ПОЛТАВСЬКИЙ ДЕРЖАВНИЙ АГРАРНИЙ УНІВЕРСИТЕТ
Навчально-науковий інститут економіки, управління, права та інформаційних технологій
Кафедра інформаційних систем та технологій

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття ступеня вищої освіти магістр

на тему: **«Використання інструментів OSINT для перевірки на достовірність даних з відкритих джерел»**

Виконав: здобувач вищої освіти
за освітньою програмою
Інформаційні управляючі системи та технології
спеціальності 126 Інформаційні системи та технології
ступеня вищої освіти магістр
групи 126ІСТ_мд_2023
Давиденко Андрій Сергійович
Керівник: Поночовний Юрій Леонідович
Рецензент: Муравльов Володимир Вячеславович

Полтава – 2024 року

ВСТУП

Актуальність теми: Протягом останніх десятиліть стрімкий розвиток цифрових технологій, інтернету та соціальних мереж значно змінив спосіб, у який збирається, аналізується та використовується інформація. У цьому контексті концепція розвідки за відкритими джерелами (OSINT) набула надзвичайної популярності, забезпечуючи аналітикам доступ до значного обсягу даних для вирішення завдань у сфері кібербезпеки, правоохоронної діяльності, економіки та журналістики.

Особливої актуальності OSINT набуває в умовах сучасних глобальних викликів, таких як кіберзагрози, дезінформація, тероризм і конфлікти, що потребують швидкого аналізу відкритих джерел для прийняття обґрунтованих рішень. Військові та безпекові організації використовують OSINT для виявлення потенційних загроз і аналізу активностей ворога. Наприклад, у контексті російсько-української війни, OSINT став важливим інструментом для аналізу соціальних мереж, геопросторової розвідки та виявлення злочинів агресора.

Роботи вчених, таких як T. Pelgrin, R. Steele, H. Lasswell, та дослідження у рамках міжнародних проектів, як-от Bellingcat, відображають теоретичні основи та практичне застосування OSINT у сучасному світі. Їхній внесок заклав основу для розуміння методів та інструментів, які використовуються в OSINT, зокрема для роботи з великими масивами даних та їх візуалізації.

Ураховуючи зростаючу роль відкритих даних у кіберпросторі, дослідження ефективності використання OSINT-інструментів, таких як SpiderFoot, Maltego та OSINT Framework, є надзвичайно важливим для оптимізації процесів аналізу інформації, підвищення кібербезпеки та забезпечення інформаційної гігієни.

Метою кваліфікаційної роботи є аналіз сучасних методів та інструментів OSINT, розробка алгоритмів застосування їх для аналізу даних з відкритих джерел і дослідження практичного застосування OSINT у вирішенні завдань кібербезпеки.

Для досягнення поставленої мети були визначені такі завдання:

1. Аналіз сутності та основних принципів OSINT, дослідження сучасних інструментів OSINT та їх можливостей.

2. Розробка алгоритму використання OSINT-інструментів для аналізу даних, практичне тестування інструментів OSINT на реальних кейсах.

3. Оцінка ризиків і перспектив застосування OSINT у різних галузях.

Об'єкт дослідження: процеси збору, аналізу та використання даних з відкритих джерел.

Предмет дослідження: інструменти та методи OSINT для забезпечення аналізу відкритих даних.

Проведені в роботі дослідження базуються на загальнонаукових методах аналізу, синтезу, класифікації та систематизації, а також спеціалізованих методах OSINT, зокрема аналізу мережі, візуалізації зв'язків та перевірки достовірності даних.

Інформаційна база кваліфікаційної роботи складається з наукових статей, міжнародних аналітичних видань і звітів, матеріалів конференцій, а також з інтернет-ресурсів, що містять інформацію про сучасні інструменти OSINT.

Елементи наукової новизни полягають у розробці алгоритму інтеграції OSINT-інструментів для аналізу відкритих даних, що забезпечує підвищення ефективності виявлення загроз і збору інформації для прийняття рішень.

Практична значущість роботи полягає в можливості повторного застосування та модифікації розробленого програмного коду та алгоритмів для аналізу відкритих даних у сферах кібербезпеки, журналістики, економіки та правоохоронної діяльності. Отримані результати можуть бути корисними для спеціалістів з інформаційної безпеки, дослідників і аналітиків.

Структура та обсяг кваліфікаційної роботи логічно пов'язані з задачами досліджень. Робота містить перелік умовних позначень, вступ, три розділи основної частини, висновки, список використаних джерел, додатки. Загальний обсяг текстової частини дипломної роботи складає 63 сторінки формату А4. Вона містить 10 рисунків і 8 таблиць. В роботі використано 48 науково-технічних джерел.

РОЗДІЛ 1
АНАЛІЗ МЕТОДІВ OSINT ТА ОСНОВ ПЕРЕВІРКИ ДАНИЗ З ВІДКРИТИХ ДЖЕРЕЛ

1.1 Сутність і концепція OSINT

Розвідка за відкритими джерелами, відома як OSINT (Open Source Intelligence), є сучасним методом отримання інформації, який ґрунтується на зборі, аналізі та систематизації даних із загальнодоступних джерел. Ця концепція набуває все більшого значення у сучасному світі через стрімкий розвиток цифрових технологій, соціальних мереж та інтернету загалом. Використання OSINT дозволяє аналітикам зосереджувати увагу на відкритих даних, не порушуючи законів, що робить цю методологію важливим інструментом у багатьох сферах, зокрема у військовій, економічній та кібербезпеці.

Термін OSINT досі не має єдиного загальноприйнятого визначення. Проте одне з найточніших його трактувань наведене у «Посібнику НАТО з розвідки з використанням відкритих джерел», опублікованому у 2001 році. Цей документ містить рекомендації щодо роботи з публічною інформацією для аналітиків альянсу, приділяючи увагу таким аспектам, як інформаційна гігієна, зберігання даних та їх коректна агрегація. У звіті Офісу Директора Національної Розвідки США (2011) OSINT визначено як діяльність зі збору та аналізу інформації з відкритих джерел для задоволення потреб аналітичних служб [1].

Згідно з сучасними підходами, OSINT включає поєднання технологій, методологій і концепцій, які спрямовані на здобування даних із відкритих джерел та їх аналіз відповідно до конкретних аналітичних завдань. Дані для OSINT можуть надходити з різноманітних відкритих джерел, серед яких:

1) засоби масової інформації (ЗМІ): газети, журнали, радіо, телебачення;
2) інтернет: вебсайти, блоги, відео, соціальні мережі;
3) державні ресурси: публічні звіти, бюджети, слухання, довідники;
4) комерційні джерела: фінансові оцінки, ринкові дослідження, бази даних;

5) «сіра література»: документи некомерційних організацій, технічні звіти, патенти.

Історичне коріння OSINT сягає 1941 року, коли було створене Агентство з моніторингу іноземних трансляцій (FBMS) у США. Його завданням був аналіз новин і радіопередач, зокрема з держав-членів Осі. Аналізуючи пропагандистські матеріали та інші джерела, аналітики FBMS формували висновки, які допомагали у військовій розвідці. Зокрема, під час Другої світової війни до 95% інформації про стан економіки Японії було отримано саме завдяки цьому агентству.

У період Холодної війни OSINT значно розширив свої можливості, забезпечуючи аналіз ситуації в СРСР та його сателітах. Наприклад, інформація про радянські ракети на Кубі та участь СРСР у міжнародних конфліктах була здобута через відкриті джерела.

Сьогодні розвідка за відкритими джерелами охоплює не лише військову сферу, а й інші галузі, включаючи правоохоронну діяльність, кібербезпеку, економіку та журналістику. Стрімкий розвиток інтернету та соціальних мереж зробив OSINT більш комплексним явищем, дозволяючи аналітикам отримувати інформацію не лише про події, але й про конкретних осіб, їхні мережі та вподобання [2].

Наприклад, аналіз соціальних мереж дозволяє встановлювати зв'язки між людьми, організаціями та подіями. Завдяки цьому OSINT став важливим інструментом у боротьбі з тероризмом, незаконним обігом зброї, фінансовими злочинами, а також у кібербезпеці.

Сфери застосування OSINT:

1) правоохоронна діяльність: OSINT використовується для запобігання та розслідування кіберзлочинів, боротьби з тероризмом, відмиванням коштів та іншими злочинами;

2) кібербезпека: аналітики застосовують OSINT для виявлення вразливостей систем та перевірки дотримання службових правил у компаніях;

3) економічна діяльність: OSINT допомагає перевіряти репутацію контрагентів, аналізувати фінансові звіти та уникати співпраці з ненадійними партнерами;

4) журналістика: журналісти використовують OSINT для розслідувань корупції та інших суспільно важливих питань. Яскравим прикладом є діяльність команди Bellingcat, яка розкриває дані про військові злочини та інші міжнародні події. Нижче наведенна таблиця для зрозумілішого розуміння.

Таблиця 1.1 – Порівняльна таблиця сфер застосування OSINT

Сфера застосування	Мета використання	Основні джерела інформації	Приклади застосування
Правоохоронна діяльність	Розслідування та запобігання злочинам, виявлення незаконної діяльності	Соціальні мережі, бази даних, відеоматеріали, офіційні документи	Пошук терористичних організацій, протидія відмиванню коштів, боротьба з розповсюдженням наркотиків та зброї.
Кібербезпека	Виявлення вразливостей систем, оцінка ризиків витоку інформації	Інтернет-форуми, технічні звіти, соціальні мережі	Аналіз витоків даних, перевірка дотримання працівниками правил конфіденційності, реверсивний аналіз атак.
Економічна діяльність	Аналіз ринку, перевірка партнерів і контрагентів	Фінансові звіти, комерційні бази даних, офіційні реєстри	Оцінка ризиків співпраці з офшорними компаніями, аналіз афілійованих осіб, перевірка на участь у тіньових схемах.
Журналістика	Розслідування корупційних схем, виявлення зловживань владою	Декларації доходів, публічні звіти, соціальні мережі	Викриття корупційної діяльності, аналіз відповідності реальних статків задекларованим доходам, розслідування міжнародних подій, наприклад, діяльності спільноти Bellingcat.

Порівняльна таблиця (табл. 1.1) допомагає систематизувати інформацію про сфери застосування OSINT, акцентуючи увагу на їхніх особливостях, джерелах даних та практичних прикладах [3].

Концепція OSINT є одним із найважливіших досягнень сучасної інформаційної епохи. Її універсальність та доступність дозволяють застосовувати цей підхід у найрізноманітніших сферах, забезпечуючи як безпеку, так і прозорість

процесів у суспільстві. Широке використання OSINT у військовій, економічній та соціальній галузях доводить її значення для розвитку сучасного світу.

1.2 Класифікація джерел відкритих даних та їх особливості

Відкриті джерела даних стають дедалі важливішими у сучасному інформаційному суспільстві, адже вони є основою для збору, аналізу та використання інформації в різних сферах. Одним із ключових понять у цій галузі є OSINT (Open Source Intelligence), що означає отримання інформації з відкритих джерел. Аналіз і систематизація цих даних допомагають глибше зрозуміти їхню природу та можливості застосування [4].

OSINT визначається як діяльність із отримання інформації з відкритих джерел для розвідки, аналізу чи інших цілей. Це поняття охоплює широкий спектр діяльності, включаючи журналістику, досудове розслідування та аналітичну роботу. Його основні характеристики включають цілеспрямовані дії, спрямовані на отримання релевантної інформації, використання відкритих джерел у різних формах, а також процес збору, аналізу даних і формування висновків.

OSINT слід відрізняти від традиційної розвідки, яка регулюється законодавством і може здійснюватися лише обмеженим колом суб'єктів. Джерела відкритих даних можна умовно розділити на кілька категорій залежно від їхнього характеру, формату і способу доступу [5].

Основні категорії інформаційних джерел включають мас-медіа, до яких відносяться традиційні друковані видання, зокрема газети та журнали, а також електронні медіа, як-от онлайн-видання, новинні портали, радіо та телебачення.

Крім того, соціальні мережі відіграють важливу роль у поширенні інформації в реальному часі. Державні ресурси включають офіційні реєстри та бази даних, такі як реєстри юридичних осіб, судові рішення та нормативно-правові акти, а також відкриті дані, що публікуються державними установами для широкого доступу.

Наукові та технічні джерела охоплюють академічні публікації, наукові журнали, дисертації, технічні звіти, патенти та стандарти. Корпоративні дані включають публічні звіти компаній, такі як фінансові результати чи звіти про корпоративну соціальну відповідальність, а також інформацію, доступну на офіційних сайтах організацій. Краудсорсингові платформи забезпечують форми, на яких користувачі добровільно надають дані, наприклад, у геоінформаційних сервісах або в проєктах з моніторингу навколишнього середовища. Спеціалізовані платформи включають сайти для обміну даними, такі як GitHub, Stack Overflow, а також сервіси, що надають відкриті API для доступу до даних [6].

Різноманітність відкритих джерел даних зумовлює їхні специфічні особливості. Відкриті дані зазвичай є вільно доступними, хоча для окремих типів інформації може знадобитися реєстрація або авторизація. Вони охоплюють значні масиви інформації, що потребує спеціальних інструментів для аналізу. Рівень оновлення таких даних варіюється: соціальні мережі надають інформацію в режимі реального часу, тоді як академічні публікації мають триваліший цикл створення.

Перевірка достовірності даних є однією з головних проблем, адже відкриті джерела часто містять застарілу або викривлену інформацію. Дані представлені у різних форматах, включаючи текстові документи, таблиці та мультимедійний контент, що ускладнює їхню обробку.

Відкриті джерела даних мають величезний потенціал для бізнесу, науки, урядування та громадської активності, сприяючи глибокому аналізу й прогнозуванню, створенню нових сервісів, продуктів та інструментів, а також забезпеченню прозорості й підзвітності державних і приватних структур.

Однак ефективне використання відкритих джерел вимагає наявності відповідної інфраструктури, інструментів для аналізу даних та спеціалістів із навичками роботи з великими масивами інформації [7].

Таким чином, класифікація та аналіз джерел відкритих даних є ключовим етапом у розумінні їхнього потенціалу і обмежень. Це сприяє не лише їх ефективному застосуванню, але й подальшому розвитку галузі відкритих даних.

1.3 Методологія перевірки достовірності даних: ключові підходи та критерії

Перевірка достовірності даних є важливою складовою інформаційного аналізу, особливо в умовах широкого використання відкритих джерел даних (OSINT). Методологія перевірки охоплює кілька етапів, кожен з яких спрямований на забезпечення максимальної точності, надійності та обґрунтованості отриманої інформації.

