ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

« Дослідження шляхів та розроблення рекомендацій щодо розслідування кіберзлочинів за допомогою OSINT »

зі спеціальності *125 Кібербезпека*
(код, найменування спеціальності)

освітньо-професійної програми *Інформаційна та кібернетична безпека*
(назва програми)

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

_____ Лисенко Антон
(підпис)

Виконав: здобувач вищої освіти групи БСД-43

_____
(прізвище, ім'я)

Керівник асистент БОЙКО Анна
(науковий ступінь, вчене звання, прізвище, ім'я)

Рецензент _____
(науковий ступінь, вчене звання, прізвище, ім'я)

Київ 2024

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

Кафедра Інформаційної та кібернетичної безпеки
Ступінь вищої освіти Бакалавр
Спеціальність 125 Кібербезпека
Освітньо-професійна програма Інформаційна та кібернетична безпека

ЗАТВЕРДЖУЮ
Завідувач кафедри ІКБ
_____ Галина ГАЙДУР
“___” _____ 2024 року

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Лисенко Антону Сергійовичу
(прізвище, ім’я)

1. Тема кваліфікаційної роботи: «Дослідження шляхів та розроблення рекомендацій щодо розслідування кіберзлочинів за допомогою osint

керівник кваліфікаційної роботи Бойко Анна, асистент
(прізвище, ім’я, науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від «___» _____ 2024 року № ____.

2. Строк подання здобувачем вищої освіти кваліфікаційної роботи 31.05.2024 р.

3. Вихідні дані до кваліфікаційної роботи Рішення OSINT
наукова та технічна література, експлуатаційна документація, нормативні документи, міжнародні стандарти.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Дослідження проблеми розслідування кіберзлочинів
2. Аналіз методів та засобів розслідування кіберзлочинів
3. Розробка рекомендацій щодо застосування засобів розслідування

5. Перелік графічного матеріалу
Презентація PowerPoint.

6. Дата видачі завдання 15.04.2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ зп	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Визначення актуальності кіберзлочинів.	10.02.2024 р.	
2.	Аналіз існуючих інструментів OSINT.	20.02.2024 р.	
3.	Аналіз підходів до проведення OSINT.	01.03.2024 р.	
4.	Розроблення рекомендацій щодо застосування методів та засобів розслідування кіберзлочинів.	01.04.2024 р.	
5.	Практична реалізація пошу по фото.	10.04.2024 р.	
6.	Оформлення результатів дослідження.	01.05.2024 р.	
7.	Підготовка доповіді до захисту.	31.05.2024 р.	

Здобувач вищої освіти _____ Лисенко Антон
(підпис) *(ім'я, прізвище)*

Керівник кваліфікаційної роботи _____ Анна БОЙКО
(підпис) *(ім'я, прізвище)*

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну роботу

здобувача Лисенко Антона

на тему: «Дослідження шляхів та розроблення рекомендацій щодо розслідування кіберзлочинів за допомогою OSINT»

Актуальність: Кіберзлочини є однією з найбільших загроз сучасного цифрового світу, і ефективне розслідування таких злочинів потребує використання передових методів і технологій. Використання OSINT (Open Source Intelligence) дозволяє збирати й аналізувати інформацію з відкритих джерел, що може бути надзвичайно корисним для ідентифікації кіберзлочинців, розкриття їхніх методів та запобігання майбутнім атакам. Тема кваліфікаційної роботи є актуальною, оскільки вона спрямована на підвищення ефективності розслідування кіберзлочинів, що є важливим для забезпечення кібербезпеки.

Позитивні сторони:

У роботі детально розглянуто поняття та важливість OSINT у контексті розслідування кіберзлочинів, що дозволяє зрозуміти основні принципи та переваги цього підходу.

Проведено аналіз існуючих інструментів та методів OSINT, що можуть бути використані для розслідування кіберзлочинів, зокрема для збору, аналізу та інтерпретації даних.

Запропоновано рекомендації щодо застосування OSINT у практичних ситуаціях розслідування кіберзлочинів, що базуються на реальних кейсах та прикладах.

Висновки роботи є змістовними та обґрунтованими, а графічний матеріал якісно оформлений і добре ілюструє основні положення роботи.

Недоліки:

У кваліфікаційній роботі бажано було б додати більше прикладів реальних кейсів розслідування кіберзлочинів з використанням OSINT, що підсилило б практичну цінність роботи.

Дослідження могло б включати більш детальний аналіз правових аспектів використання OSINT, оскільки це є важливою складовою при зборі інформації з відкритих джерел.

Відзначене зауваження не впливає на загальну позитивну оцінку кваліфікаційної роботи.

Висновок: Враховуючи недоліки, кваліфікаційна робота заслуговує оцінку **“добре”**, а здобувач(ка) **Лисенко Антон** – присвоєння кваліфікації бакалавр з кібербезпеки за спеціалізацією Інформаційна та кібернетична безпека.

Рецензент:

(науковий ступінь, вчене звання)	*(підпис)*	*(ім’я, прізвище)*

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

ПОДАННЯ
ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ

на здобуття освітнього ступеня бакалавра

Направляється здобувач Лисенко Антон до захисту кваліфікаційної роботи
(прізвище, ім'я)

спеціальності 125 Кібербезпека
освітньо-професійної програми Інформаційна та кібернетична безпека
(шифр і назва спеціальності)

на тему: «Дослідження шляхів та розроблення рекомендацій щодо розслідування кіберзлочинів за допомогою OSINT».

Кваліфікаційна робота і рецензія додаються.

Директор інституту _____ Віталій САВЧЕНКО
(підпис) *(ім'я, прізвище)*

Висновок керівника кваліфікаційної роботи

Здобувач ***Лисенко Антон*** обрав тему роботи, метою якої було дослідити методи та засоби аналізу шкідливого програмного забезпечення для реагування на кіберінциденти. Перелік використаних джерел свідчить про вміння здобувачем розбиратись в наукових питаннях та застосовувати їх при дослідженнях. Під час виконання кваліфікаційної роботи ***Лисенко Антон*** показав добру теоретичну та практичну підготовку, вміння самостійно вирішувати питання і робити висновки. Роботу виконував сумлінно, акуратно та вчасно за планом.

Все це дозволяє оцінити виконану кваліфікаційну роботу здобувача **Лисенко Антон** на оцінку **"добре"** та присвоїти йому кваліфікацію бакалавр з кібербезпеки за спеціалізацією Інформаційна та кібернетична безпека.

Керівник кваліфікаційної роботи _____ Анна БОЙКО
(підпис) *(ім'я, прізвище)*
"____" _____ 2024 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач **ЛИСЕНКО Антон** допускається до захисту даної кваліфікаційної роботи в Екзаменаційній комісії.

Завідувач кафедри Інформаційної та кібернетичної безпеки
(назва)

_____ Галина ГАЙДУР
(підпис) *(ім'я, прізвище)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи: 59 сторінки, 16 рисунків, 16 джерел.

Об'єкт дослідження – процеси розслідування кіберзлочинів.

Предмет дослідження – методи та засоби розслідування кіберзлочинів за допомогою OSINT.

Мета роботи – дослідити процес розслідування кіберзлочинів за допомогою OSINT для отримання результатів, на основі яких можна ефективно виявляти та попереджати кіберзлочини.

Методи дослідження – інструменти для збору та аналізу інформації з відкритих джерел, використання OSINT для ідентифікації та розслідування кіберзлочинів.

OSINT відіграє ключову роль у розслідуванні кіберзлочинів, забезпечуючи доступ до великої кількості інформації з відкритих джерел, що дозволяє швидко ідентифікувати потенційні загрози та злочинців.

В роботі досліджено проблему розслідування кіберзлочинів за допомогою OSINT, визначено його мету та завдання. Проведено аналіз існуючих методів та засобів розслідування кіберзлочинів з використанням OSINT. Досліджено методи та засоби використання результатів OSINT для подальшого розслідування та попередження кіберзлочинів.

На основі досліджень, проведених у роботі, запропоновано методи розслідування кіберзлочинів за допомогою відкритих джерел інформації та спеціалізованих OSINT-інструментів. Розроблено рекомендації фахівцям з кібербезпеки щодо реалізації отриманих результатів розслідування кіберзлочинів за допомогою OSINT.

