.bellingcat.com/resources/2022/08/12/these-are-the-tools-open-source-researchers-say-they-need/.

22. Focsec API Documentation [Електронний ресурс] – Режим доступу до ресурсу: https://docs.focsec.com/.

23. BotScout API Documentation [Електронний ресурс] – Режим доступу до ресурсу: https://botscout.com/api.htm.

24. Micallef S. Spiderfoot [Електронний ресурс] / Steve Micallef – Режим доступу до ресурсу: https://github.com/smicallef/spiderfoot.