Першим етапом у процесі перевірки є вибір джерел і засобів для збору інформації. Цей крок передбачає аналіз доступних платформ, таких як пошукові системи (Google, Bing), соціальні мережі (Facebook, LinkedIn, Twitter) та бази даних (державні реєстри, архіви судових рішень). Різноманітність джерел дає можливість охопити різні аспекти об'єкта дослідження та виявити потенційні джерела помилок чи викривлень. Важливим аспектом на цьому етапі є правильний вибір інструментів. Наприклад, інструменти для моніторингу новин, такі як Google Alerts, дозволяють автоматизувати процес збору нової інформації. Для поглибленого аналізу часто використовуються спеціалізовані платформи, такі як Maltego, OSINT Framework або SpiderFoot. Вибір інструментів залежить від характеру даних та кінцевих цілей перевірки [8].

На наступному етапі ключовим є структурований підхід до збору інформації. Дотримання систематичності допомагає уникнути пропусків важливих деталей. Важливо починати з перевірених джерел, таких як офіційні сайти або публічні реєстри, а потім переходити до аналізу менш надійних платформ, таких як соціальні мережі чи новинні сайти з низькою репутацією. Особливу увагу слід приділяти деталям. Наприклад, інформація про людину може включати фотографії, місця роботи або навчання, рецензії чи коментарі. Додаткові деталі, такі як погода на фото чи назви об'єктів у кадрі, можуть дати важливі підказки щодо часу або місця події.

Після збору інформації з різних джерел наступним кроком є її обробка та аналіз. Перевірка достовірності починається з оцінки джерела. Наприклад, дані,

отримані з офіційних урядових сайтів, зазвичай вважаються більш надійними, ніж інформація з соціальних мереж. Одним із критеріїв достовірності є час публікації. Свіжі дані зазвичай мають більшу цінність, тоді як застаріла інформація може втратити актуальність [9].

Контекст публікації також відіграє важливу роль – необхідно враховувати, з якою метою опубліковані дані та чи є джерело зацікавленим у їх спотворенні. Ефективність перевірки залежить від правильно сформульованих критеріїв, серед яких можна виділити об'єктивність, повторюваність, точність і повноту. Об'єктивність передбачає незалежність та незаангажованість джерела. Повторюваність означає, що інформація має підтверджуватися кількома різними джерелами. Точність вимагає, щоб дані відповідали фактам і були актуальними. Повнота передбачає достатність інформації для аналізу та прийняття рішень. Ці критерії допомагають виявити можливі суперечності в даних і оцінити їхню цінність.

Фінальним етапом є підготовка звіту, в якому узагальнюються результати перевірки та аналізу. Такий звіт має включати джерела, з яких отримані дані, оцінку їхньої надійності, висновки щодо достовірності та можливих обмежень використання отриманої інформації. Перевірка достовірності стикається з низкою викликів, таких як дезінформація, брак контексту та юридичні чи етичні обмеження. Дезінформація включає навмисно спотворені або фальсифіковані дані. Брак контексту означає, що дані можуть бути вирвані з контексту, що ускладнює їх інтерпретацію. Юридичні та етичні обмеження стосуються регулювання збору персональних даних, що може обмежувати доступ до певних джерел [10].

Ретельно розроблена методологія перевірки достовірності даних є важливим інструментом для підвищення якості аналітичної роботи. Вона забезпечує системність і обґрунтованість процесу, допомагаючи зменшити ризики прийняття рішень на основі ненадійної інформації. Завдяки таким підходам організації можуть оптимізувати процеси роботи з великими масивами даних, покращити стратегічне планування та зменшити ймовірність помилок у своїй діяльності.

1.4 Огляд сучасних інструментів OSINT

У світі, де інформація стає важливим ресурсом, інструменти розвідки з відкритих джерел (OSINT) займають ключову позицію в аналізі даних. Вони дозволяють збирати, структурувати й аналізувати дані з різних джерел, сприяючи побудові повної картини про об'єкт дослідження. Сучасні інструменти OSINT, такі як Maltego, SpiderFoot і OSINT Framework, забезпечують фахівцям з кібербезпеки, аналітикам і дослідникам ефективні методи отримання інформації.

Maltego є потужною платформою для OSINT, яка забезпечує широкі можливості аналізу та візуалізації даних. Її ключовими перевагами є інтеграція з 58 різними джерелами даних, здатність обробляти до мільйона об'єктів у базі та наявність ручного завантаження. Інструмент дозволяє створювати графіки різних типів: ієрархічні, кругові чи блочні, що полегшує аналіз складних взаємозв'язків.

Завдяки Maltego, фахівці з кібербезпеки, правоохоронні органи та групи довіри можуть швидко отримувати результати досліджень. Інструмент застосовується для аналізу даних у фінансових послугах, правоохоронній діяльності та багатьох інших галузях [11].

Maltego дозволяє проводити детальні дослідження для виявлення потенційних загроз. Наприклад, він може використовуватися для виявлення зв'язків між об'єктами, аналізу даних про кіберзлочинців або моніторингу активності в мережі. Також платформа надає доступ до навчальних матеріалів і курсів, таких як Maltego Foundation, що сприяє підвищенню професійних навичок користувачів. Інтерфейс Maltego є інтуїтивно зрозумілим, а результати дослідження у вигляді графів дозволяють швидко виявляти взаємозв'язки, які могли залишитися непоміченими при традиційному аналізі. Також підтримує інтеграцію з іншими OSINT-інструментами, такими як Shodan, що робить її особливо універсальною у роботі з великими масивами даних.На рисунку 1.1 зображено один із інферфейсних меню програми.

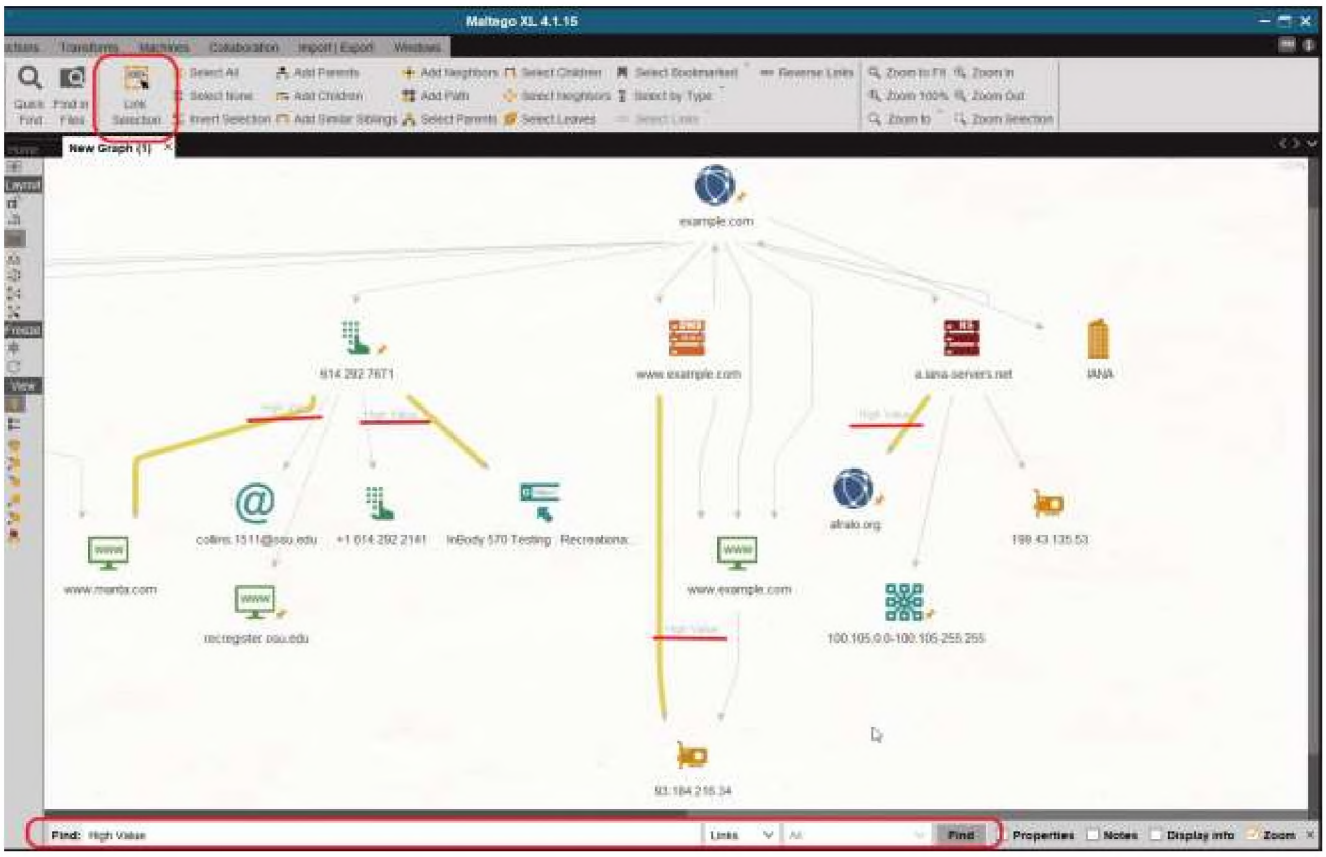

Рисунок 1.1 – Інтрефейс Maltego

SpiderFoot є багатофункціональним інструментом OSINT із відкритим вихідним кодом, який спеціалізується на зборі та аналізі інформації. Його функціонал включає роботу з IP-адресами, доменами, електронними адресами, телефонними номерами, іменами користувачів і навіть криптовалютними адресами. SpiderFoot підтримує понад 200 модулів, які забезпечують детальний аналіз та виявлення ключових деталей про об'єкти дослідження.

Інструмент пропонує два варіанти інтерфейсу: командний рядок і веб-інтерфейс. Останній має зручний графічний інтерфейс користувача, що дозволяє працювати з даними ефективно та інтуїтивно. SpiderFoot є чудовим інструментом для оцінки ризиків безпеки в організаціях, оскільки допомагає виявляти потенційно вразливі дані. SpiderFoot активно застосовується для виявлення витоків інформації, аналізу потенційних загроз та моніторингу активності в Інтернеті [12].

На наступному рисунку 1.2 зображено консольну версію інтерфейсу данного інструменту.

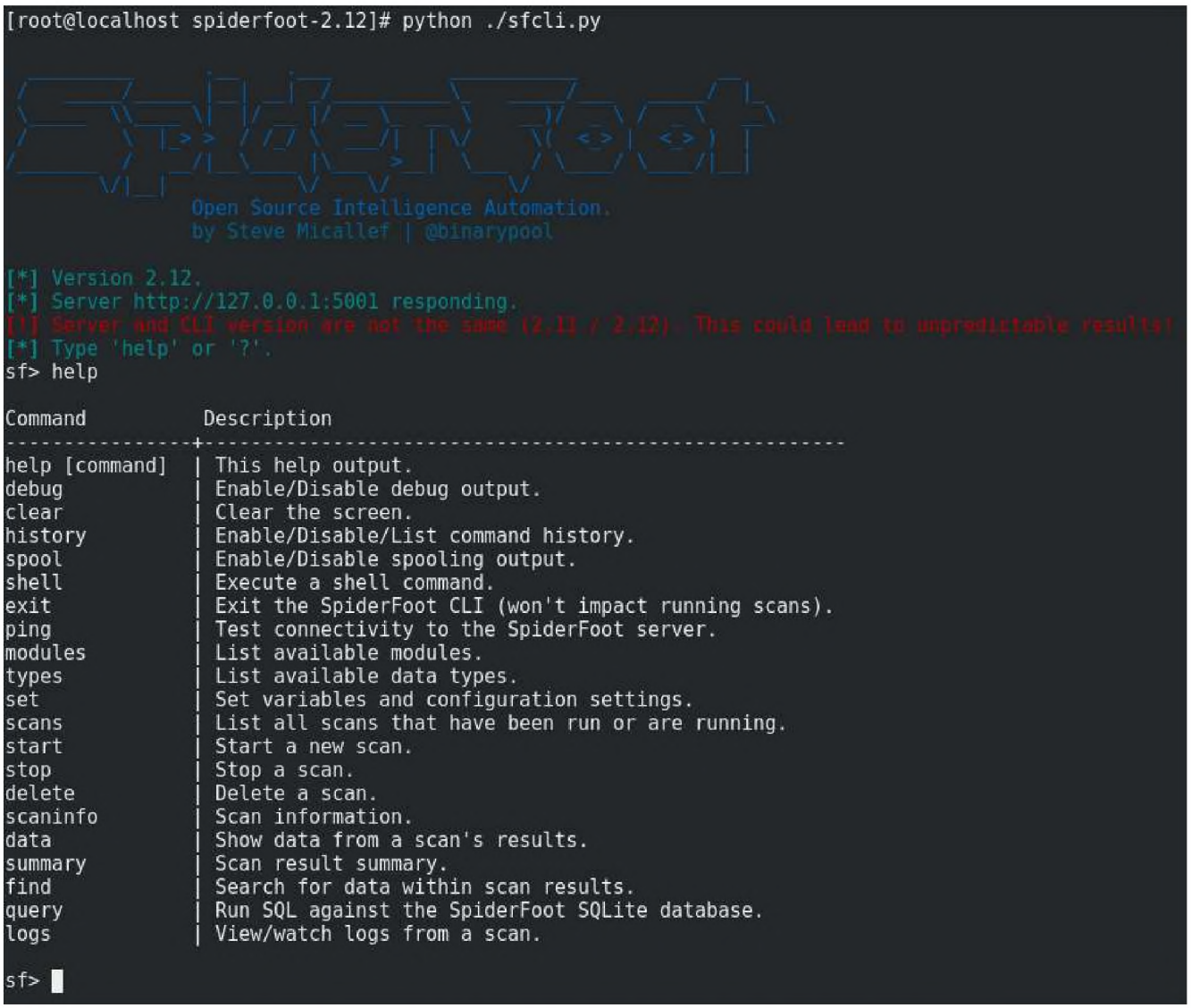

Рисунок 1.2 – Консольний інтерфейс SpiderFoot

Однією з ключових функцій SpiderFoot є можливість виконувати комплексний аналіз, поєднуючи дані з різних джерел для створення повного профілю об'єкта дослідження. Він також корисний для перевірки відкритих джерел організації на предмет наявності даних, що можуть стати причиною порушень безпеки. SpiderFoot має гнучкий веб-інтерфейс і можливість інтеграції з іншими платформами, що робить його зручним у використанні. Для більш складних сценаріїв він підтримує використання API, що дозволяє автоматизувати процеси збору та аналізу даних. Практичний досвід показав, що SpiderFoot є незамінним інструментом у задачах моніторингу загроз та ідентифікації ризиків. На

наступному рисунку 1.3 показано один із інтерфейсів інструменту який робить роботу з інструментом більш легкою.