Галузь використання – кібербезпека інформаційних ресурсів організації.

РОЗСЛІДУВАННЯ КІБЕРЗЛОЧИНІВ, OSINT, КІБЕРБЕЗПЕКА, ВІДКРИТІ ДЖЕРЕЛА ІНФОРМАЦІЇ, АНАЛІТИКА.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

OSINT – Open Source Intelligence

IP - Internet Protocol

API - Application Programming Interface

URL - Uniform Resource Locator

WEBINT - Web Intelligence

EXIF - Exchangeable image file format

BGP - Border Gateway Protocol

ВСТУП

*Актуальність дослідження.*Цифрові технології докорінно змінюють парадигму та методологію слідчої діяльності, зумовлюючи підвищення ефективності та розумну швидкість цього процесу. У сучасному світі, де зростає рівень небезпеки як у реальному, так і у віртуальному світі, актуальність інноваційних рішень та цифрових технологій у сфері оперативно-розшукової діяльності набуває особливого значення. Сучасні цифрові технології розширюють можливості оперативних служб у сфері обробки та аналізу великих обсягів інформації, відкриваючи нові перспективи в розкритті злочинів. Інноваційні методи, доступні правоохоронним органам, дозволяють ефективно відстежувати комунікації, аналізувати данні, досліджувати соціальні мережі та застосовувати аналітику для отримання інформації. Ці інструменти допомагають правоохоронним органам підвищити ефективність і розширити можливості в проведенні операцій і розслідуванні сучасних злочинних явищ.

Об'єкт дослідження – процеси розслідування кіберзлочинів

Предмет дослідження – розслідування кіберзлочинів за допомогою OSINT

Мета роботи – методи та засоби розслідування кіберзлочинів за допомогою OSINT

Наукові завдання:

Дослідження проблеми кіберзлочинності у сучасному цифровому світі;

Аналіз підходів правоохоронних органів;

Аналіз існуючих методів OSINT;

Методи розслідування кіберзлочинів;

Використання аналізу зображень у розслідуваннях;

Правові підстави використання методів OSINT;

Інструменти технології OSINT;

OSINT Framework;

Практичні рекомендації при розслідуванні кіберінциндента за допомогою методів OSINT;

Практичний приклад пошуку по фото;

Практичне значення одержаних результатів: розроблено рекомендації щодо розслідування кіберзлочинів за допомогою OSINT, а також розроблено рекомендації фахівцям з кримінального аналізу щодо їх реалізації.

1 ДОСЛІДЖЕННЯ ПРОБЛЕМИ РОЗСЛІДУВАННЯ КІБЕРЗЛОЧИНІВ ЗА ДОПОМОГОЮ OSINT

1.1 Дослідження проблеми кіберзлочинності у сучасному цифровому світі

Сьогодні технологія OSINT має широке застосування в різних галузях. У кібербезпеці вона допомагає виявляти загрози та вразливості шляхом моніторингу Інтернету для виявлення інформації про потенційні атаки, шкідливі програми та інші кіберзагрози. Компанії використовують OSINT для конкурентного аналізу, що дозволяє збирати інформацію про конкурентів, включаючи дані про їхні продукти, маркетингові стратегії, цінову політику та клієнтську базу. Це допомагає компаніям зрозуміти ринок, ідентифікувати свої конкурентні переваги та розробити ефективні стратегії. Крім того, вони можуть здійснювати моніторинг репутації, відстежуючи громадську думку про свій бренд, продукти та послуги, реагуючи на негативну інформацію і забезпечуючи задоволеність клієнтів. OSINT дозволяє компаніям збирати інформацію про потенційні загрози безпеці, кібернапади, ризики та вразливості. Вони можуть відстежувати активність хакерських груп, зловживання співробітниками, інформацію про вразливості програмного забезпечення тощо. Це допомагає вживати відповідних заходів безпеки та знижувати ризики. У сфері розвідки та розслідувань OSINT є незамінним інструментом для збору інформації про осіб, організації чи події. Служби безпеки, поліція та розвідувальні агентства використовують цю технологію для отримання важливих відкритих даних, що допомагають приймати рішення та запобігати злочинам. Загалом, використання OSINT дозволяє отримати цінні дані, які сприяють прийняттю рішень, забезпеченню безпеки та підвищенню ефективності діяльності.

За останні роки інтернет став не лише платформою для обміну інформацією та спілкування, а й місцем для вчинення різних злочинів. Кіберзлочини набули різних форм: від хакерських атак на корпоративні мережі до крадіжок особистої інформації

через соціальні мережі. Зростання кількості цифрових слідів у віртуальному просторі відбувається разом із розвитком технологій, що ускладнює завдання правоохоронних органів у виявленні та розслідуванні злочинів. Наприклад, хакери стають дедалі вправнішими в обході захисних механізмів, що призводить до зростання частоти та складності кібератак. Крім того, з'являються нові види кіберзлочинів, такі як кібершпигунство та фішинг, які можуть завдати серйозної шкоди як окремим особам, так і організаціям. Однією з причин зростання кіберзлочинності є глобалізація технологій. Завдяки інтернету злочинці можуть діяти з будь-якої точки світу, використовуючи анонімність та швидкість цифрового зв'язку для своїх цілей. Також важливо враховувати збільшення кількості інтернет-користувачів, що створює більше можливостей для вчинення злочинів в онлайн-середовищі.

1.2 Аналіз підходів правоохоронних органів

Правоохоронні органи постійно оновлюють свої методи, використовуючи сучасні технології та інноваційні підходи для ефективного проведення розслідувань. Наприклад, вони застосовують програми для аналізу цифрових слідів, моніторингу соціальних мереж і розпізнавання зображень для ідентифікації злочинців і запобігання кібернападам. Щоб ефективно діяти в сучасних умовах, правоохоронним органам потрібно вивчати та впроваджувати новітні методики і цифрові технології в оперативно-розшукову діяльність. Лише об'єднання зусиль та застосування передових засобів дозволяє ефективно боротися з кіберзлочинністю та забезпечувати безпеку інтернет-користувачів. Кіберзлочинність ускладнюється через швидкі та непередбачувані зміни в технологіях. Злочинці постійно вдосконалюють свої методи, пристосовуючись до нових захисних заходів, що ускладнює їх виявлення та запобігання їхнім діям. Використовуючи шифрування та анонімні мережі, кіберзлочинці можуть приховувати свої сліди та уникати виявлення. Крім того, незахищені пристрої та мережі стають легкими мішенями для нападників. Зростання

кількості та складності кібератак вимагає від правоохоронців не лише реагувати на конкретні інциденти, але й активно працювати на попередження майбутніх загроз, використовуючи сучасні інструменти та методики. Співпраця з іншими державами та міжнародними організаціями є критично важливою для боротьби з кіберзлочинністю, оскільки ця проблема не знає кордонів. Лише спільними зусиллями можна ефективно протистояти цій загрозі[6]. Сучасні методи та інструменти OSINT дозволяють виявити практично будь-яку інформацію, яка належно не захищена, що створює додаткові ризики для організацій. Важливо контролювати інформацію, яка публікується співробітниками в соціальних мережах, розкривається на інтерв'ю або випадково потрапляє в Інтернет.