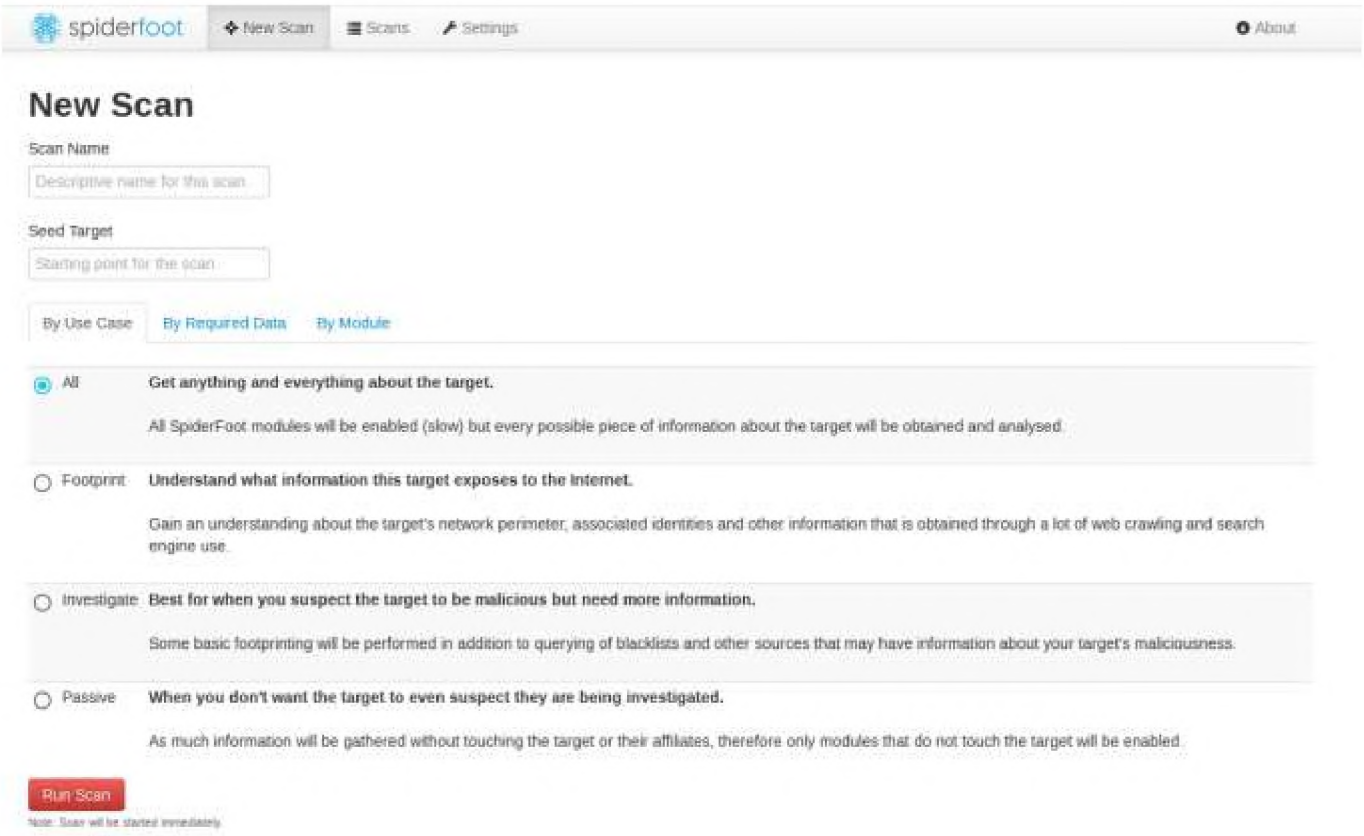

Рисунок 1.3 – Веб інтерфейс SpiderFoot

OSINT Framework є інтерактивним каталогом, який містить широкий спектр інструментів для збору та аналізу даних із відкритих джерел. Він включає джерела даних і корисні посилання на інструменти, які дозволяють зосереджуватися на конкретних аспектах пошуку, таких як реєстрація транспортних засобів, електронна пошта чи інші дані [13].

Цей ресурс є універсальним і підходить для різних операційних систем, що робить його доступним для широкого кола користувачів. OSINT Framework значно полегшує процес пошуку та сортування інформації, завдяки чому стає невід'ємним інструментом для розвідки.

OSINT Framework активно використовується як платформа для навчання та розвитку навичок у сфері OSINT. Він також служить ефективним інструментом для

початківців, надаючи чітко структуровані посилання на популярні інструменти та методи роботи з відкритими даними.

Використання інструментів OSINT, таких як Maltego, SpiderFoot і OSINT Framework, має велике значення для різних галузей. Вони сприяють підвищенню рівня кібербезпеки, забезпечують можливість швидкого аналізу даних та допомагають виявляти потенційні загрози. Завдяки розширеному функціоналу та доступності, ці інструменти є незамінними для роботи з великими обсягами інформації [14].

Очікується, що зростання ринку OSINT буде продовжуватися, що створює нові можливості для стартапів і розробників. Це також відкриває перспективи для подальшого розвитку технологій у галузі аналітики даних, етичного злому та бізнес-розвідки.

Таким чином, Maltego, SpiderFoot і OSINT Framework є одними з найефективніших інструментів для збору, аналізу та використання відкритих даних. Їхнє впровадження у професійну діяльність сприяє оптимізації процесів аналізу, забезпечуючи доступ до надійних і актуальних даних.

Сучасні інструменти OSINT пропонують широкий спектр можливостей для збору та аналізу інформації. Вибір конкретного інструменту залежить від мети дослідження, рівня знань користувача та необхідних функцій. Комбінація кількох інструментів дозволяє отримати найбільш повну та достовірну інформацію. Практичне застосування цих інструментів у завданнях OSINT демонструє, що сучасні технології є потужним засобом для перевірки інформації, збору даних і створення аналітичних звітів. Кожен із розглянутих інструментів надає унікальні можливості, які доповнюють один одного, що робить їх важливими елементами роботи аналітиків у різних галузях. Використання цих інструментів у комплексі дозволяє отримати найбільш повну картину досліджуваного об’єкта та забезпечити достовірність отриманої інформації [15].

На таблиці 1.2 вказано у яких сферах найкраще розкриваються дані інструменти.

Таблиця 1.2 – Інструменти OSINT та їхні сфери застосування

Інструмент	Основний функціонал	Сфера застосування
Maltego	Аналіз та візуалізація зв'язків між даними; робота з 58 джерелами; графічна візуалізація даних.	- розслідування кіберзлочинів; - моніторинг фінансових загроз; - виявлення зв'язків між суб'єктами даних.
SpiderFoot	Збір даних про IP-адреси, домени, електронні адреси, телефонні номери; понад 200 модулів.	- оцінка кіберзагроз; - виявлення вразливостей; - моніторинг витоків конфіденційної інформації.
OSINT Framework	Каталог інструментів для збору даних; структуровані посилання на джерела даних.	- навчання і розвиток навичок у сфері osint; - сортування і пошук специфічної інформації; - розвідка даних.

Данна таблиця допомагає побачити різницю між інструментами та вибрати відповідний для конкретних завдань.

1.5 Правові та етичні аспекти використання OSINT

Використання OSINT (Open Source Intelligence) – технологій для збору інформації з відкритих джерел – відкриває нові можливості в аналітиці, розслідуваннях та кібербезпеці. Проте важливо, щоб ця діяльність здійснювалася відповідно до правових норм і етичних стандартів, що гарантують захист приватності, дотримання законодавства та уникнення зловживань.

В Україні використання відкритих джерел регулюється низкою нормативних актів. Конституція України гарантує захист приватного життя, зокрема таємницю листування, телефонних розмов і кореспонденції (стаття 31). Крім того, стаття 32 забороняє збір та використання конфіденційної інформації без згоди особи, за винятком випадків, передбачених законом, і лише в інтересах національної безпеки. Закон України «Про захист персональних даних» регулює обробку персональної інформації, вимагаючи збереження її конфіденційності та використання виключно за згодою власника. Кримінальний кодекс України містить

положення, що передбачають відповідальність за порушення прав на конфіденційність та недоторканність приватного життя. Наприклад, стаття 182 карає незаконний збір чи розголошення приватної інформації, а стаття 361 забороняє несанкціоноване втручання в роботу інформаційних систем [16].

Незважаючи на доступність відкритих джерел, деякі аспекти використання OSINT можуть викликати правові проблеми, зокрема:

1. Порушення конфіденційності: використання OSINT для збору приватної інформації, наприклад, фотографій чи персональних даних, може бути розцінено як незаконне;

2. Авторське право: дані з соціальних мереж чи публічних баз повинні використовуватися з урахуванням авторських прав. Їх копіювання та подальше застосування без згоди власника є незаконним.

Дотримання законодавчих вимог передбачає забезпечення прозорості процесу збору інформації, верифікацію даних із відкритих джерел та відмову від використання інформації, яка може завдати шкоди особам або організаціям.

Основним етичним принципом роботи з відкритими даними є повага до приватності. Організації та окремі фахівці зобов'язані:

1. Отримувати дані тільки з відкритих джерел. Інформація, що вимагає доступу до захищених систем, не може використовуватися без дозволу;

2. Враховувати згоду осіб на збір даних. Якщо інформація поширюється публічно, це не завжди означає, що вона може бути використана без обмежень.

Зібрані дані мають застосовуватися виключно з законною метою, наприклад, для забезпечення безпеки, розслідувань або аналізу ризиків. Заборонено використовувати інформацію для шантажу, маніпуляцій чи нанесення шкоди.

Етичні принципи також передбачають ретельну перевірку отриманих даних. Помилкова інформація може призвести до порушення прав людини або до необґрунтованих звинувачень. Кожен, хто працює з OSINT, має усвідомлювати потенційні ризики і наслідки своєї діяльності, враховуючи як правові, так і етичні аспекти.

Таблиця 1.3 – Правові та етичні аспекти використання OSINT

Аспект	Опис	Приклади регулювання/рекомендацій
Конфіденційність	Забезпечення захисту персональних даних, що збираються з відкритих джерел, з урахуванням прав суб'єктів на приватність.	GDPR (ЄС), Закон України «Про захист персональних даних»
Юридичне використання даних	Дотримання законодавчих норм під час збору та аналізу даних, включаючи авторські права та заборони на несанкціонований доступ до систем.	Кримінальний кодекс України (ст. 361 – незаконне втручання у роботу комп'ютерних систем)
Етичні стандарти	Використання OSINT із дотриманням етичних принципів, що включають повагу до приватності осіб, недопущення маніпуляцій та шантажу.	Рекомендації Bellingcat з OSINT, професійні кодекси етики у сфері журналістики

Рекомендації для дотримання правових і етичних стандартів включають кілька ключових аспектів. Організації повинні підвищувати обізнаність співробітників, організовуючи навчання щодо законодавчих вимог і етичних принципів роботи з OSINT. Важливим є розроблення внутрішніх політик, що визначають правила збору, зберігання та використання даних. Використання сучасних OSINT-інструментів, таких як SpiderFoot або Maltego, сприяє автоматизації перевірки даних, мінімізує ризики збору конфіденційної інформації та забезпечує приватність [17].

Прозорість процесів передбачає пояснення мети збору інформації та можливість відмови від цього. Крім того, організаціям слід постійно моніторити зміни в законодавстві у сфері конфіденційності та авторського права, щоб оновлювати свої політики відповідно до актуальних вимог.

Правові та етичні аспекти використання OSINT є невід'ємною складовою ефективної роботи з відкритими джерелами. У контексті глобального розвитку інформаційних технологій необхідно впроваджувати нові підходи, які б поєднували технічний прогрес із повагою до прав і свобод людини.

Висновки до розділу 1

У першому розділі було розглянуто сутність і концепцію OSINT (розвідки за відкритими джерелами), яка є сучасним методом збору, аналізу та систематизації даних із загальнодоступних джерел. Особливу увагу було приділено розвитку цієї концепції в умовах цифровізації, поширенню інтернету та соціальних мереж. Також було визначено ключові етапи історичного розвитку OSINT та сучасного застосування у військовій, економічній, кібербезпековій сферах та журналістиці.

Проаналізовано різноманітні відкриті джерела даних, зокрема традиційні засоби масової інформації, соціальні мережі, державні ресурси, наукові й технічні публікації, корпоративні звіти та краудсорсингові платформи. Розглянуто їхні особливості, включаючи доступність, обсяг, актуальність, достовірність і формат.

Виконано класифікацію джерел відкритих даних і методів перевірки їх достовірності. Запропоновано структуру процесу перевірки, який включає вибір джерел і інструментів, систематичний збір інформації, її обробку та аналіз, визначення критеріїв достовірності та складання підсумкових звітів. Було визначено ключові критерії достовірності, зокрема об'єктивність, повторюваність, точність та повноту.

Розглянуто їх функціональні можливості, переваги й прикладне застосування у сферах кібербезпеки, фінансового моніторингу, виявлення загроз і навчання. У таблиці було систематизовано інформацію про основний функціонал та сфери застосування цих інструментів.

Таким чином, у розділі систематизовано інформацію про OSINT як ключовий інструмент у сучасній аналітичній діяльності, що забезпечує доступ до широкого спектра даних, сприяє підвищенню прозорості процесів та ефективності прийняття рішень у різних галузях.

РОЗДІЛ 2
РОЗРОБКА СИСТЕМИ ПЕРЕВІРКИ ДАНИХ З ВИКОРИСТАННЯМ ІНСТРУМЕНТІВ OSINT

2.1 Практичні аспекти використання OSINT

Open Source Intelligence (OSINT) надає практикам численні інструменти для збору та аналізу інформації із відкритих джерел, включаючи соціальні мережі, які є потужним ресурсом для досліджень. У цьому розділі будуть розглянуті практичні аспекти застосування OSINT у контексті популярних платформ, таких як Instagram і Facebook.

Instagram пропонує користувачам багатий набір функцій для збору інформації, який може бути використаний у рамках OSINT-аналізу. До ключових компонентів, які досліджуються в Instagram, належать:

Профіль користувача є основним джерелом загальної інформації. Аналізуючи біографічні дані, кількість підписників, підписок та публікацій, можна зробити висновки про інтереси, соціальні зв'язки та активність користувача. Вивчення публікацій, вподобань і коментарів дозволяє глибше зрозуміти його поведінку в мережі [18].

Функції Stories і Reels містять тимчасовий контент, який часто містить цінну інформацію, наприклад, місцезнаходження, участь у заходах або дані про зв'язки. Тимчасовий характер Stories робить їх важливим джерелом оперативної інформації, яку потрібно збирати в реальному часі.

Інструмент пошуку Instagram дозволяє ідентифікувати контент за хештегами, локаціями та іменами користувачів. Поглиблений аналіз здійснюється через функцію «Переглянути джерело сторінки», яка відкриває доступ до технічної інформації, наприклад, ідентифікатора користувача (ID) або точного часу публікації за допомогою Unix Timestamp.

Доступні онлайн-сервіси, як-от Save Free, дозволяють завантажувати профільні зображення, публікації та тимчасовий контент. Пошук за зображеннями

у глобальній мережі може допомогти визначити, чи зареєстрована особа в інших соціальних мережах.

Facebook є ще однією платформою, яка часто використовується у контексті OSINT. Незважаючи на історію пов'язану з витоками даних, платформа залишається цінним джерелом інформації завдяки даним, які користувачі добровільно надають у своїх профілях.

На Facebook доступна різноманітна інформація, зокрема особисті дані користувачів, такі як ім'я, вік, стать, освіта, місце роботи, політичні та релігійні вподобання. Також можна знайти контактну інформацію, зокрема номер телефону та електронну адресу. Інтереси та вподобання користувачів представлені через групи, заходи, музику й книги, які їм подобаються. Додатково можна переглянути список друзів, взаємодії та спільні інтереси, а також публікації, включаючи фотографії, відео та місця, які відвідав користувач.

Для аналізу контенту Facebook пропонує інструменти пошуку. Можна шукати людей за ім'ям, електронною поштою чи ідентифікаторами, групи та події за ключовими словами, тематикою або геолокацією. Контент, як-от фотографії, відео, статті та хештеги, доступний через пошук. Бізнес-сторінки компаній чи підприємств також можна знайти за категоріями [19].

Для збору технічної інформації з Facebook також використовується функція «Перегляд джерела сторінки». Цей метод дозволяє дізнатися ідентифікатор користувача (ID), який можна перевірити за допомогою онлайн-сервісів.

Facebook дозволяє користувачам обмежувати доступ до персональних даних через налаштування приватності. Це підкреслює важливість використання OSINT в рамках етичних норм і відповідно до законодавства.

На додаток до внутрішніх функцій соціальних мереж, існують спеціалізовані OSINT-інструменти для автоматизації аналізу:

– Maltego - для картографування зв'язків між користувачами;

– OSINT Framework - каталог інструментів для пошуку інформації;

– Shodan - для пошуку підключених до Інтернету пристроїв.

Практичне використання OSINT у соціальних мережах базується на аналізі відкритих даних, які доступні завдяки функціоналу платформ і спеціалізованих інструментів. Хоча зібрана інформація може бути корисною для розслідувань, її слід використовувати етично та відповідно до правових норм. OSINT є важливим інструментом для аналітиків, журналістів і дослідників, який дозволяє отримувати цінні інсайти з відкритих джерел [20].

2.2 Архітектура та алгоритм роботи системи перевірки

Система перевірки SpiderFoot є одним із потужних інструментів для автоматизованого збору інформації з відкритих джерел (OSINT). Вона дозволяє здійснювати глибокий аналіз даних, забезпечуючи високу швидкість та зручність. У цьому розділі детально розглянуто архітектуру та алгоритм роботи SpiderFoot, включаючи її функціональні можливості та підходи до налаштування.

SpiderFoot має модульну архітектуру, що дозволяє інтегрувати понад 100 джерел даних для аналізу IP-адрес, доменів, електронної пошти, імен та інших параметрів. Вона забезпечує:

– модульність: кожен компонент виконує певну функцію, наприклад, збір даних із соціальних мереж, аналіз DNS-записів або виявлення вразливостей;

– конфігурованість: користувачі можуть налаштовувати модулі, обираючи лише ті, які відповідають їхнім завданням. Це дозволяє оптимізувати процес сканування та зменшити час на аналіз;

– швидкість роботи: оптимізована бекенд-архітектура у SpiderFoot HX (платній версії) забезпечує швидкість сканування, що перевищує роботу базової версії в 10 разів.

Для інтеграції з іншими системами SpiderFoot підтримує API, що дозволяє автоматизувати процес збору та аналізу даних [21].

Робота SpiderFoot складається з кількох етапів, що забезпечують ефективний збір і аналіз інформації. Спочатку користувач визначає об’єкт дослідження,

наприклад, IP-адресу, домен чи електронну пошту, та обирає відповідні модулі для аналізу. Ці налаштування можна зберігати у профілі для подальшого використання.

Наприкінці SpiderFoot генерує детальні звіти, які можуть бути використані для командної роботи або інтеграції з іншими платформами. На наступному рисунку 2.1 зображен алгоритм роботи систем перевірки.

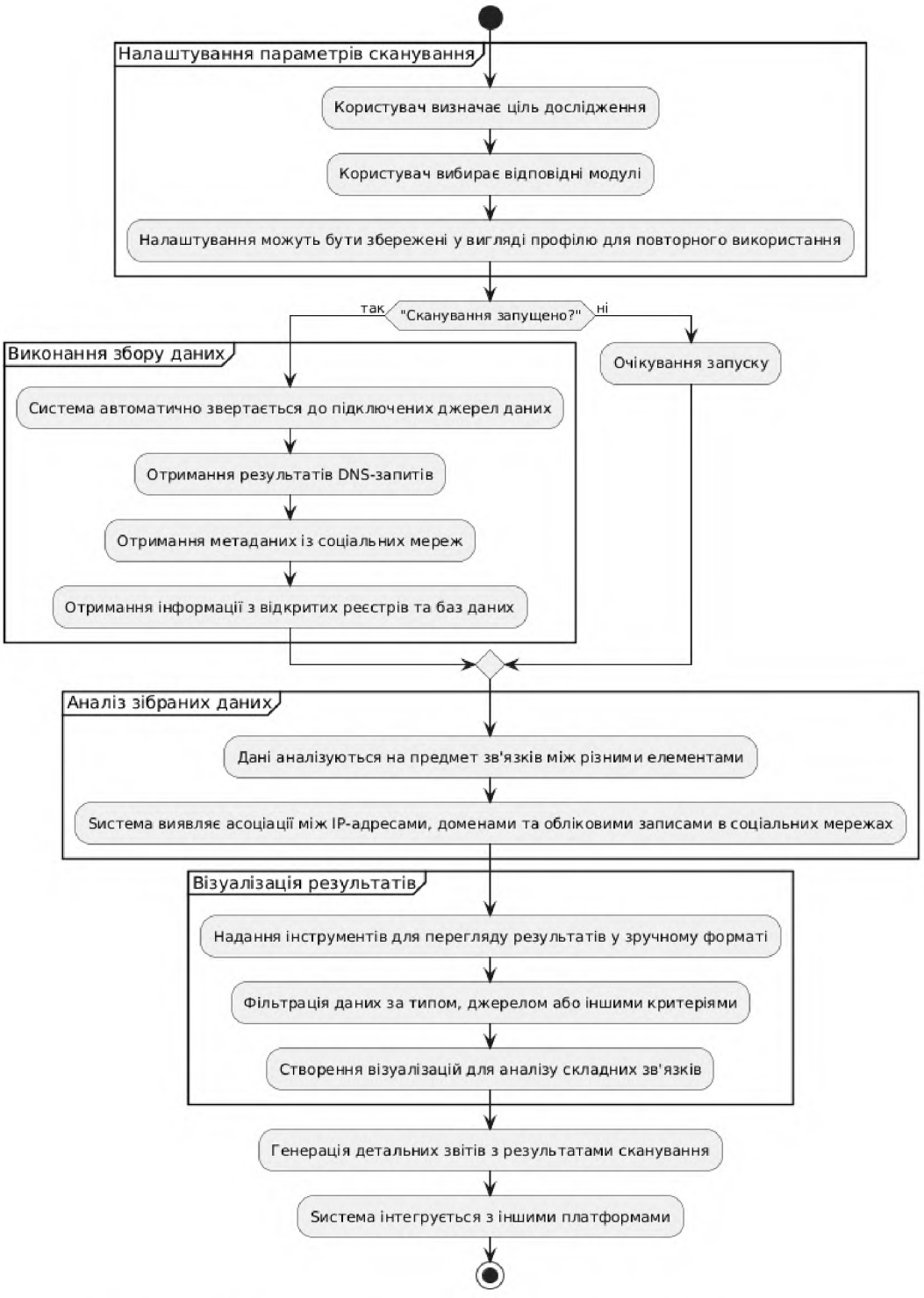

Рисунок 2.1 – Алгоритм роботи системи перевірки

На наступному етапі система автоматично звертається до джерел даних, щоб отримати необхідну інформацію, таку як результати DNS-запитів, метадані з соціальних мереж або відомості з відкритих реєстрів. Після цього відбувається аналіз зібраних даних, під час якого система шукає зв'язки між різними елементами, наприклад, між IP-адресами, доменами та акаунтами в соцмережах. Потім результативні дані представлені у вигляді візуалізацій, що дозволяють ефективно здійснити подальший аналіз [22].

SpiderFoot HX, комерційна версія системи, пропонує розширений функціонал для інтерактивних розслідувань, дозволяючи покроково збирати дані з повним контролем процесу. Система забезпечує автоматичний моніторинг OSINT шляхом запуску сканувань за графіком із фіксацією змін у даних. Вона надсилає сповіщення електронною поштою або через Slack про завершення сканувань чи виявлені зміни. Додаткові модулі дозволяють сканувати UDP-порти, визначати мову контенту, створювати знімки екранів соціальних профілів і вебсторінок.

SpiderFoot HX також забезпечує високий рівень безпеки завдяки двофакторній автентифікації, яка запобігає несанкціонованому доступу, ролям користувачів для керування доступом до функцій і інтеграції з TOR для анонімності сканувань. Ця система ефективно використовується для тестування на проникнення, допомагаючи виявляти вразливості й оцінювати ризики, загрозової розвідки для виявлення потенційних витоків даних, а також для командної роботи, де можливо виконувати колективні сканування з використанням ролей і спільних профілів.

Архітектура та алгоритм роботи SpiderFoot відображають її здатність адаптуватися до різних завдань. Завдяки модульній структурі, розширеним можливостям налаштування та інтеграції, система є універсальним інструментом для OSINT-досліджень, забезпечуючи високий рівень автоматизації та зручності. Моделювання процесу перевірки даних за допомогою OSINT-інструментів, таких як SpiderFoot і Maltego, дозволяє ефективно працювати з великими обсягами інформації, забезпечуючи високу швидкість і точність аналізу [23].

2.3. Впровадження методів аналізу даних на прикладі практичних сценаріїв

Аналіз даних стає невід'ємною складовою сучасних стратегій вирішення складних завдань у різних сферах, зокрема у сфері безпеки, журналістики, IT, а також у військових конфліктах. Одним із ефективних інструментів для збору, обробки та аналізу даних є Open Source Intelligence (OSINT). У цьому розділі розглянуто впровадження методів аналізу даних на основі практичних прикладів, зокрема в контексті поточного російсько-українського конфлікту.

OSINT, або розвідка з відкритих джерел, є методом пошуку, збору та використання інформації, яка доступна у відкритих реєстрах, на вебсайтах або у статистичних даних. Особливістю OSINT є легальність методів, адже всі джерела, що використовуються, є публічно доступними. Це дозволяє аналізувати дані без необхідності порушення правових норм.

У рамках повномасштабної війни в Україні агентство Molfar використовує OSINT для протидії російській пропаганді, перевірки фактів, геопросторової розвідки та ідентифікації військових злочинців. Спеціалісти Molfar також діляться своїми знаннями, навчаючи аналітиків з державних установ і громадських організацій [24].

Під час війни методи OSINT стають особливо важливими для збору інформації, що може впливати на стратегічні рішення. Один із прикладів – виявлення місцезнаходження ворожих баз. Процес складається з наступних етапів:

- пошук даних - аналіз інформації, яку публікують російські військові в соціальних мережах;
- обробка інформації - вивчення отриманих даних для виявлення потенційно корисних елементів;
- перевірка - переконання в достовірності інформації;
- передача даних - надання підтвердженої інформації Збройним Силам України;
- дії на основі даних - удари по виявлених цілях.

Цей процес ілюструє, як аналітика даних допомагає у виконанні військових завдань, водночас підкреслюючи важливість верифікації зібраної інформації.

Використання OSINT супроводжується низкою труднощів, пов'язаних із обсягом даних, адже мережа постійно генерує величезну кількість інформації, що ускладнює пошук ключових відомостей. Також існує проблема перевірки точності, оскільки отримана інформація може бути застарілою, неправдивою або викривленою. Не менш важливими є правові аспекти, оскільки закони щодо використання даних відрізняються між країнами, що потрібно враховувати під час аналізу.

Додатково виникають питання етичності, адже навіть за легального використання методів OSINT існують моральні межі, як-от недопустимість втручання у приватне життя без належних підстав [25].

Іноді дані можуть бути отримані лише через безпосередній контакт з людьми. У таких випадках використовується Human Intelligence (HUMINT), що передбачає отримання інформації від ключових осіб чи експертів. Це особливо актуально, коли дані є закритими або вимагають верифікації. Наприклад, агентство Molfar застосовувало HUMINT для отримання інформації про шпигунів, використовуючи комунікації під прикриттям.

Інтернет-користувачі відіграють важливу роль у забезпеченні безпеки, тому їм варто уважно ставитися до даних, які вони публікують. Зокрема, слід обережно розкривати інформацію про своє місцезнаходження, особисте життя або роботу, а також дані про родину чи друзів.

Злочинці та терористи можуть використати ці дані для своїх цілей, тому важливо двічі подумати перед публікацією. Це стосується не лише військових чи державних службовців, а й звичайних громадян.

Зростання популярності OSINT стимулює організацію навчальних подій, наприклад, зустрічей на конференціях, як-от IT Arena. Це платформа для обміну досвідом, що допомагає підвищувати рівень безпеки та технологічної обізнаності. Наприклад, під час зустрічі на тему «OSINT як кіберзахист від російської агресії» обговорювалися можливості OSINT у сфері кібербезпеки.

Впровадження методів аналізу даних на основі OSINT є важливим кроком у багатьох професійних сферах. На прикладі практичних сценаріїв, як-от аналіз інформації під час війни, можна побачити значущість OSINT у сучасному світі. Попри існування викликів, пов'язаних із обсягом даних, перевіркою точності та етикою, цей інструмент залишається потужним засобом для підвищення ефективності та безпеки. Завдяки навчанню та обміну досвідом із використання OSINT можна досягти вищого рівня як індивідуальної, так і національної безпеки.

2.4. Моделювання процесу перевірки даних: приклади застосування

Моделювання процесу перевірки даних є важливим етапом аналізу інформації, особливо у сучасному середовищі, де обсяг даних постійно зростає, а достовірність інформації часто викликає сумніви. Інструменти OSINT, такі як SpiderFoot і Maltego, дозволяють автоматизувати та ефективно виконувати перевірку даних, використовуючи відкриті джерела. У цьому розділі розглянуто приклади застосування таких інструментів та описано етапи моделювання процесу перевірки [26].

Процес перевірки даних у контексті OSINT охоплює кілька важливих етапів. Спочатку відбувається збір даних з відкритих джерел, таких як вебсайти, соціальні мережі, бази даних і різні інші ресурси. На наступному етапі зібрані дані систематизуються, після чого оцінюється їхня достовірність і релевантність для конкретного дослідження. Після цього проводиться верифікація інформації, що включає перехресний аналіз різних джерел для підтвердження отриманих відомостей.