Етичні хакери та пентестери можуть використовувати інструменти OSINT для виявлення вразливостей організацій і вдосконалення їхнього захисту до того, як ці вразливості будуть використані зловмисниками. Збір та аналіз інформації з відкритих джерел має здійснюватися відповідно до правових норм держави, забезпечуючи конституційні права у сфері пошуку, збору, передачі та використання інформації. Законодавство багатьох країн підтримує впровадження систем розвідки з відкритих джерел. Наприклад, у 1996 році в США був прийнятий Закон про свободу інформації, який зобов'язує федеральні агентства надавати громадянам доступ до своєї інформації, за винятком матеріалів, пов'язаних з національною безпекою, фінансовими та особистими документами, а також документації правоохоронних органів[8]. Проте в деяких країнах законодавство може обмежувати таку діяльність, фактично забороняючи розвідку з відкритих джерел.В Україні “кожен має право вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово або в інший спосіб – на свій вибір” (Конституція України, Розділ 2, ст. 34). В Україні правове регулювання в інформаційній сфері ґрунтується на наступних принципах:

1) Свобода законно шукати, отримувати, передавати, виробляти та поширювати інформацію;

2) встановлювати обмеження на доступ до інформації лише законами держави;

3) відкритість інформації про діяльність державних органів та органів місцевого самоврядування та вільний доступ до такої інформації, крім випадків, передбачених законодавством держави;

4) За категорією доступу інформація поділяється на відкриту (загальнодоступну) та з обмеженим доступом. Разом з тим, узаконеного поняття "OSINT" в Україні сьогодні не існує, хоча діяльність зі збирання, зберігання, обробки та розповсюдження інформації регулюється цілою низкою законодавчих і нормативних актів:

• Закон України "Про інформацію" від 02.10.92 р. № 2657-XII (зі змінами від 13.01.11 р.), ст. 5–7 [4];

• Закон України "Про друковані засоби масової інформації (пресу) в Україні" від 16.11.92 р. № 2782-XII, ст. 6, 25[12] ;

• Закон України "Про охоронну діяльність" від 22.03.12 р. № 4616-VI, ст. 9, 13, 19 [13];

• Закон України "Про захист персональних даних" № 2297-VI від 01.06.10 р. [14];;

• Цивільний кодекс України (ст. 505), Кримінальний кодекс України (ст. 231, 232), Кодекс України про адміністративні правопорушення (ст. 163, ст. 163); Варто зазначити, що реалізація заходів у частині забезпечення безпеки підприємництва навіть в рамках розвідки з відкритих джерел інформації в окремих випадках сприймається як проведення оперативно-розшукової діяльності, здійснювати яку, згідно із Законом України "Про оперативно- розшукову діяльність"№ 2135-XII від 18.02.1992 р. [15] вправі тільки суб'єкти, згадані в окремих статтях означених Законів України. У затвердженій Указом Президента України "Стратегії кібербезпеки України" від 15.03.16 р. No96/2016 декларуються основні завдання силовим органам, а також передбачається "створення системи своєчасного виявлення, протидії та нейтралізації кіберзагроз, в тому числі із залученням волонтерських організацій", все

це, безумовно, відноситься до застосування засобів конкурентної розвідки в цій галузі[7].

Кримінальним кодексом України передбачена кримінальна відповідальність за незаконне збирання та використання відомостей, що становлять комерційну таємницю, а також за їх розголошення. Проте така інформація не стосується розвідки з відкритих джерел. При неоднозначному тлумаченні законодавчих норм будь-які процедури збору, обробки та зберігання інформації про конкурентів можуть стати практично безкарними, тобто легітимними, але водночас важкодоступними для громадян. В українській практиці доступ до багатьох видів інформації, яка вільно доступна в інших демократичних державах, таких як відомості про земельні ділянки, нерухомість, наявність банківських рахунків тощо, фактично закритий. Більшість такої інформації можна отримати лише через консультації з спеціальними експертами.

Сьогодні фундаментальними цінностями людства стають приватність життя особи, разом з правом на захист життя та свободу слова. Інформація про людей, зокрема персональні дані, стає цінним товаром, за який готові платити великі гроші. У руках зловмисників така інформація може стати потужною зброєю. Державні інституції, банківські установи, великі бізнес-корпорації не завжди можуть самостійно забезпечити належний захист баз персональних даних, що зберігаються у них, через що великий потік конфіденційної інформації потрапляє на ринок. Таким чином, персональні дані потрібно надійно захищати. На сьогодні, основними європейськими правовими стандартами в галузі захисту персональних даних є Конвенція Ради Європи “Про захист осіб у зв’язку з автоматичною обробкою персональних даних” від 28 січня 1981 року (ETS№108) та “Пакет захисту даних” Європейського Парламенту та Ради від 27 червня 2016 року[16] , які є обов’язковими для всіх держав-членів Європейського Союзу і які є предметом для наслідування в області законодавства, в тому числі, і нашою країною. Країни Євросоюзу мають приводити своє законодавство у відповідність зазначеним правовим стандартам.

Право на приватність гарантується Конституцією України. Стаття 32 Конституції України говорить: “Ніхто не може зазнавати втручання в його особисте і сімейне життя, крім випадків, передбачених Конституцією України”.

В Конституції України передбачений захист ще деяких аспектів приватності. Так, стаття 30 Конституції України захищає недоторканність житла (територіальна приватність), стаття 31 – таємницю листування, телефонних розмов, телеграфної та іншої кореспонденції (комунікаційна приватність), стаття 32 передбачає заборону збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди (інформаційна приватність), а стаття 28 передбачає заборону піддавати особу без її вільної згоди медичним, науковим чи іншим дослідженням (захищаючи елементи фізичної приватності). Конвенція РЄ про захист осіб у зв’язку з автоматизованою обробкою персональних даних від 28 січня 1981 року (ратифікована Україною 06.07.2010 р.) визначає положення стосовно передачі через національні кордони за допомогою будь-яких засобів персональних даних, що піддаються автоматизованій обробці або зібраних з метою їхньої автоматизованої обробки.

Наведені нижче дані, які зазвичай використовуються для ідентифікації особи, визначені Управлінням США з управління та бюджету як особистий:

- повне ім'я та прізвище;
- ідентифікаційний номер;
- IP-адреса (в деяких випадках);
- номер посвідчення водія;
- номери кредитних карток;
- цифрова ідентифікація (цифровий підпис);
- дата народження;
- місце народження;
- генетична інформація[17].

Українське законодавство передбачає інформаційний характер обробки персональних даних. Перед обробкою персональних даних власник або відповідальна особа (оператор) зобов'язані повідомити компетентний орган з питань захисту прав персональних даних про намір обробляти персональні дані. Далі про власника або керівника (оператора) вносяться в спеціальний реєстр операторів. Інформація, що міститься в реєстрі операторів, стає загальнодоступною. Закони про захист персональних даних поширюються на більшість населення як учасників процесу обробки даних. А оскільки кожен є суб'єктом персональних даних, закон є загальним і поширюється на всіх. Персональні дані часто використовуються в соціальних мережах і, зокрема, в службах електронної пошти.

Сучасна інтернет-компанія збирає та обробляє різні категорії персональних даних - своїх співробітників, своїх підрядників і деякі дані користувачів її послуг. Люди, які розміщують інформацію про себе в соціальних мережах або сервісах знайомств, свідомо роблять її доступною всім користувачам ресурсу і за законом можуть бути інтерпретовані як «публічні», тобто для цього не потрібна особлива конфіденційність, але в соціальних мережах є також інформація, яку користувач приховує і робить її доступною лише для певної групи користувачів («друзів»). У цьому випадку інтернет-ресурс повинен запропонувати спеціальні заходи захисту.

Органи, які здійснюють розвідувальну інформацію з відкритих джерел, обробляють персональні дані, які є загальнодоступними, тобто загальнодоступними, в мережі Інтернет. Для обробки згоди суб'єкта даних персональні дані не потрібні.

Довести, що оброблені персональні дані є загальнодоступними, є обов'язком власника або адміністратора. Це означає, що ви повинні або надати докази того, що дані були взяті з загальнодоступних джерел, або отримати згоду суб'єкта даних, а потім зберегти цей документ. Крім того, необхідно мати документ, що підтверджує публічну доступність джерел персональних даних. При цьому без відповіді залишається питання про підтвердження власником інформаційного ресурсу (веб-сайту) письмової згоди на обробку.

1.3 Аналіз існуючих методів OSINT

Одним із інноваційних методів оперативно-розшукової діяльності є використання відкритих джерел для отримання інформації про протиправну діяльність.OSINT— це процес збору, аналізу та використання інформації, яка є загальнодоступною через різні відкриті джерела.Ця інформація може включати дані з веб-сайтів, соціальних мереж, джерел новин, форумів, блогів, онлайн-видань та інших джерел.OSINT виконує різні види аналізу, розвідки, та іншої розвідувальної діяльності для розуміння конкретних ситуацій, виявлення загроз і використання інформації для різних цілей, у тому числі для забезпечення безпеки та дослідження.OSINT відіграє вирішальну роль у розвідці, кібербезпеці, правоохоронних органах та інших галузях, де інформація є стратегічно важливою.OSINT є дуже корисним інструментом для правоохоронних операцій та слідчої діяльності. Основними напрямами використання OSINT в оперативно-розшуковій діяльності є:

1.Збір відкритої інформації про підозрюваних – правоохоронці можуть використовувати OSINT для збору інформації про осіб, щодо яких вони проводять розшук або розслідування. Ця інформація може включати в себе адреси, номери телефонів, профілі у соціальних мережах та інші дані, які допоможуть встановити місцезнаходження або спільнокримінальні зв’язки.

2. Моніторинг соціальних мереж, оскільки підозрювані часто залишають сліди своєї діяльності у соціальних мережах. За допомогою OSINT правоохоронці можуть відстежувати активності підозрюваних, спостерігати за змінами в статусі та взаємодії з іншими користувачами.

3. Аналіз геоданих через інформацію з мобільних додатків і сервісів, таких як картографічні додатки та фотографії з геотегами, що може надати важливі дані про місцезнаходження підозрюваних або потенційних свідків подій.

4. **Моніторинг новин та інших джерел** – онлайн-новини, блоги та форуми можуть надати важливі вказівки, що стосуються подій або осіб, що фігурують у справах. Вони можуть слугувати джерелом нової інформації або підтвердженням існуючих даних.

5. Виявлення відомостей про транспорт – через визначення власників транспорту, перевірку страхових полісів, водійських посвідчень та інших транспортних документів.

6. Аналіз зображень і відео – для виявлення доказів та інформації про злочини чи підозрюваних

У більшості випадків це дуже корисно для надання контексту розвідувальним даним, наданим з інших режимів, але це ще не все, у багатьох сценаріях він міг надавати розвідувальні дані, які можна безпосередньо використовувати для прийняття стратегічного рішення. На думку багатьох, якщо не більшості, це один із найпростіших і найлегших режимів, однак у нього є свої труднощі; одним із найбільших і унікальних з усіх є велика кількість даних. Там, де іншим формам розвідки не вистачає даних, OSINT має стільки даних, що найскладнішою частиною є їх фільтрація та перетворення в придатну для дії форму. OSINT вже давно використовується урядом, військовими, а також корпоративним світом, щоб стежити за конкуренцією та мати конкурентну перевагу над ними. Для OSINT існують різні публічні джерела, з яких можливо збирати розвідувальні дані, але вкваліфікаційній роботі розглядаються ті, що використовує лише Інтернет як засіб масової інформації. Цей специфічний тип OSINT часто називають WEBINT. Може виглядати так, що, зосереджуючись на конкретному типі, втрачаємо величезну частину OSINT, що було б правильним кілька десятиліть тому, але сьогодні, коли більшість даних оцифровано, ця різниця повільно зменшується. Тому для розуміння будемо використовувати терміни WEBINT і OSINT як синоніми. Технологія OSINT) здобуває все більшу популярність і використовується в різних галузях для збору, узагальнення та аналізу інформації з відкритих джерел. Її потужний потенціал виявляється у здатності

надавати доступ до значної кількості даних, що можуть бути корисними для різних цілей, включаючи аналіз трендів, конкурентного середовища, репутації компаній, кібербезпеки та багато іншого.За даними досліджень, обсяг інформації, доступної через відкриті джерела, постійно зростає. Від соціальних мереж і блогів до новинних сайтів та форумів - Інтернет просто переповнений даними, які можуть бути використані для отримання цінної інформації. Саме тому все більше організацій і фахівців використовують технологію OSINT для підтримки своїх потреб у зборі та аналізі даних .. Незважаючи на всі переваги, використання технології OSINT також супроводжується деякими викликами і обмеженнями. Одним з них є потреба управляти великим обсягом даних та використовувати ефективні інструменти для їх аналізу. Також важливо враховувати етичні аспекти та дотримуватися правових рамок під час збору та використання інформації з відкритих джерел. Загалом, технологія OSINT є потужним інструментом, що відкриває безліч можливостей для збору, узагальнення та аналізу інформації з різних соціальних мереж та відкритих джерел. Вона знайшла своє застосування в різних галузях і продовжує розвиватися, стаючи невід'ємною частиною сучасного інформаційного простору.

2 АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ РОЗСЛІДУВАННЯ КІБЕРЗЛОЧИНІВ

2.1 Методи розслідування кіберзлочинів

Протокол Берклі – це практичний посібник з ефективного використання цифрової інформації з відкритим вихідним кодом при розслідуванні порушень міжнародного кримінального права, права людини та гуманітарного права, розроблений школою права Університету Каліфорнії в Берклі разом з представниками ООН. Над цим практичним посібником працювало понад 150 експертів протягом трьох років.

Протокол Берклі містить керівні положення про міжнародні стандарти для проведення онлайн-розслідування передбачуваних порушень, керівництво про методи та процедури для збирання, аналізу та зберігання цифрової інформації з дотриманням професійних, правових та етичних принципів[10].

У ньому також викладено заходи, які слідчі можуть вжити в інтернеті, щоб забезпечити фізичний та психосоціальний захист самих себе та інших людей, включаючи свідків, постраждалих та фахівців з надання першої допомоги, включаючи громадян, активістів та журналістів, які ризикують своїм благополуччям задля того, щоб задокументувати порушення прав людини та серйозні порушення міжнародного права. Використання зібраних доказів із зазначених вище джерел, означає забезпечення справедливого судочинства.

Цей протокол може бути корисним та практичним у роботі адвокатів, журналістів та правоохоронних органів.Варто зазначити, що автори протоколу врахували сучасні тенденції та не посилаються на конкретні інструменти, оскільки технології розвиваються стрімкіше ніж наукові методи, які їх підкріплюють.Даний посібник затверджує мінімальні стандарти необхідні для знаходження, збирання, зберігання, перевірки та аналізу контенту із соціальних мереж та відкритих

джерел.Такими джерелами можуть бути, контент створений користувачами у соціальних мережах, таких як YouTube, Facebook, Instagram та інших.Іншими джерелами можуть бути дані супутникових знімків, які зможуть бути використанні в рамках різних справ у Міжнародному кримінальному суді.З точки зору роботи правоохоронних органів, такі джерела можуть слугувати додатковою доказовою базою та надаватимуть слідчим ширше уявлення про осіб або події.З іншого боку, таким особам варто досить уважно перевіряти інформацію з відкритих джерел, оскільки вона може бути неправдивою, неточною або хибною, тому важливо їх так само ретельно перевіряти, як і інші докази.Негативною стороною на мою думку є те, що правоохоронні органи витрачатимуть більше часу на досудове розслідування, а суди відповідно, на судовий розгляд, оскільки потенційно можуть існувати сотні тисяч фотографій, відео та публікацій, які мають бути перевірені та дослідженні всіма сторонами процесу.Варто зазначити, що наприклад в України діє Національний стандарт України «Інформаційні технології. Методи захисту. Настанови для ідентифікації, збирання, здобуття та збереження цифрових доказів», який стосується не лише цифрових доказів у відкритих джерелах, а й цифрових даних на конкретних пристроях.Однак, ;інститут електронних доказів в КПК України не деталізований та не врегульований на достатньому рівні, саме тому питання внесення відповідних змін до КПК України є нагальним, в тому числі щодо чіткого визначення поняття та видів електронних доказів, а також доповнення переліку процесуальних джерел доказів, і розмежування поняття електронного документа як офіційного документа та інших документів, які подаються в електронній формі.Підсумовуючи, в реаліях сучасного світу рамки правдивості або неправдивості інформації стерлися настільки, що в будь-якому випадку збір та використання інформації з відкритих джерел, є вигідним для всіх сторін, оскільки допоможе підвищити стандарти розслідування та судового розгляду.