Завершальним етапом є візуалізація даних, що дозволяє створити моделі зв'язків між елементами, полегшуючи розуміння їхньої структури і взаємозв'язків. Ключовими аспектами є автоматизація, модульність і можливість інтеграції з іншими інструментами. SpiderFoot і Maltego є яскравими прикладами таких інструментів, які підтримують весь процес перевірки.

SpiderFoot – це багатофункціональний інструмент для автоматизованого збору даних з відкритих джерел. доменів, електронної пошти, ідентифікаційних даних і навіть соціальних зв'язків.

Основні етапи роботи SpiderFoot:

- налаштування параметрів - користувач задає ціль дослідження (наприклад, IP-адресу) і вибирає модулі, які будуть активовані;
- сканування - система звертається до понад 100 джерел даних, отримуючи інформацію, яка включає доменну історію, записи DNS, метадані;
- аналіз результатів - дані групуються за категоріями, такими як тип джерела або природа інформації;
- формування звітів - інструмент створює деталізовані звіти, що можуть бути корисними для прийняття рішень. На наступному рисунку зображено загальний алгоритм процесу перевірки даних.

Рисунок 2.2 – Загальний алгоритм процесу перевірки даних

SpiderFoot може використовуватися для виявлення вразливостей у мережах, аналізу зв'язків між об'єктами або моніторингу змін у відкритих джерелах. Наприклад, у контексті кібербезпеки інструмент дозволяє швидко ідентифікувати потенційні ризики [27].

Maltego – ще один OSINT-інструмент, що спеціалізується на побудові графічних моделей зв'язків між даними. Його унікальність полягає у здатності інтерактивно візуалізувати складні мережі даних.

Етапи роботи з Maltego:

- визначення цілі - наприклад, аналіз домену для виявлення пов'язаних облікових записів.

- збір даних - інструмент автоматично використовує трансформації – модулі, які звертаються до відкритих джерел для отримання інформації.

- створення графів - дані представляються у вигляді графів, які демонструють зв'язки між різними об'єктами.

- аналіз графів - користувач аналізує отримані зв'язки, фільтруючи нерелевантні дані. На наступному рисунку зображена послідовність етапів роботи Maltego

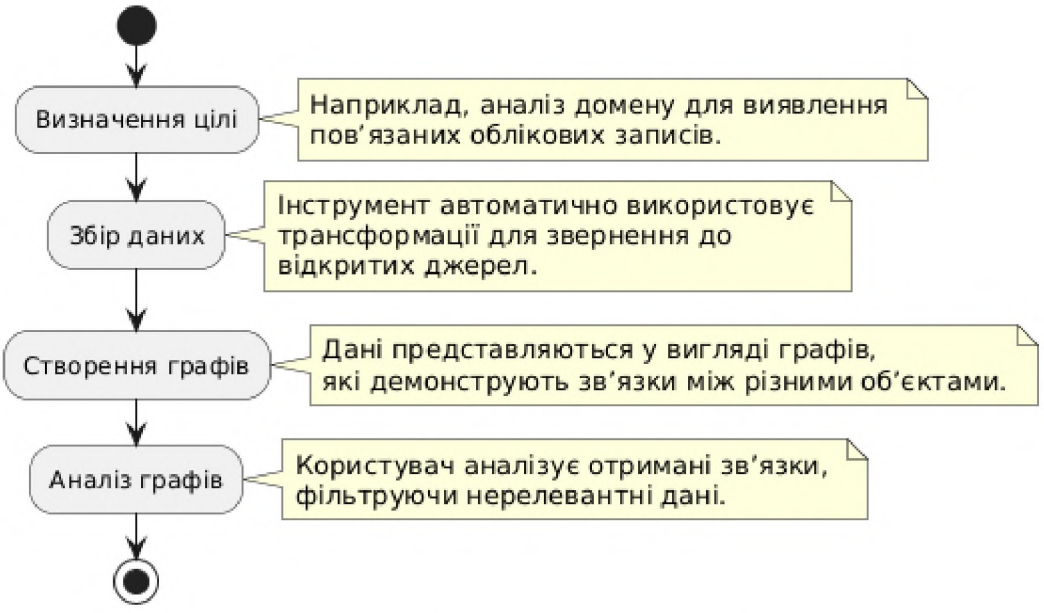

Рисунок 2.3 – Послідовність етапів роботи Maltego

Maltego є корисним для розслідувань, оскільки дозволяє швидко ідентифікувати ключових осіб або організації, пов'язані з досліджуваною метою. Наприклад, у розслідуваннях кіберзлочинів можна виявити зв'язки між IP-адресами, доменами і соціальними профілями [28].

Приклад 1. Перевірка кіберзлочинної активності. Уявімо, що аналітик розслідує атаку на корпоративну мережу. Використовуючи SpiderFoot, він отримує дані про IP-адресу атакувальника, що включають доменні зв'язки, геолокацію та наявні вразливості. Далі Maltego дозволяє візуалізувати зв'язки IP-адреси з іншими кіберзлочинцями чи організаціями, що дає змогу створити повну картину кіберзагрози.

Приклад 2. Верифікація інформації у розслідуванні. Журналіст досліджує діяльність певної компанії. Використовуючи Maltego, він виявляє зв'язки між компанією, її керівництвом та іншими організаціями. Додатково SpiderFoot допомагає перевірити наявність доменів, зареєстрованих на ту ж компанію, а також можливі витоки даних.

Попри те, що OSINT-інструменти значно полегшують перевірку даних, існують певні труднощі. Обробка великого обсягу інформації залишається складною задачею, оскільки навіть автоматизовані інструменти потребують фільтрації та аналізу. Додатково виникають питання щодо достовірності, оскільки зібрані дані можуть бути застарілими або неточними. Також слід враховувати правові обмеження, адже використання деяких методів OSINT регулюється законодавством.

Моделювання процесу перевірки даних за допомогою OSINT-інструментів, таких як SpiderFoot і Maltego, дозволяє ефективно працювати з великими обсягами інформації, забезпечуючи високу швидкість і точність аналізу. Ці інструменти забезпечують автоматизацію процесів збору, аналізу та візуалізації, що є незамінним у розслідуваннях, кібербезпеці та журналістиці. Водночас важливо враховувати можливі виклики, зокрема необхідність ретельної верифікації даних та дотримання законодавчих норм.

Дослідження у сфері OSINT, що стосуються кібербезпеки, переважно зосереджені на покращенні методів захисту від загроз. Проте рідко хто займається завданням ідентифікації кіберзлочинців. OSINT надає знання, які можуть стати основою для розслідування кіберінциденту: від аналізу дрібних деталей атаки до пошуку причин і мотивів. Завдяки цьому можна зрозуміти мотиви злочинців, встановити їхню методику дій та створити профіль зловмисника. Це пов'язано з розв'язанням так званої проблеми атрибуції – встановлення відповідальних за кібератаки.

Таблиця 2.1 – Інструменти OSINT та їхні сфери застосування

Етап	Опис	Інструменти
Формулювання завдання	Визначення цілей, типу даних і критеріїв перевірки	Не потребує інструментів
Збір даних	Збір інформації з відкритих джерел через OSINT-інструменти	SpiderFoot, TheHarvester, Shodan, Maltego
Аналіз	Перевірка достовірності отриманих даних	Sherlock, Google Dorking, Phishtank
Візуалізація	Побудова графів зв'язків і підготовка звітів	Maltego, SpiderFoot, MS Excel
Інтерпретація	Формулювання висновків і рекомендацій	Залежить від контексту

Збирання таких даних є початковою фазою процесу OSINT. Ці сліди служать основою для подальшого збору інформації з відкритих джерел. На цьому етапі OSINT починає формувати комплексну картину кіберінциденту. Дані, отримані на цих рівнях, значно збагачують етап аналізу в рамках OSINT. Наприклад, кореляція між новими даними та інформацією про раніше зафіксовані інциденти дозволяє розширити розуміння подій і краще оцінити контекст нападу [30].

Таким чином після наведених прикладів зрозуміло, що моделювання процесу перевірки даних є важливим кроком у систематизації роботи OSINT-інструментів. Застосування такого підходу може підвищити ефективність аналізу, уникнути дезінформації та уможливити прийняття обґрунтованих рішень у різних сферах.

2.5 Інтеграція OSINT у розслідування кібернападів

У сучасному світі забезпечення кібербезпеки стає одним із ключових обов'язків для компаній і організацій. Інтернет розширює доступ до цифрових ресурсів, водночас підвищуючи ризик кіберзагроз. Для захисту своїх активів організації активно впроваджують механізми для виявлення кіберінцидентів і реагування на них. Ефективне управління ризиками й інцидентами, що впливають на інформаційні системи, є необхідною складовою стратегії безпеки.

Оборона в кіберпросторі не обмежується лише використанням технологічних засобів, таких як брандмауери, системи виявлення вторгнень (IDS), запобігання вторгнень (IPS), SIEM-системи (управління подіями та інформацією безпеки) чи антивіруси. Хоча ці технології допомагають запобігти відомим загрозам, для глибшого розуміння та аналізу кіберінцидентів потрібна кіберрозвідка. Вона дозволяє збирати й аналізувати сліди, схеми та наслідки кібернападів. Ця діяльність, відома як "розвідка загроз", включає безперервний процес збору, обміну та аналізу даних. Використання такої розвідки значно підвищує ефективність традиційних механізмів захисту, збагачуючи їх актуальною інформацією для кращого управління ризиками та реагування на загрози.

Типова інформація, що використовується в судово-технічній експертизі або під час розслідувань, здебільшого технічна. Проте дані, які залишають після себе кіберзлочинці, можуть містити важливу інформацію. Ці дані варто аналізувати не лише за допомогою баз даних інцидентів, але й з використанням відкритих джерел: соціальних мереж, форумів, ЗМІ, технічних звітів і урядових документів. Використання цих джерел дозволяє отримати семантичну інформацію, яка допомагає здійснювати складні та далекоглядні висновки. Оскільки зловмисники використовують Інтернет як для проведення незаконних операцій (хакінг, фішинг, атаки на відмову в обслуговуванні, ботнети, крадіжка ідентичності тощо), так і в особистих цілях, дані з відкритих джерел можуть бути корисними для виявлення їхніх дій [31].

Дослідження у сфері OSINT, що стосуються кібербезпеки, переважно зосереджені на покращенні методів захисту від загроз. Проте рідко хто займається завданням ідентифікації кіберзлочинців. OSINT надає знання, які можуть стати основою для розслідування кіберінциденту: від аналізу дрібних деталей атаки до пошуку причин і мотивів. Завдяки цьому можна зрозуміти мотиви злочинців, встановити їхню методику дій та створити профіль зловмисника. Це пов'язано з розв'язанням так званої проблеми атрибуції – встановлення відповідальних за кібератаки.

Для демонстрації інтеграції OSINT використовується модель DML (Detection Maturity Level) Райана Стіллліонса, яка структурно представляє рівні складності виявлення кібератак. Компанії, які не інвестують у кібербезпеку, зазвичай здатні досягти лише початкових рівнів моделі. Натомість організації з високим рівнем технічної підготовки мають змогу аналізувати більш складні дані й підніматися до вищих рівнів абстракції. Рівень DML-1 охоплює найпростіші індикатори компрометації, наприклад, окремі символи у змінених файлах, значення в пам'яті або передані байти в мережі. На наступному рисунку 2.4 зображена інтеграція OSINT з DML моделями

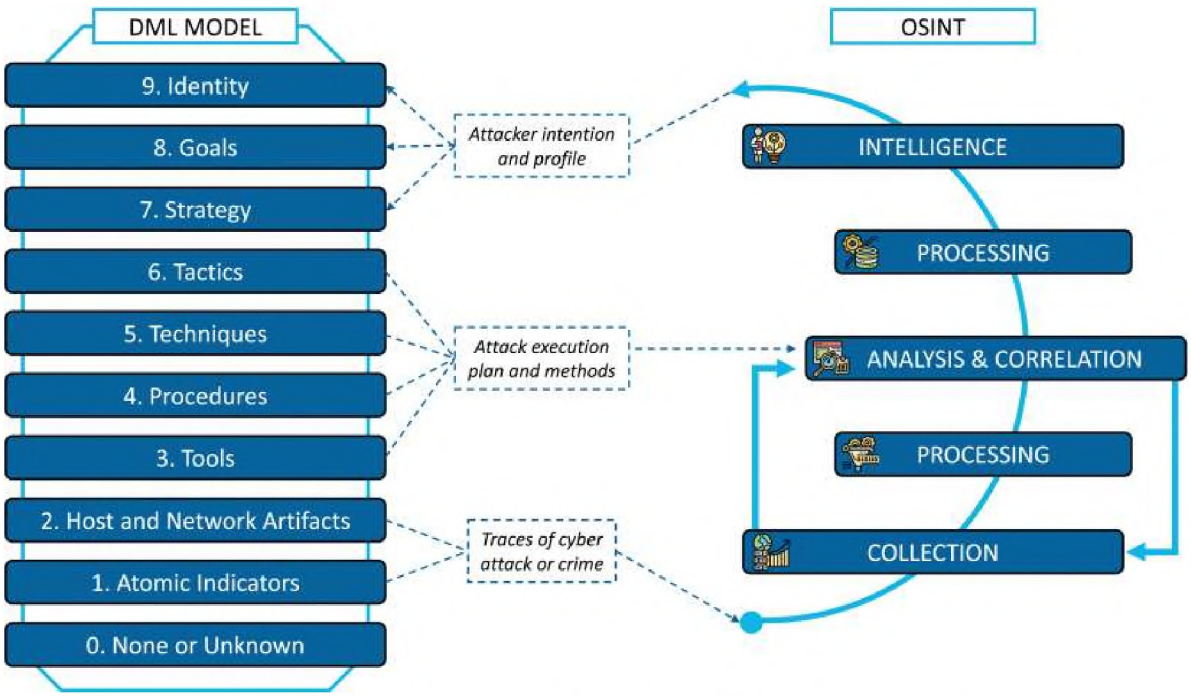

Рисунок 2.4 – Інтеграція OSINT з DML моделями

Модель складається з кількох рівнів. Початкові рівні, такі як DML-1 і DML-2, є базовими. Ці дані мають невелику самостійну цінність, проте у сукупності формують основу для наступного рівня. Рівень DML-2 зосереджений на артефактах хоста та мережі, таких як IP-адреси, доменні імена, журнали подій, хеш-значення або транзакції [32].

Збирання таких даних є початковою фазою процесу OSINT. Ці сліди служать основою для подальшого збору інформації з відкритих джерел. На цьому етапі OSINT починає формувати комплексну картину кіберінциденту.

Більш складними є рівні від DML-3 до DML-6. На рівні DML-3 аналізуються інструменти, які використовувались під час атаки. DML-4 включає дослідження процедур, здійснених зловмисником, тоді як DML-5 дозволяє зрозуміти специфічні техніки, використані під час нападу. DML-6 охоплює аналіз тактик – узагальнених підходів і стратегій, що використовувались під час нападу.

Дані, отримані на цих рівнях, значно збагачують етап аналізу в рамках OSINT. Наприклад, кореляція між новими даними та інформацією про раніше зафіксовані інциденти дозволяє розширити розуміння подій і краще оцінити контекст нападу.

Використання OSINT уможливлює досягнення найвищих рівнів моделі DML – від DML-7 до DML-9. На рівні DML-7 визначається стратегія кіберзлочинця, що дозволяє краще зрозуміти його плани. DML-8 зосереджується на конкретних цілях злочинця, що розкривають справжні мотиви нападу. Найвищий рівень, DML-9, передбачає ідентифікацію виконавця нападу, яким може бути як окрема особа, так і організація чи навіть держава. Хоча прямий доступ до таких даних є складним завданням, використання аналогій із попередніми подіями може допомогти у встановленні відносної атрибуції.

Інтеграція OSINT у процеси розслідування кіберінцидентів є перспективним напрямом, що значно підвищує ефективність протидії кіберзагрозам. OSINT дозволяє поєднати технічні деталі з даними з відкритих джерел, що дає змогу глибше зрозуміти контекст подій. Це підходить для профілювання зловмисників і

вдосконалення методів виявлення складних атак. Таким чином, OSINT стає важливим інструментом для досягнення нового рівня кібербезпеки.

Висновки до розділу 2

У розділі було розглянуто основні аспекти застосування OSINT-інструментів, таких як SpiderFoot і Maltego, у процесі перевірки та аналізу даних. Основну увагу приділено архітектурі цих систем, їхнім функціональним можливостям і алгоритмам роботи, що дозволяє автоматизувати процеси збору інформації з відкритих джерел і забезпечує їх ефективне використання в різних практичних сценаріях.

Проаналізовано особливості використання SpiderFoot, зокрема його здатність інтегрувати понад 100 джерел даних, що дає змогу виконувати комплексний аналіз IP-адрес, доменів, електронних адрес та інших об'єктів. Інструмент дозволяє виконувати сканування за заданими параметрами, систематизувати зібрану інформацію та створювати звіти для подальшого аналізу. Також було відзначено високу швидкість і можливості кастомізації, які забезпечують оптимізацію роботи з великими обсягами даних. Виконано огляд функціональності Maltego, зосереджуючись на його здатності візуалізувати зв'язки між даними. Maltego також забезпечує інтерактивність у процесі аналізу, що дозволяє адаптувати дослідження до змінних умов.

Виконано моделювання процесу перевірки даних на практичних прикладах, таких як виявлення кіберзагроз і верифікація інформації у журналістських розслідуваннях. Особливу увагу приділено етапам збору даних, аналізу, верифікації та візуалізації результатів.

Таким чином, у розділі було висвітлено ключові аспекти впровадження OSINT-методів у процесі аналізу даних, розглянуто переваги використання спеціалізованих інструментів та їх практичне застосування.

РОЗДІЛ 3
ОЦІНКА ЕФЕКТИВНОСТІ РОЗРОБЛЕНОЇ СИСТЕМИ ТА ПЕРСПЕКТИВИ РОЗВИТКУ

3.1 Тестування розробленої системи на реальних кейсах

Для демонстрації можливостей OSINT-інструментів було проведено тестування на прикладі домену, пов'язаного з електронною поштою. Було вибрали домен (.com), який асоціюється з електронною адресою visan38640@eoilup.com.

Мета тестування – визначити, чи є адреса підозрілою, та провести перевірку її використання в різних контекстах. Етапи тестування починаються з формулювання завдання а саме об'єкт аналізу: електронна адреса visan38640@eoilup.com.

Метою є з'ясування, чи використовується ця адреса на різних веб-сайтах, чи асоціюється вона з підозрілою активністю. Інструмент: SpiderFoot для автоматичного збору інформації та перевірки репутації [26].

Далі іде збір даних за допомогою SpiderFoot. Для цього процесу треба запустили SpiderFoot із такими параметрами Вхідний об'єкт: visan38640@eoilup.com

Активовані модулі:

- spiderfoot.sfwhois (Whois-аналіз);
- spiderfoot.sfipinfo (інформація про IP-адресу);
- spiderfoot.sfurlscan (аналіз згадок на веб-сайтах);
- spiderfoot.sfdatawatch (аналіз у базах даних витоків);

Результатом є згадки на сайтах: виявлено 10 веб-сайтів, на яких використовується адреса visan38640@eoilup.com. Сайти включають різноманітні сервіси: Соціальні мережі та реєстраційні портали а також форуми з сумнівною репутацією [33].

Whois-аналіз домен example.com зареєстрований понад 5 років тому, але власник приховує свої дані через анонімізацію Whois-запитів. При перевірці на

витоки знайдено згадки про visan38640@eoilup.com у базах даних витоків, також використовувалася у шахрайських схемах, згідно з кількома джерелами. Також домен має низький рейтинг у базах даних репутації.

Було використано OSINT Framework для ручного аналізу даних про адресу та домен. Проведено перевірку через інструменти для зворотного пошуку електронної пошти. Перевіривши наявність адреси в чорних списках (через модуль Email Reputation). Та використав сервіси перевірки доменів (DNS Dumpster, VirusTotal).

Результатами є реєстрація на сервісах виявлено, що електронна адреса була використана для створення облікових записів на підозрілих форумах. Знайдені згадки про можливе використання в фішингових кампаніях. Також адреса присутня у витоках даних із великих платформ. Пошук показав кілька сайтів, що використовують цю адресу у шахрайських цілях. Домен фігурує в списках доменів із сумнівною репутацією на VirusTotal.

На основі зібраних даних сформували висновки, що електронна адреса є підозрілою, оскільки використовувалася на форумах і сервісах із сумнівною репутацією. Згадується в базах даних витоків і має асоціації з фішинговими кампаніями. Рекомендовано уникати використання домену example.com для офіційної комунікації.

Також слід провести моніторинг подібних адрес через OSINT-інструменти для подальшого аналізу і заблокувати цей домен у корпоративних мережах [34].

Для побудови зв'язків між об'єктами використовували Maltego. Отримано граф, що демонструє зв'язки між доменом example.com, знайденими сайтами та репутаційними базами і взаємодію з IP-адресами, що використовуються для підозрілої активності. Інтерфейс Maltego є інтуїтивно зрозумілим, а результати дослідження у вигляді графів дозволяють швидко виявляти взаємозв'язки, які могли залишитися непоміченими при традиційному аналізі. Maltego також підтримує інтеграцію з іншими OSINT-інструментами, такими як Shodan, що робить її особливо універсальною у роботі з великими масивами даних.

На рисунку 3.1 зображено один з варіантів інтерфейсів інструменту.

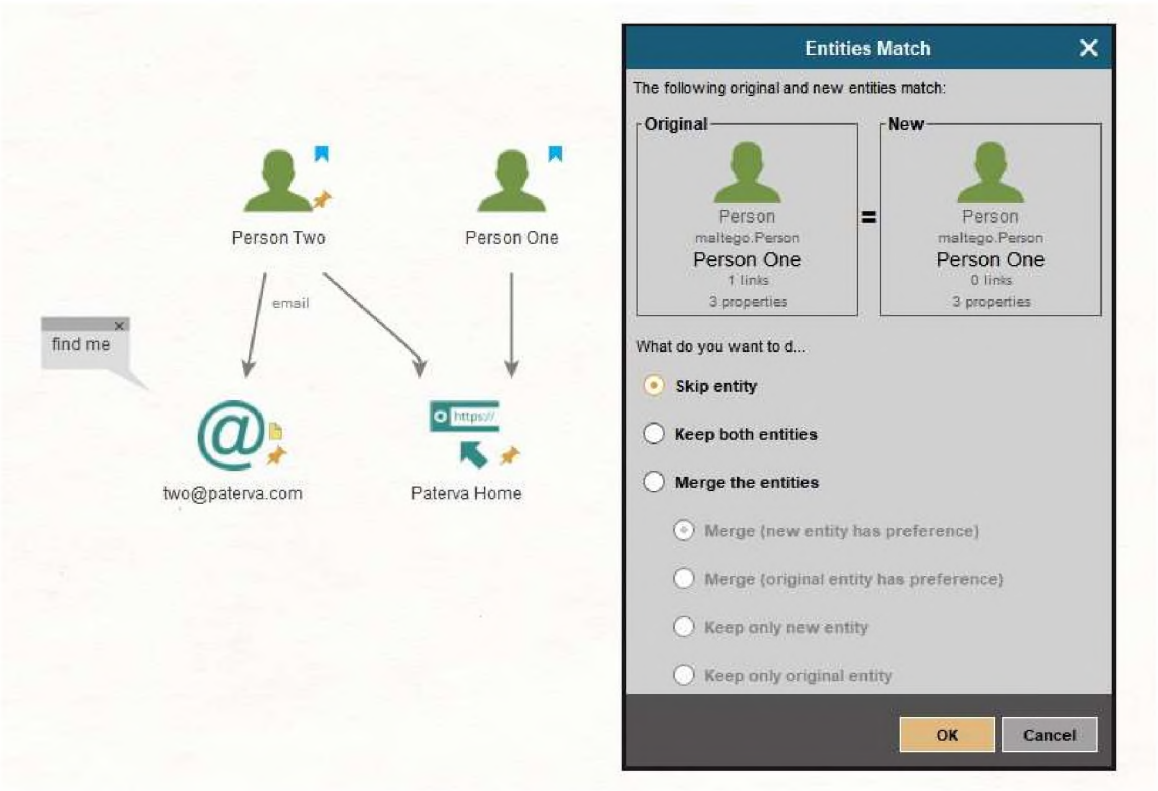

Рисунок 3.1 – Інтерфейс зв'язків

Для аналізу соціальних мереж Maltego може знайти та візуалізувати зв'язки між різними акаунтами, що дозволяє визначити ключових осіб у мережі або розкрити джерела поширення інформації. Тестування за допомогою SpiderFoot та OSINT Framework показало, що електронна адреса visan38640@eoilup.com має підозрілий статус. Інструменти OSINT дозволяють швидко виявити пов'язані ризики та надати конкретні рекомендації щодо безпеки [35].

Використання Maltego дозволило візуалізувати зв'язки між досліджуваною адресою, її доменом та іншими об'єктами, такими як IP-адреси та веб-сайти. Побудований граф продемонстрував наявність зв'язків із підозрілими ресурсами, що посилило висновки щодо високого рівня ризиків. Інструмент TheHarvester додатково зібрав згадки адреси на сайтах і показав її використання для реєстрації облікових записів на форумах із сумнівною репутацією. Завдяки цим графам можна уникнути або мінімізувати шкоду через обізнаність про небезпеку.

На рисунку 3.2 показано приклад вигляду побудованого графу зв'язків.

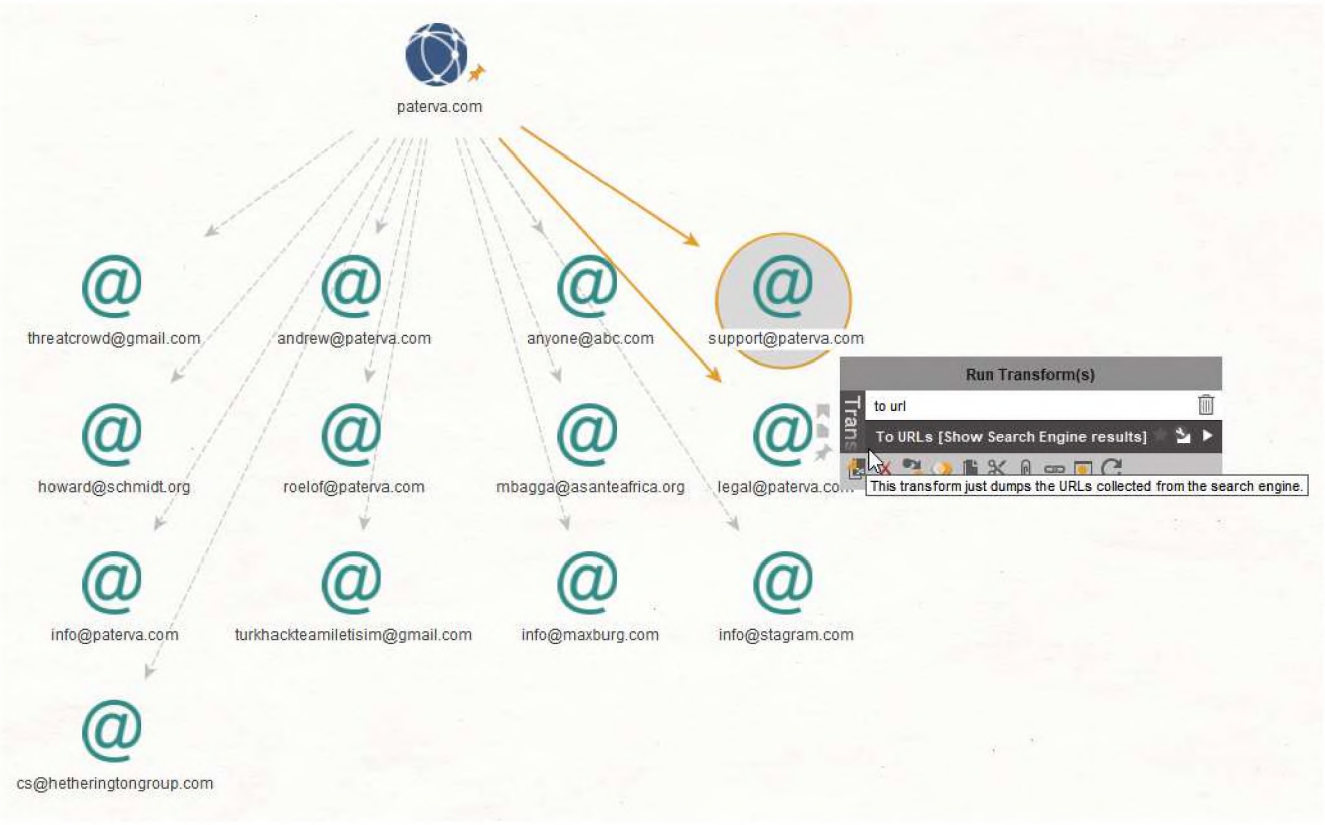

Рисунок 3.2 – Граф зв'язків між доменом та адресами

3.2 Аналіз результатів перевірки даних

На основі проведеного тестування електронної адреси visan38640@eoilup.com за допомогою інструментів SpiderFoot та OSINT Framework, були отримані численні результати, які дозволяють оцінити достовірність і безпеку цієї адреси.

У цьому розділі було проведено детальний аналіз отриманих даних, та виявлені основні ризики та зробити висновки.