2.2 Інструменти технології OSINT

Пошук інформації у відкритих джерелах за логіном є однією з ключових можливостей OSINT.Дуже зручно проводити такі пошуки за допомогою OSINT-фреймворку.Серед ресурсів і можливостей OSINT-фреймворку для пошуку інформації за іменем користувача з відкритих джерел я зупинився на наступному:

Ресурс Namechk – це інструмент, який дозволяє перевіряти доступність конкретного імені користувача або назви на різноманітних популярних платформах, соціальних мережах, ресурсах тощо. Ресурс проводить одноразовий пошук на декількох ресурсах одночасно, з’ясовуючи, чи доступне обране ім’я користувача на кожному з них. Namechk охоплює багато різних веб-сайтів і сервісів, включаючи соціальні мережі, форуми, блог платформи і багато інших майданчиків для взаємодії в Інтернеті. Є можливість налаштувати пошук, щоб врахувати спеціальні символи або певний формат імені користувача.

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

ThatsThem – це онлайн-ресурс і пошуковий інструмент, який надає можливість шукати інформацію про осіб за допомогою їхнього імені, адреси електронної пошти, номера телефону або адреси. Цей ресурс в основному спеціалізується на пошуку контактних даних та публічної інформації про осіб у Сполучених Штатах Америки. Основні функції та можливості ThatsThem включають: пошук за іменем, що дозволяє отримати інформацію про адресу, номер телефону,

можливих родичів та інші контактні дані особи; пошук за адресою електронної пошти; пошук за номером телефону.

Check Usernames – це онлайн-інструмент, який призначений для перевірки доступності користувацьких імен або нікнеймів на різних популярних платформах і соціальних мережах. Основні функції та можливості Check Usernames включають: пошук доступності імен користувачів, робота зі списоком платформ, які підтримуються для перевірки імен користувачів (Twitter, Instagram, Facebook, GitHub, Reddit, YouTube, і багато інших)

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

Google Dorking "Dork" - це техніка, яка використовується для пошуку вразливостей на веб-сайтах за допомогою спеціалізованих пошукових запитів у пошукових системах, зокрема Google. Ці запити складаються таким чином, що дозволяють виявляти інформацію, яка зазвичай не є доступною через звичайний пошук або навіть прихована від більшості користувачів Інтернету

Shodan – це пошукова система, яка дозволяє користувачам шукати різні типи серверів (веб-камери, маршрутизатори, сервери тощо), підключених до Інтернету, використовуючи різні фільтри. Деякі також описують її як пошукову систему банерів сервісів, які представляють собою метадані, що сервер відправляє назад клієнту. Це може бути інформація про програмне забезпечення сервера, про те, які опції підтримує сервіс, вітальне повідомлення або будь-що інше, що клієнт може дізнатися перед взаємодією з сервером.

Sherlock - це скрипт на Python, який допомагає знайти профілі в соціальних мережах за ім'ям користувача.За допомогою скрипта можна знайти користувача і зібрати всі його профілі в один документ та перевірити, чи вільне ім'я для реєстрації нового акаунта.Скрипт перевіряє сайти, які додані в список Sherlock. Зараз у ньому

понад 300 ресурсів, серед яких VK, Twitter, Tinder, TikTok, Steam, Slack, Instagram, Facebook та інші популярні сервіси. Можна також додати у список свої сайти.

Seon. В сучасній цифровій економіці перевірка особистості людини за допомогою різних облікових записів у соціальних мережах та онлайн-платформах стає все більш поширеним явищем. SEON знаходиться в авангарді цього руху за цифрову ідентифікацію.Використовуючи системи електронної пошти та номерів телефонів, ваша компанія може отримати доступ до понад 50 різних соціальних сигналів, які дозволяють отримати вичерпну оцінку ризиків. Ці сигнали не лише підтверджують достовірність адреси електронної пошти або номера телефону клієнта, але й дозволяють отримати більш докладну інформацію про їх цифрове присутність.Крім того, SEON надає компаніям можливість гнучко виконувати запити вручну, через API або навіть через розширення Google Chrome, що робить його більш простим у використанні та доступним.

Recon-ng - це потужний інструмент, що використовується для пошуку інформації, пов'язаної з доменами веб-сайтів. Спочатку це був скрипт, але тепер він перетворився на повноцінний фреймворк.При використанні Recon-ng користувачі можуть виявляти веб-вразливості, включаючи пошук за GeoIP, DNS і сканування портів. Це дуже корисно для пошуку конфіденційних файлів, таких як robots.txt, пошуку прихованих піддоменів, вразливостей SQL-ін'єкцій та отримання інформації про CMS компанії або WHOIS.Незважаючи на те, що він є більш технічним за своєю природою порівняно з іншими інструментами, доступними на ринку, існує безліч корисних ресурсів, які ви можете використовувати, щоб навчитися повністю використовувати переваги цього першокласного програмного забезпечення.

theHarvester – інструмент для пошуку та збирання адрес електронної пошти, пошуку піддоменів, пошуку даних про співробітників компанії. Простий та безкоштовний інструмент OSINT на Python. Він був розроблений для збору інформації з різних джерел, таких як пошукові системи, бази даних Shodan, Hunter, Baidu і т.д. Може знаходити інформацію про домени, піддомени, IP-адреси, облікові

записи електронної пошти, імена співробітників та багато іншого. Дозволяє використовувати модулі з API, такі як bingapi, gitHub та інші.

Metagoofil – утиліта, яка дозволяє завантажити всі документи з цільового сайту та витягти з них метадані. Це безкоштовний збирач метаданих, написаний на Python. Його використовують з метою вилучення інформації з документів: pdf, doc, XLS, ppt, ODP та ods, які знаходяться на цільовій веб-сторінці або будь-якому іншому загальнодоступному сайті. Інструмент використовує Google для пошуку документів, після чого завантажує їх, витягує та аналізує метадані. Він може знайти конфіденційну інформацію, таку як імена користувачів, електронні листи і т.д. Він також може показати шлях до файлів, які можуть розкрити особисті дані, мережеві імена, загальні ресурси і багато іншого.

DarkOwl Vision – пошук інформації у даркнеті Платформа дозволяє проводити моніторинг та аналітику загроз у просторі Dark web для ефективного пошуку скомпрометованих конфіденційних даних. Програма DarkOwl Vision в автоматичному режимі безперервно та анонімно займається збором, індексацією та ранжуванням важливих даних розвідки даркнету. Інтерфейс користувача зручний для роботи, пошукова система підтримує логічні вирази і фільтри.

Розширені можливості пошуку Google:

Таблиця 2.1.

site:	Обмежує результати результатами з певного домену
“ ”	Лапки вказують на пошук точного вислову
AND	Показує результати лише для обох умов
OR	Пошук терміну А, Б чи обох. Символ труби – те саме, що й АБО

*****	Підстановковий знак для слів у фразі, яку ви не знаєте
( )	Групує набір слів/операторів окремо
-	Виключає результати, що містить це слово
$	Пошук за певною ціною
cache:	Остання кешована версія домену, наприклад cache:boston.gov
filetype:	Пошук лише за певним типом файлу
related:	Пошук сайтів, пов'язаних з доменом
intitle:	Пошук сторінок із умовою в заголовку сторінки
inurl:	Виводить сторінки, що містять вказане слово в UR
around(x)	Сторінки, що містять два слова або фрази на відстані X слів один від одного
info:	Знайти інформацію про конкретну сторінку, включаючи час останнього кешування

Розширений пошук Bing:

Таблиця 2.2

( )	Групує набір слів/операторів окремо
OR	Всі запити Bing розглядаються як I якщо ви не вкажете умови або між ними g
NOT	Виключає результати з певним терміном
loc:	Пошук сторінок з певного регіону

prefer:	Надає пріоритет умові пошуку або іншому оператору
near:x	Пошук слів на відстані X одне від іншого
ip	Знаходить сайти, розміщені на IP адресі
site/domain:	Фільтр для конкретного типа домену
feed:	Знаходить RSS-канали на основі пошукових запитів

Робота з соціальними мережами

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

Такі соціальні мережі, як LinkedIn, Instagram, Facebook і X, є важливими джерелами для проведення OSINT-розвідки.

Instagram - це популярна соціальна мережа, яка дозволяє користувачам ділитися фотографіями, відео, історіями та спілкуватися з людьми з усього світу. Платформа надає можливість створювати особисті профілі, вести прямі трансляції, використовувати різноманітні фільтри та редагувати контент, а також взаємодіяти з іншими користувачами через лайки, коментарі та приватні повідомлення.