1.Аналіз джерел інформації, виявлено згадки на сайтах. Адреса visan38640@eoilup.com була знайдена на 10 веб-сайтах. Типи сайтів соціальні мережі, реєстраційні платформи, форуми із сумнівною репутацією. Адресу

використовували для реєстрації облікових записів, а також як контактну інформацію у публікаціях із підозрілим змістом.

Домен example.com має низький рейтинг у репутаційних базах даних, що свідчить про його можливе використання у шкідливих активностях. Whois-аналіз показав приховування власника домену, що може свідчити про спробу уникнути ідентифікації. Електронна адреса виявлена у базах даних витоків, таких як Have I Been Pwned, також пов'язана з обліковими записами, зламаними у минулому.

Дані, зібрані через SpiderFoot, показують, що адреса використовувалася у фішингових кампаніях, і виявлено згадки на сайтах, які обговорюють шахрайські дії, де використовувалася ця адреса.

2. Оцінка ризиків. Шахрайство - використання адреси у фішингових кампаніях створює ризик для користувачів, які можуть довіряти її достовірності [36]. Компрометація: якщо адреса використовується для облікових записів у системах, що зберігають чутливу інформацію, це може призвести до витоку даних.

Репутаційні ризики - якщо адреса використовується компанією, це може вплинути на її репутацію через зв'язок із шахрайськими активностями. Інфраструктурні ризики: згадки про домен example.com у підозрілих джерелах можуть вказувати на його використання для розповсюдження шкідливого програмного забезпечення.

3. Візуалізація. Для виявлення ключових зв'язків і взаємозалежностей використовувалися такі підходи: Граф зв'язків: Побудовано граф за допомогою Maltego, який демонструє: Зв'язки між адресою visan38640@eoilup.com, підозрілими доменами та базами витоків.

Детальніше на рисунку 3.3 зображен граф зв'язків пов'язаних з піідозрілою адресою.

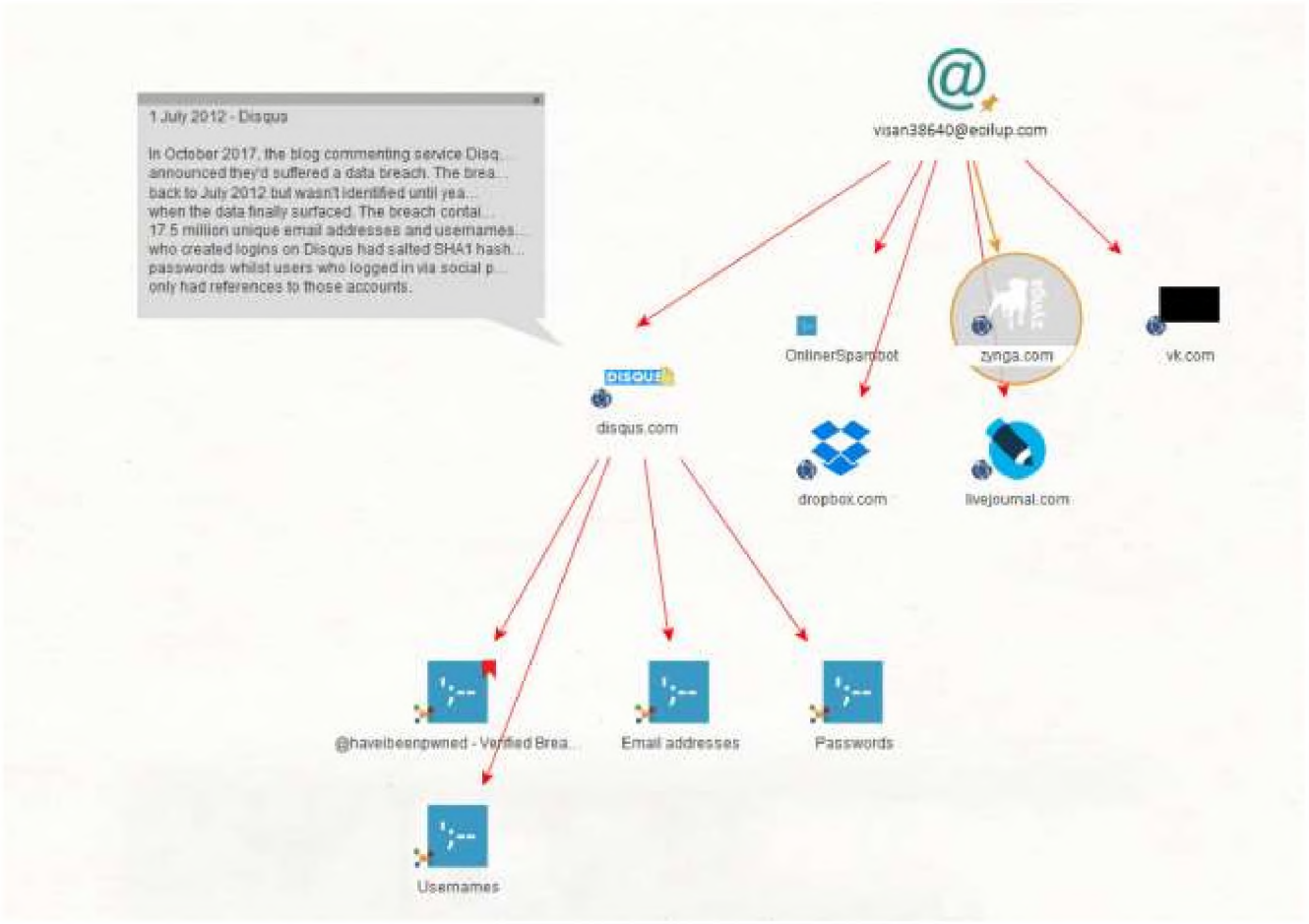

Рисунок 3.3 – Граф зв’язків з підозрілою адресою

Використання IP-адрес для діяльності домену. Зібрані дані дозволили відстежити періоди активності домену. Зокрема, домен був найбільш активним у рамках підозрілих кампаній протягом останніх двох років та структурування результатів.

Таблиця 3.1 – Ризики подізрілих доменів.

Ризик	Джерело	Ймовірність	Потенційний вплив
Використання у фішингу	Підозрілі сайти	Висока	Компрометація даних
Наявність у базах витоків	Have I Been Pwned	Висока	Витік облікових даних
Сумнівна репутація домену	SpiderFoot репутаційні модулі	Середня	Репутаційні ризики

Електронна адреса visan38640@eoilup.com має підозрілу репутацію через виявлені згадки у фішингових кампаніях, витоках даних і сумнівну репутацію

домену. Домен example.com використовується для активностей, які можуть становити загрозу для користувачів та організацій [37].

Рекомендовано блокування: заборонити доступ до домену example.com у корпоративних мережах. Моніторинг: використовувати OSINT-інструменти для постійного моніторингу підозрілих адрес, пов'язаних із компанією чи проектами. Обізнаність, провести навчання співробітників з метою уникнення взаємодії з адресами та доменами, які можуть бути небезпечними.

Подальше тестування: розширити перевірку на інші адреси, пов'язані з доменом, і проводити глибший аналіз IP-активності [29].

3.3 Порівняння ефективності використання різних інструментів OSINT

Ефективність інструментів OSINT залежить від специфіки завдання, типу даних для аналізу та особливостей функціоналу кожного інструмента. У цьому розділі розглянуто порівняльний аналіз SpiderFoot, OSINT Framework, Maltego, та TheHarvester на основі кейсів, проведених у попередніх розділах.

Для порівняння інструментів використані такі критерії:

- функціонал: набір доступних модулів та їх призначення;
- швидкість: час, необхідний для збору та аналізу даних;
- зручність: інтерфейс, налаштування та доступність для користувачів різного рівня;
- точність результатів: якість і релевантність отриманих даних;
- можливості інтеграції: робота з іншими інструментами або API.

Далі представлені кейси справ, де потрібно використати вище згаданні інструменти OSINT.

Кейс 1. Перевірка електронної пошти. SpiderFoot автоматично зібрав згадки адреси на форумах, перевірив витоки даних і репутацію домену. OSINT Framework надано список інструментів для пошуку вручну. Вимагає більше часу через необхідність індивідуальної перевірки. Maltego побудував граф зв'язків, але

потребував додаткових налаштувань для виявлення релевантної інформації. TheHarvester швидко зібрав згадки про електронну адресу та її використання на сайтах.

Таблиця 3.2 – Порівняння інструментів OSINT

Критерій	SpiderFoot	OSINT Framework	Maltego	TheHarvester
Функціонал	Автоматичний збір даних з багатьох джерел, широкий набір модулів	Каталог посилань на інші OSINT-інструменти	Потужні візуалізаційні можливості, інтеграція з API	Сканування поштових доменів, IP-адрес, імен
Швидкість	Швидкий автоматичний аналіз	Залежить від обраного інструмента	Залежить від розміру графу	Дуже швидкий аналіз поштових адрес та доменів
Зручність	Простий веб-інтерфейс, мінімальна конфігурація	Потрібен досвід для вибору релевантних інструментів	Складний інтерфейс для початківців	Командний рядок, потребує знання команд
Точність результатів	Висока точність при обранні відповідних модулів	Залежить від обраного інструмента	Висока, але потребує коректної конфігурації	Висока точність для вузькоспеціалізованих завдань
Можливості інтеграції	API для інтеграції з іншими системами	Інтегрується через сторонні інструменти	Інтеграція з багатьма джерелами через API	Обмежені можливості інтеграції

Кейс 2. Аналіз репутації домену. SpiderFoot надало вичерпну інформацію про домен, його реєстрацію, IP-адреси та згадки в базах даних витоків. OSINT Framework запропонувало інструменти для детального аналізу домену, але процес вимагає часу. Maltego побудував граф взаємозв'язків між доменом, IP-адресами та іншими об'єктами, підходить для візуалізації. TheHarvester швидко зібрав інформацію про домен та його використання в електронній пошті [38].

Кейс 3. Візуалізація та інтеграція SpiderFoot. Надає базову візуалізацію, але більше зосереджений на зборі даних. OSINT Framework відсутня візуалізація, потрібна інтеграція з іншими інструментами. Maltego найкращий вибір для графічного представлення зв'язків між об'єктами. TheHarvester не має

можливостей візуалізації, орієнтований на швидке збирання.

SpiderFoot є універсальним і підходить для автоматичного збору даних із різних джерел. Його головна перевага – автоматизація та широкий набір модулів. OSINT Framework ефективний як навігаційний інструмент для вибору релевантних програм, але вимагає ручної роботи. Maltego найкраще підходить для візуалізації складних зв'язків і використовується для детального аналізу, його недолік – складність у налаштуванні [39].

TheHarvester ефективний для швидкого збору даних про домени та електронні адреси, але має обмежені можливості для більш складного аналізу. Для початкового збору даних та їх автоматизації SpiderFoot – оптимальний вибір. Для складних випадків, що потребують візуалізації, варто використовувати Maltego. Для вузькоспеціалізованих завдань, як-от перевірка поштових адрес, найкраще підходить TheHarvester. OSINT Framework корисний для навчання та вибору додаткових інструментів. Кожен інструмент має свої сильні та слабкі сторони, тому вибір слід робити залежно від поставлених завдань та рівня підготовки користувача [40].

3.4 Перспективи розвитку OSINT для перевірки даних з відкритих джерел у різних сферах діяльності

Перспективи розвитку OSINT для перевірки даних з відкритих джерел у різних сферах діяльності (медіа, кібербезпека, бізнес)

Сфера використання Open Source Intelligence (OSINT), або розвідки з відкритих джерел, стрімко розвивається, пропонуючи широкі можливості для отримання та перевірки інформації. Це особливо важливо в умовах, коли цифрові дані набувають критичного значення у багатьох сферах діяльності. Сьогодні OSINT стає ключовим інструментом у медіа, кібербезпеці та бізнесі, адаптуючись до викликів і потреб сучасного світу.

Журналісти, які займаються розслідуваннями, активно застосовують OSINT для збору інформації з різноманітних відкритих джерел. Цей інструмент дозволяє їм перевіряти достовірність фактів, знаходити зв'язки між подіями чи суб'єктами

та підтверджувати інформацію за допомогою перехресного аналізу. Наприклад, аналіз профілів у соціальних мережах чи доступ до баз даних дозволяють журналістам виявляти невідповідності у публічних заявах [41].

Потенціал OSINT у медіа зростає завдяки цифровізації, що відкриває доступ до ще більшої кількості джерел інформації. Однак це також висуває нові виклики, пов'язані із захистом конфіденційності джерел та обробкою великих обсягів даних. Майбутнє OSINT у журналістиці залежить від розробки нових алгоритмів автоматизації та штучного інтелекту для ефективнішої обробки великих масивів інформації.

Кібербезпека є одним із напрямків, де OSINT відіграє особливо важливу роль. Фахівці з кіберзахисту використовують цей інструмент для виявлення потенційних загроз, аналізу тактик та методів зловмисників і реагування на інциденти.

Аналітики загроз застосовують OSINT для збору даних про методи атак, що дозволяє краще підготуватись до можливих інцидентів. Їх робота зосереджена на моніторингу соціальних мереж, форумів і навіть DarkWeb для ідентифікації можливих ризиків.

Мисливці за загрозами доповнюють OSINT власними дослідженнями, шукаючи приховані небезпеки у системах. Використання публічної інформації допомагає їм збагачувати внутрішні дані та встановлювати зв'язки між підозрілою активністю і вже відомими шаблонами атак [42].

Інші фахівці, такі як етичні хакери, застосовують OSINT для первинного аналізу цільового середовища, а пентестери імітують реальні атаки, що базуються на даних, отриманих із відкритих джерел. Усі ці напрямки демонструють, що ефективність OSINT у кібербезпеці залежить від інтеграції з іншими технологіями, включно зі штучним інтелектом та машинним навчанням [43].

У бізнес-середовищі OSINT стає потужним інструментом для аналізу ринкових тенденцій, конкурентів та ризиків. Бізнес-аналітики використовують загальнодоступні дані для створення стратегій, орієнтованих на ефективність і мінімізацію ризиків. Це включає збір інформації про ринкові умови, дії конкурентів

і нові можливості для зростання.

Інструменти OSINT допомагають компаніям:

- виявляти зміни у споживчих настроях через аналіз соціальних мереж;

- відслідковувати фінансові та юридичні ризики, використовуючи публічні реєстри та інші джерела;

- розробляти більш обґрунтовані стратегії ціноутворення.

Особливу роль OSINT відіграє у сферах, де потрібен точний аналіз репутації. Рекрутери, наприклад, перевіряють потенційних кандидатів, аналізуючи їхні профілі у соціальних мережах та професійний досвід. Цей підхід дозволяє не лише оцінити кваліфікацію, а й зрозуміти культурну відповідність кандидата [44].

Інший важливий аспект – це використання OSINT для ідентифікації можливих ризиків у фінансовій сфері. Аналітики AML (протидії відмиванню грошей) можуть відслідковувати підозрілі операції, знаходячи зв'язки між учасниками фінансових схем.