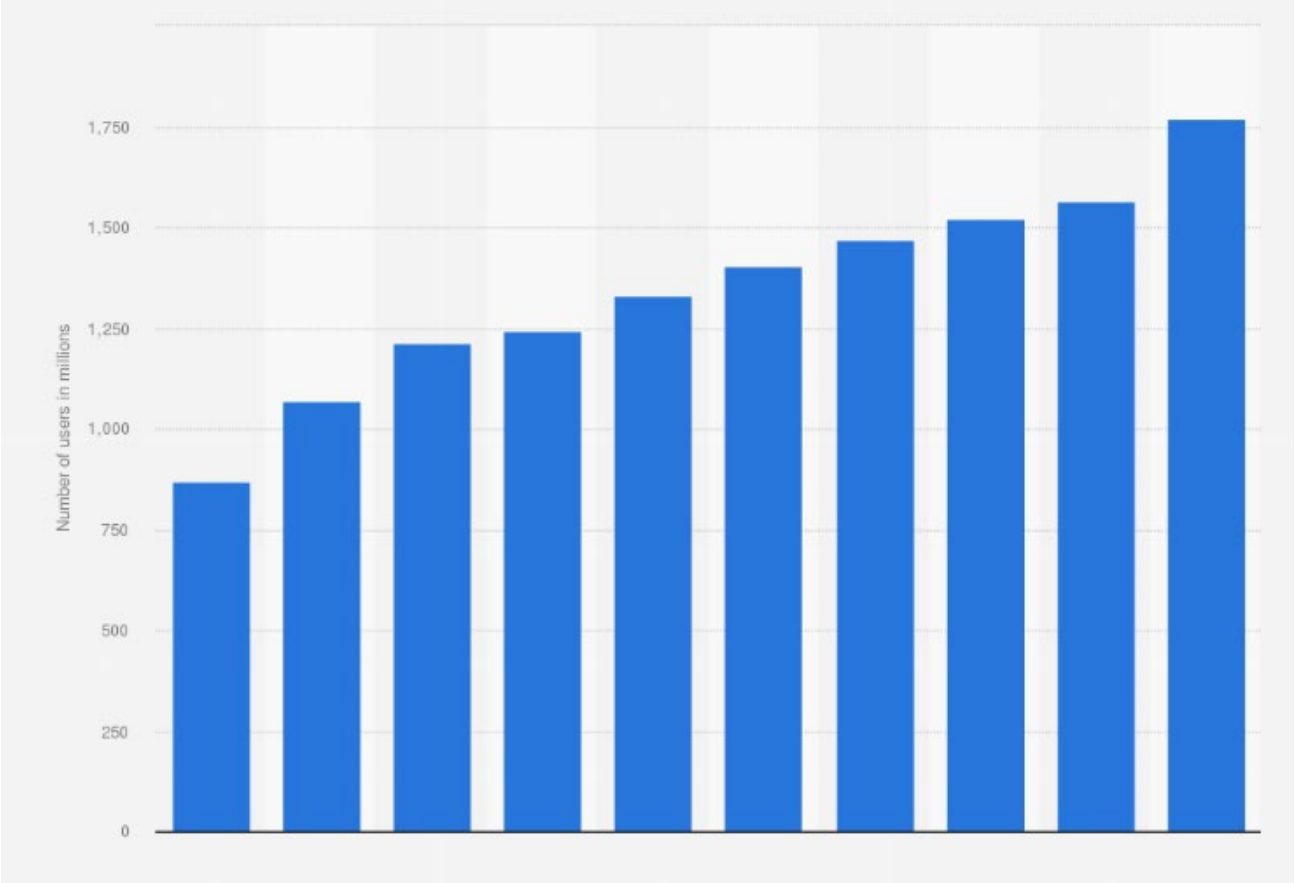

Рис.21 стистика користувачів intagram з 2019 по 2024

Instagram може бути корисним в OSINT розвідці з кількох причин:

1)Особиста інформація: користувачі Instagram часто розміщують у своїх профілях особисту інформацію, таку як місце проживання, інтереси, діяльність та подорожі. Ця інформація може бути використана для отримання деталей про конкретну особу, її зв'язки, інтереси та стиль життя.

2)Фотографії та відео: Instagram фокусується на візуальному контенті, тому користувачі активно завантажують фотографії та відео, які можуть містити цінну інформацію. Це може включати зображення людей, місць, подій та інших важливих аспектів, які можуть бути використані для аналізу.

3)Історії та прямі трансляції: Користувачі Instagram часто діляться подіями зі свого життя в реальному часі через історії та прямі трансляції. Це може надати актуальну інформацію про місцезнаходження та діяльність певних осіб.

5)Групи та хештеги: На Instagram існують тисячі хештегів, які об'єднують людей за спільними інтересами, темами або подіями. Досліджуючи популярні хештеги, можна отримати інформацію про активності, думки та дії групи людей, що може бути корисною в розвідці.

6)Взаємодія та комунікація: Instagram надає засоби для взаємодії з іншими користувачами через коментарі, відмітки, приватні повідомлення тощо. Це може допомогти встановити зв'язки з особами, виявити залежності та отримати додаткову інформацію про конкретну особу чи групу людей.

7)Аналіз громадської думки: Instagram є місцем, де люди вільно висловлюють свої думки та обговорюють різні питання через публікації та коментарі. Аналіз громадської думки на певну тему може допомогти отримати інсайти, оцінити настрої, тенденції або реакції людей на певні події.

8)Відстеження інформаційних потоків: Instagram може бути зручним інструментом для відстеження та моніторингу новин, трендів або подій у реальному часі.Використовуючи хештеги та підписки на певні профілі, можна отримати доступ до широкого спектру інформації та оновлень з різних джерел та перевіряти їх автентичність.

2.3 Огляд OSINT Framework

OSINT Framework пропонує значні можливості для роботи з IP адресами: визначення приблизної геолокації IP-адреси, аналіз IP-адреси на предмет загроз або інцидентів, таких як історія атак чи злочинних дій; пошук пов’язаних доменів та служб, а також інші служби, які можуть використовуватися на цій IP-адресі; моніторинг активності та статус IP-адреси в мережі; зв’язок із суміжними інформаційними джерелами, тобто OSINT Framework може надати посилання на інші додаткові ресурси, такі як блоги, форуми або соціальні мережі; аналіз історії IP-адреси для інформації щодо її реєстрації та власника.

Blacklists у контексті OSINT Framework вказують на списки IP-адрес, доменів, а також URL-адрес, які розглядаються як небажані або потенційно небезпечні. Ці списки містять інформацію про об’єкти, що можуть бути пов’язані зі спамом, шахрайством, кіберзлочинністю або іншими видами шкідливої діяльності в Інтернеті. OSINT Framework має вбудовані інструменти та ресурси для роботи з цими чорними списками та регулярно оновлює їх, щоб користувачі мали доступ до актуальної інформації, надаєкористувачам посилання на інші інструменти та ресурси, які дозволяють докладніше досліджувати IP-адреси або домени, виявлені в чорних списках, створює умови для автоматизації перевірки IP-адрес та доменів на предмет наявності в чорних списках. Чорні списки OSINT Framework дозволяють оперативно виявляти й ідентифікувати потенційно небезпечні об’єкти та сприяють підвищенню рівня безпеки в Інтернеті.

Border Gateway Protocol, в контексті OSINT Framework, вказує на інструменти та ресурси, які дозволяють збирати та аналізувати інформацію про маршрутизацію мережі та активність систем, які використовують протокол BGP. Серед можливостей BGP в рамках OSINT Framework виділю: пошук інформації про конкретне Autonomous System, включаючи інформацію про власників, географічне розташування та інші характеристики; моніторинг маршрутів BGP, що може бути корисним для виявлення аномалій чи атак на мережу; аналіз AS-відносин для визначення потенційних точок відмови чи атак на мережу; визначення геолокації AS та вивчення, де саме відбувається маршрутизація мережевих пакетів; пошук інформації про BGP-підприємства та інтернет-постачальників, що може бути корисним для аналізу мережевих інфраструктур; пошук потенційних точок відмови тощо.