Майбутній розвиток OSINT залежить від інтеграції з новими технологіями. Автоматизація процесів збору та аналізу даних, впровадження алгоритмів машинного навчання та штучного інтелекту дозволять значно підвищити ефективність використання OSINT.

Для медіа це означає кращу перевірку інформації, у кібербезпеці – швидше реагування на загрози, а у бізнесі – ще більш детальний аналіз ринків. Водночас зростання популярності OSINT створює виклики, пов'язані із захистом приватності, етикою використання даних і відповідністю нормативним вимогам.

У підсумку, OSINT має значний потенціал у різних сферах діяльності. Його інтеграція з інноваційними технологіями забезпечує нові можливості для аналізу, моніторингу та перевірки інформації, роблячи цей інструмент незамінним у сучасному світі [45].

3.5 Оцінка економічної ефективності запропонованих рішень

Питання вартості операцій у сфері OSINT (розвідка з відкритих джерел) охоплює широкий спектр аспектів, включаючи використання технологій, наймання спеціалістів, амортизацію обладнання та можливі витрати на додаткові послуги, такі як залучення приватних детективів. Визначення таких витрат має ключове значення для оцінки економічної доцільності операцій, адже оптимізація витрат сприяє збереженню ресурсів організації або окремої особи.

OSINT є економічно вигідним інструментом, оскільки його основою є доступ до загальнодоступної інформації, зібраної з відкритих джерел, таких як інтернет, бази даних, соціальні мережі та публічні записи. Це дозволяє уникати значних витрат на спеціалізоване обладнання чи залучення закритих розвідувальних платформ. У порівнянні з традиційними методами збору інформації, які вимагають значних людських або технічних ресурсів, OSINT забезпечує більшу прозорість та контроль над витратами.

Прикладом економічної ефективності є те, що OSINT дозволяє оперативно отримувати важливі дані без необхідності залучення великої кількості працівників або придбання дорогого програмного забезпечення. Це, однак, не скасовує витрат на утримання обладнання та наймання кваліфікованих спеціалістів, які здатні ефективно працювати з такими джерелами інформації.

Одним із важливих аспектів оцінки вартості операцій є амортизація комп'ютерного обладнання.

Таблиця 3.3 – Вартість комп'ютерного обладнання.

Найменування	Ціна у долларах	Ціна в грн	Кількість
Комп'ютер	1202	50000	1

Для розрахунку амортизації можна застосувати лінійний метод, який є одним із найпоширеніших і найзручніших у практиці. Відповідно до цього методу, амортизація розраховується за формулою:

$$A = C \times H \div 100\%, \qquad \text{Формула 3.1}$$

де А – сума амортизаційних відрахувань за рік, грн;

С – середньорічна вартість основних засобів, грн;

Н – норма амортизаційних відрахувань, %.

Наприклад, якщо середньорічна вартість комп'ютера складає 50000 грн, а норма амортизації – 20%, то річна амортизація становитиме: А = 50000 × 20 ÷ 100 = 10000 грн.

Ця сума враховується при формуванні загальної вартості операцій OSINT. Зважаючи на часте використання сучасних обчислювальних пристроїв у цій сфері, амортизація обладнання є невід'ємною частиною загальних витрат.

У багатьох випадках до операцій OSINT можуть долучатися приватні детективи. Це стає актуальним, коли виникає потреба в зборі більш детальної інформації, зокрема у юридичних чи комерційних розслідуваннях. Вартість послуг приватного детектива залежить від складності завдання, термінів виконання та регіону, в якому надаються послуги.

Середня вартість послуг приватного детектива в Україні коливається в межах 400-1000 грн за годину роботи. У разі триваліших або складніших операцій може застосовуватися погодинна ставка або фіксована сума за виконання завдання. Наприклад, розслідування особистих справ, пошук інформації чи відстеження активності об'єкта може коштувати від 15000 до 50000 грн залежно від обсягу роботи.

Використання послуг приватних детективів дає можливість отримати додаткову експертизу та досвід, але водночас суттєво збільшує загальну вартість операції. Тому їх залучення доцільне лише у випадках, коли традиційних методів OSINT недостатньо.

До вартості операцій також можуть входити витрати на навчання персоналу, придбання програмного забезпечення для автоматизації OSINT-операцій, витрати на оплату підписок до платних баз даних тощо. У кожному конкретному випадку загальні витрати залежать від масштабу проекту, специфіки завдань і ресурсів, які використовуються.

Вартість операцій у сфері OSINT залежить від багатьох факторів, включаючи

амортизацію обладнання, оплату праці фахівців, можливі додаткові витрати на послуги приватних детективів чи програмне забезпечення. Висока економічна ефективність OSINT у порівнянні з іншими методами збору інформації забезпечує його популярність серед різних організацій. Однак оптимальне управління витратами залишається важливим завданням для забезпечення максимальної рентабельності операцій. До розрахунках було прийнято середній за грудень 2024 року курс долара по відношенню до гривні: $1 = 41,59 грн.

3.6 Оцінка ризиків та обмежень при використанні OSINT

Використання OSINT (розвідки з відкритих джерел) забезпечує широкі можливості для збору, аналізу та перевірки інформації, але супроводжується певними ризиками та обмеженнями. Основна дилема полягає у створенні безпечного інтернет-простору, де права на конфіденційність дотримуються, одночасно зберігаючи свободу слова та доступ до знань і інновацій [46].

Основні ризики при використанні OSINT:

- загроза деанонімізації, OSINT значно спрощує процес деанонімізації особистостей через відкриті джерела, такі як соціальні мережі, публічні бази даних і форуми. Інструменти дозволяють встановлювати зв'язки між акаунтами, адресами електронної пошти, IP-адресами та іншими персональними даними. Це створює потенційну загрозу для конфіденційності особистої інформації та може використовуватися у злочинних цілях;

- неправильне використання зібраної інформації. Зібрані через OSINT дані можуть бути використані для маніпуляцій, шантажу чи дезінформації. Відсутність належного контролю за зібраною інформацією може спричинити соціальні конфлікти або шкоду репутації окремих осіб чи організацій;

- недостовірність джерел, не всі відкриті джерела є достовірними. Використання ненадійної інформації без належної перевірки може призвести до помилкових висновків та рішень. Спеціалісти повинні ретельно перевіряти

джерела, щоб уникнути дезінформації;

- юридичні обмеження, закони про захист персональних даних, наприклад, GDPR у Європі або законодавство України, можуть обмежувати використання OSINT. Незаконний збір або обробка конфіденційної інформації може призвести до серйозних правових наслідків;

- етичні проблеми, повага до приватності осіб є ключовою етичною вимогою. Використання OSINT у розвідці або бізнес-аналізі повинно враховувати інтереси суб'єктів даних і уникати втручання в особисте життя.

Способи мінімізації ризиків:

- впровадження правових стандартів, користувачі OSINT повинні дотримуватись законодавства щодо захисту даних. Використання інструментів OSINT варто адаптувати до вимог місцевих і міжнародних норм;

- застосування технологій анонімності, для захисту від слідів цифрової активності рекомендується використовувати VPN, приватні браузери або анонімізуючі програми, такі як TOR. Також слід уникати доступу до ненадійних джерел, щоб мінімізувати ризики компрометації даних;

- навчання фахівців, спеціалісти, що працюють із OSINT, повинні постійно підвищувати свою кваліфікацію, проходити тренінги з кібербезпеки та етики роботи з даними;

- автоматизація перевірки достовірності, інструменти OSINT, такі як Maltego чи SpiderFoot, можуть допомогти перевіряти достовірність джерел. Це знижує ризик використання неправдивої інформації;

- забезпечення прозорості, організації повинні чітко визначати цілі використання OSINT, а також дотримуватися політик відкритості та прозорості в роботі з даними [43].

На наступній таблиці 3.4 зібрані та сформульовані способи мінімізації ризиків при використанні OSINT інструментів для більш безпечної роботи.

Таблиця 3.4 – Способи мінімізації ризиків

Ризик	Способи мінімізації	Інструменти/методи
Загроза деанонімізації	Застосування технологій анонімності.	VPN, TOR, приватні браузери.
Неправильне використання зібраної інформації	Забезпечення прозорості та чітке визначення цілей.	Політики відкритості та етичні стандарти.
Недостовірність джерел	Автоматизація перевірки достовірності.	Maltego, SpiderFoot.
Юридичні обмеження	Дотримання правових стандартів.	Законодавчі вимоги, місцеві та міжнародні.
Етичні проблеми	Навчання фахівців з етики роботи з даними.	Тренінги, курси з етики та кібербезпеки.

Рекомендації для користувачів OSINT полягають у наступному: постійно слідкуйте за новинами в галузі кібербезпеки та проходьте відповідні курси, щоб бути обізнаними у сфері безпеки; використовуйте лише відкриті джерела інформації та уникайте дій, що можуть порушувати права інших, дотримуючись етичних стандартів; інтеграція перевірених інструментів OSINT у ваші робочі процеси допоможе мінімізувати ризики; збирайте лише необхідну для досягнення мети інформацію, дотримуючись принципу мінімізації даних і уникаючи надмірного втручання в приватність [47].

Робота з OSINT вимагає врахування ризиків та обмежень, пов’язаних із конфіденційністю, етикою та правовими нормами. Основна дилема полягає в тому, як забезпечити безпечний простір в інтернеті, поважаючи права на конфіденційність, і при цьому не обмежувати свободу слова та доступ до знань. Розробка зрозумілих стандартів використання OSINT, навчання фахівців і автоматизація процесів допоможуть забезпечити баланс між ефективністю технології та безпекою користувачів [48].

Висновки до розділу 3

У розділі було розглянуто можливості OSINT-інструментів для аналізу та перевірки даних у цифровому просторі. Детально було проаналізовано тестування електронної адреси, проведене за допомогою інструментів SpiderFoot, Maltego,

OSINT Framework та TheHarvester, що дозволило оцінити їх ефективність у зборі інформації, виявленні підозрілих активностей і формуванні зв'язків між об'єктами.

Виконано практичну перевірку адреси visan38640@eoilup.com із метою виявлення її використання у різних контекстах та оцінки репутації. Для цього було використано автоматизовані модулі SpiderFoot, що зібрали дані про реєстрацію на веб-сайтах, зв'язки з шахрайськими кампаніями та присутність у базах даних витоків. Зокрема, виявлено, що адреса згадується на десяти веб-сайтах, серед яких форуми з сумнівною репутацією, а також пов'язана із фішинговими активностями та витоками чутливих даних.

Whois-аналіз домену example.com показав приховування інформації про власника, що може свідчити про наміри уникнути ідентифікації. Додатково оцінено репутацію домену через бази даних, такі як VirusTotal, де він фігурує у списках із сумнівною репутацією. За допомогою інструменту Maltego було побудовано граф зв'язків між доменом, виявленими IP-адресами та іншими об'єктами, що дозволило візуалізувати можливі схеми шахрайських дій.

На основі отриманих даних виконано оцінку ризиків, включаючи загрози шахрайства, компрометації даних та репутаційні ризики для організацій. Було встановлено, що використання адреси у корпоративних цілях є небажаним через її асоціацію із підозрілими активностями. Запропоновано рекомендації щодо блокування домену example.com у корпоративних мережах, а також моніторинг подібних адрес із використанням OSINT-інструментів.

Проведено порівняльний аналіз функціоналу використаних інструментів. SpiderFoot визнано універсальним для автоматичного збору даних із різноманітних джерел, Maltego відзначено як найкращий інструмент для візуалізації складних зв'язків, OSINT Framework охарактеризовано як довідковий інструмент для вибору програм, а TheHarvester – для швидкого збирання даних про домени та електронні адреси.

У підсумку, розділ демонструє, що ефективність OSINT-інструментів значною мірою залежить від конкретних завдань. Для автоматизації збору даних рекомендовано SpiderFoot, для графічного представлення – Maltego.

ВИСНОВКИ

У роботі була поставлена і вирішена актуальна задача дослідження можливостей OSINT (Open Source Intelligence) для збору, аналізу та перевірки даних із відкритих джерел у різних сферах діяльності.

1. Виконано аналіз сучасного стану та концепції OSINT. Встановлено, що цей метод є універсальним інструментом для отримання інформації з відкритих джерел, таких як медіа, соціальні мережі, державні ресурси та комерційні бази даних. Визначено, що OSINT застосовується у кібербезпеці, правоохоронній діяльності, економічному аналізі та журналістських розслідуваннях. Особливу увагу було приділено історичному розвитку OSINT і його актуальності у сучасному світі.

2. Досліджено джерела відкритих даних та їх класифікацію. Було визначено основні категорії даних: мас-медіа, державні ресурси, наукові публікації, корпоративні звіти та краудсорсингові платформи. Проаналізовано їх особливості, зокрема доступність, актуальність і достовірність. Наголошено на проблемах перевірки точності отриманих даних, а також на необхідності створення інфраструктури для ефективного використання цих ресурсів.

3. Описано методологію перевірки достовірності даних у контексті OSINT. Розглянуто ключові етапи: вибір джерел, систематичний збір даних, аналіз інформації, формування критеріїв достовірності та створення звіту. Особливу увагу приділено важливості об'єктивності та повторюваності даних для забезпечення їхньої надійності.

4. Проведено огляд сучасних інструментів OSINT, таких як Maltego, SpiderFoot та OSINT Framework. Встановлено, що кожен із цих інструментів має свої переваги та сферу застосування. Maltego ефективний для візуалізації складних зв'язків, SpiderFoot забезпечує автоматизований збір даних, а OSINT Framework є довідковим ресурсом для вибору спеціалізованих інструментів.

5. Розглянуто практичний кейс перевірки електронної адреси за допомогою OSINT-інструментів. На прикладі тестування адреси visan38640@eoilup.com

проаналізовано її репутацію та виявлено зв'язки з підозрілими активностями. Встановлено, що інструменти OSINT, такі як SpiderFoot та Maltego, дозволяють ефективно збирати інформацію, формувати зв'язки між об'єктами та оцінювати ризики.

Проведений аналіз у роботі дозволив сформувати наступні висновки. OSINT є ефективним і економічно доцільним методом збору та аналізу інформації з відкритих джерел. Його інтеграція в кібербезпеку, журналістику, економічну діяльність та інші сфери дозволяє покращити якість рішень і забезпечити прозорість процесів.

На основі отриманих висновків запропоновано наступні рекомендації щодо використання OSINT: розвивати інфраструктуру для аналізу відкритих даних, впроваджувати сучасні інструменти OSINT у корпоративних і державних структурах, а також забезпечувати навчання спеціалістів у цій сфері.

Таким чином, поставлені задачі розв'язано у повному обсязі. Напрямком подальших досліджень є розширення можливостей OSINT через використання штучного інтелекту та автоматизації процесів аналізу даних.