Images в OSINT Framework вказують на можливості та ресурси, які допомагають аналізувати та збирати інформацію зображень, включаючи фотографії, знімки відео та інший мультимедійні вміст. OSINT Framework дозволяє проаналізувати метадані, які вбудовані в зображення (EXIF-дані), такі як географічні

координати, дату та час створення, модель камери та інші параметри. Є можливість здійснювати реверсний пошук зображень, що дозволяє визначити джерело, де це зображення було раніше опубліковане в Інтернеті. Засоби Images дозволяють визначити місце на зображенні (геолокацію), об'єкти та їхні характеристики. Засоби пошуку схожихзображень допомагають виявити дублікати або подібні матеріали зображень в соціальних мережах та інших онлайн-ресурсах. Перевірка на аутентичність зображень полегшує виявлення ознак фотошопу або монтажу.

Videos в OSINT Framework вказують на можливості та ресурси, які допомагають аналізувати та збирати інформацію з відеозаписів та мультимедійних матеріалів, включаючи відеоматеріали, опубліковані в Інтернеті. OSINT Framework дозволяє аналізувати метадані відеозаписів, такі як дата та час створення, власник відео, географічні координати, модель камери, а також інші параметри. Є засоби для проведення реверсного пошукувідео для визначення джерела, де відеозапис був раніше опублікований в Інтернеті.

Засоби Videos в OSINT Framework надають можливість визначити місце та об'єкти, які зображені на відео, включаючи геолокацію та розпізнавання облич, виявлення звідки було отримано або опубліковано відео,можливість аналізу аудіо-слідів відео для ідентифікації розмов, музики, а також інших звукових даних, визначення слідів фотошопу або монтажу, пошук відеозаписів, які схожі на вказане відео, що може бути корисно для виявлення дублікатів або аналізу подібних матеріалів.

Images та Videos в OSINT Framework є сучасними та зручними засобами для проведення оперативно-розшукової діяльності через аналіз змісту фото та відеоматеріалів.У своїй сукупності засоби OSINT Framework, такі як Malicious File Analysis, Digital Currency, Mobile Emulation, Metadata, Geolocation Tools / Maps, Transportation, Business and Public Records, Telephone Numbers, Social Networks, Images / Videos / Docs, IP Address та інші, є корисним інструментом у сфері оперативно-розшукової діяльності для збору відкритої інформації з використанням різноманітних

джерел та ресурсів. Ці інноваційні засоби дозволяють збирати інформацію про осіб, включаючи їхні імена, контактну інформацію, адреси, соціальні мережі, родину та інші персональні дані; відстежувати активність осіб на соціальних мережах, аналізувати їхні публікації, фотографії та зв'язки; визначати місцезнаходження осіб чи об'єктів; аналізувати IP-адреси, визначати їхні власників, геолокацію та зв'язок з іншими даними; проводити аналіз відео та фотографій для виявлення об'єктів, подій чи здійснення реверсного пошуку для встановлення походження зображень; шукати інформацію на веб-сайтах, форумах, блогах та інших ресурсах; досліджувати аудіо-файли для ідентифікації голосів, розмов та іншої аудіо-інформації; проводити моніторинг і аналіз відкритих джерел на можливі загрози чи аномалії, пов'язані з певними особами або подіями.

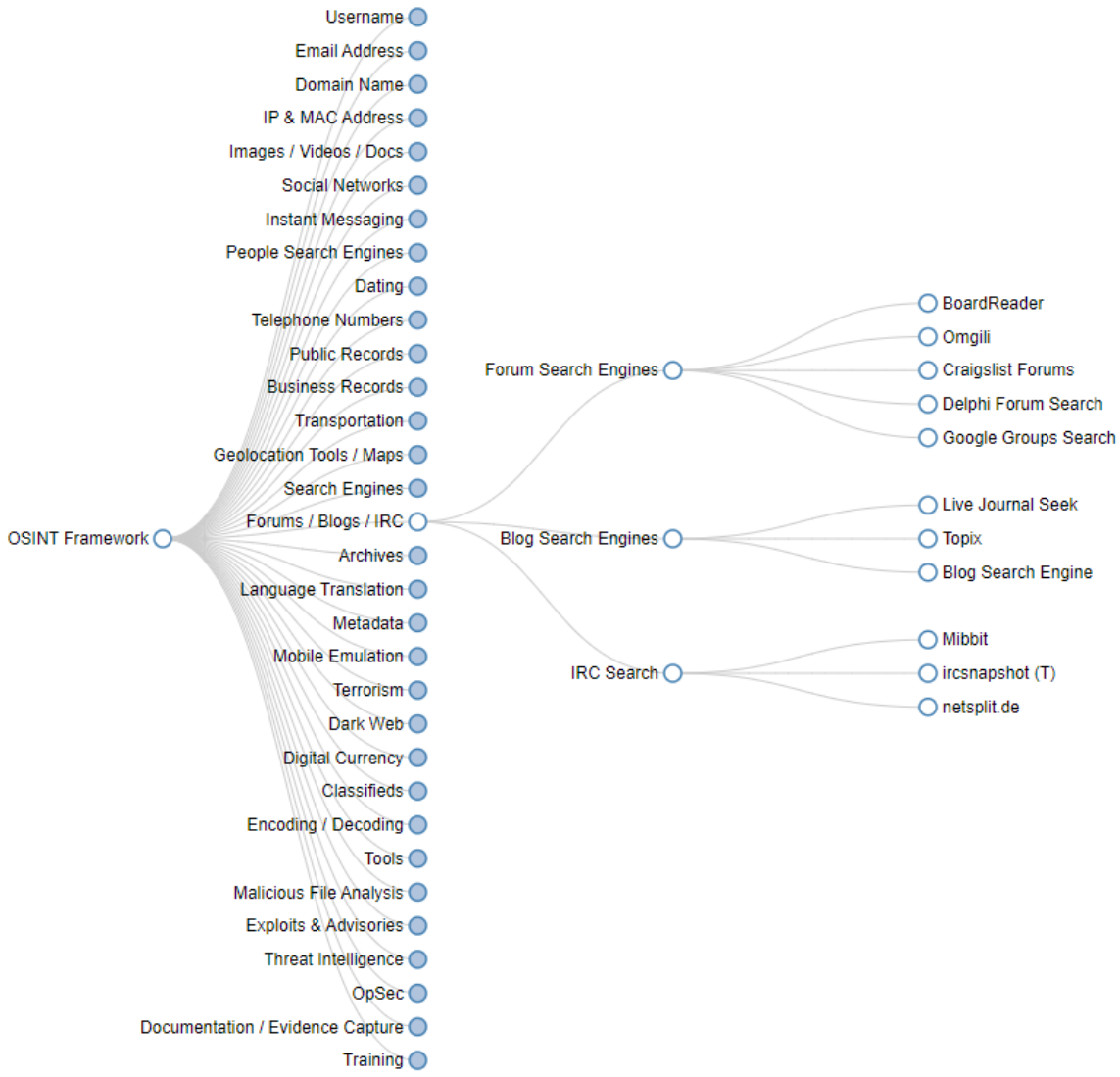

Рис.2.2 вигляд OSINT Framework [11]

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

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

Оновлення та розширення: OSINT Framework постійно оновлюється з новими інструментами та ресурсами, що відповідають змінюючимся потребам OSINT

розвідки. Це дозволяє користувачам отримувати доступ до найновіших інструментів та методик.

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

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

OSINT Framework став популярним серед дослідників безпеки, кіберрозвідки, приватних детективів та інших спеціалістів, які займаються збором інформації з відкритих джерел. Його універсальність та зручність робить його цінним інструментом для виконання OSINT розвідки. За допомогою цього фреймворку на прикладі пошуку по соціальним мережам можливо вибрати усі потрібні інструменти, які допоможуть провести ретельним пошук заданої теми.

2.4 Використання аналізу зображень у розслідуваннях

Аналіз зображень є важливою складовою розслідувань у сфері кібербезпеки та OSINT. Від зображень можна отримати багато інформації, яка може допомогти у виявленні місця, часу і обставин їх створення.

Першим кроком у пошуку додаткової інформації про зображення є перевірка даних EXIF. Дані EXIF вбудовані в зображення під час його створення і часто містять цікаву інформацію, таку як дата створення, використана камера, іноді GPS-дані тощо. Для перевірки цих даних можна використовувати наступні інструменти:

ExifTool: Командний рядок, який дозволяє зчитувати та редагувати дані EXIF.

Exif Viewer: Розширення для браузерів Chrome та Firefox, яке зручно для швидкого перегляду даних EXIF.

Photo Forensic: Вебсайт, який має багато цікавих функцій для аналізу зображень.

Exif.regex.info: Альтернативний ресурс для перегляду даних EXIF.

Foto Forensics: Інший корисний інструмент для аналізу зображень.

Для пошуку схожих зображень існують кілька потужних інструментів:

Google Images: Найбільш відомий пошуковик зображень.

Bing Images: Має корисну функцію, яка дозволяє шукати конкретну частину зображення.

TinyEye: Інструмент, який має корисний API для автоматизації пошуку.

Для покращення результатів пошуку схожих зображень може бути корисним видалення фону. Для цього можна скористатися інструментом remove.bg, який дозволяє швидко та якісно видаляти фон зображення.

Аналіз вмісту зображення для визначення його місцезнаходження та інших деталей вимагає уважного вивчення специфічних предметів на зображенні. Це дозволяє зробити припущення про місце зйомки, а потім провести онлайн-дослідження та порівняти результати з супутниковими знімками. Рекомендовано ознайомитися з якісними розслідуваннями від Bellingcat, які демонструють методи такого аналізу.

3 РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ЗАСТОСУВАННЯ МЕТОДІВ ТА ЗАСОБІВ РОЗСЛІДУВАННЯ КІБЕРЗЛОЧИНІВ ЗА ДОПОМОГОЮ OSINT

3.1. Практичні рекомендації при розслідуванні кіберінциндента за допомогою методів OSINT

Створення плану є дуже важливим під час проведення OSINT-розвідки, оскільки вам потрібно чітко розуміти свій план дій, щоб знайти всю корисну інформацію.План проведення OSINT у соціальних мережах може включати такі кроки:

-Поставлення цілі. Потрібно чітко пояснити мету розвідки. Це може включати збір інформації про конкретних осіб, компанії чи організації або виявлення певної діяльності чи зв’язків.

-Вибір соціальної мережі. Вирішіть, які соціальні мережі дослідити. Наприклад, Facebook, Twitter, Instagram, LinkedIn, YouTube тощо.

-Збір публічної інформації. Переглядайте профіль особи чи організації та переглядайте їхні публічні повідомлення, фотографії та взаємодію з іншими користувачами.Зверніть увагу на деталі профілю, такі як місцезнаходження, освіта, інтереси та зв’язки.Записуйте всю корисну інформацію.

-Дослідження з’єднання. Аналізуйте зв'язки між об'єктами інтелекту та іншими користувачами.Знайдіть список друзів, підписників, підписок і спільних груп.Це дає уявлення про соціальні мережі людини, її вплив і зв’язки з іншими людьми.

-Дослідження діяльності. Вивчається активність об'єктів розвідки в соціальних мережах. Подивіться уважніше на його пости, коментарі, лайки та реакції на пости інших користувачів. Це може виявити думки, погляди, інтереси або потенційно небезпечну діяльність .

- Використання інструментів і пошуку. Знаходьте детальну інформацію про об’єкти розвідки за допомогою спеціальних інструментів розвідки OSINT, таких як Maltego, Social-Searcher і Echosec, або виконуючи розширений пошук за допомогою певних ключових слів або пошукових запитів.

-Аналіз інформації. Зібравши інформацію, проведіть аналіз і зробіть висновки. З’єднайте точки, розпізнайте закономірності та визначте можливі ризики та перспективи.

-Запишіть свої результати та створіть звіт.

Це загальний план, який можна використовувати для запуску інформації OSINT у соціальних мережах але кожен випадок може мати свої унікальні характеристики та вимоги, тому плани можуть змінюватися залежно від ваших обставин та інформаційних потреб.

3.2. Практичний приклад пошуку по фото

Сучасні смартфони та численні цифрові камери вбудовують GPS-координати в кожну фотографію. Таким чином, знімки, зроблені цими пристроями, містять дані про місцезнаходження, вбудовані за замовчуванням. Під час обміну конфіденційними фотографіями в Інтернеті цю інформацію можна приховати. GPS-координати зберігаються як метадані, вбудовані в самі файли фотографій, і для їх перегляду достатньо відкрити властивості файлу. Проте розслідування, засновані лише на інтуїції, не є надійними методами в будь-якій програмі підготовки фахівців із розслідування. Висновки дослідника повинні підтверджуватися об’єктивними доказами, а також бути відтворюваними для забезпечення надійності результатів.

Тим не менш, будь-який досвідчений дослідник значною мірою покладається на інтуїцію, навіть якщо цього не усвідомлює. Причина цьому проста: інтуїція є набагато раціональнішим процесом, ніж здається. За одну секунду мозок здійснює десятки

несвідомих обчислень, заснованих на попередньому досвіді, що дозволяє дійти до швидкого рішення.

Задумом цього методу є пошук з широкого аналізу і поступового уточнювання параметрів пошуку для локалізації і зрештою визначення точного місцезнаходження, використовується підхід, що передбачає розрізнення "глобальних" і "місцевих" індикаторів. Замість використання термінів "великий" і "маленький", застосовується поняття "глобальний" та "місцевий". "Глобальні" підказки – це елементи на зображенні, які можуть вказати на регіон світу, де воно зроблене. "Місцеві" підказки допомагають знайти точне розташування після того, як глобальні підказки визначать приблизний регіон. Цей метод був використаний на Рис.3.1 .

Рис. 3.1. Фотографія з поверху будівлі

На Рис.3.2, елементи в зелених прямокутниках класифіковані як глобальні індикатори – якщо їх можна ідентифікувати, а потім зібрати разом, вони приблизно покажуть, у якому це місті. Елементи у червоних прямокутниках є місцевими індикаторами: вони не є характерними для країни та міста, але разом із глобальними індикаторами допоможуть знайти конкретне місце.

Рис. 3.2. Використання методу “Глобальне – Місцеве”

Короткий виклад індикаторів по яким був проведений OSINT

Глобальні індикатори:

1) одноповерховий автобус із червоно-білим розфарбуванням. Зокрема, це червона смужка на задній нижній частині та білий у решті частини;

2) група будівель, що виділяється – набагато вище, ніж оточуючі. Одна, жовтого кольору;

3) зелений знак автомагістралі, що виглядає так, ніби він вказує на виїзд. Здається на ній одна цифра номера дороги;

Місцеві індикатори:

1) знак автомагістралі. Демонструє нам, що місце буде поряд із дорогою, можливо, поряд із з’їздом;

2) дивна схожа на намет дах, що веде до мосту, що йде через автомагістраль;

3) стіл та стільці. Це, мабуть, найбільш місцевий індикатор, і буде корисним лише для з’ясування остаточного точного розташування;

Таким чином, можна стверджувати, що це місце розташоване в місті з червоно-білими автобусами. Домінуючим елементом міста буде висока жовта будівля, яка буде у зоні видимості місця. Поруч знаходиться автомагістраль, ймовірно, з однозначним номером. Біля локації буде розташована незвична конструкція, схожа на намет, яка веде до мосту через автомагістраль. Всередині будівлі розміщено кафе або ресторан з меблями, що відповідають вигляду на зображенні. Ймовірно, це місто знаходиться у Східній Європі, хоча поки що немає об'єктивних доказів для підтвердження цього припущення.

Було прийнято рішення зосередитися на Східній Європі, тому відправившись до Google Images та пошуку “країна” + “червоно-білий автобус” виділявся ряд країн. Спершу була розглянута Польща. Там було кілька червоно-білих автобусів, але вони були старі і не відповідали зображенню на картинці. Потім увагу привернула Словаччина. Хоча збігів було небагато, одна фотографія виглядала багатообіцяючою – переважно білий автобус із червоним ззаду на Рис. 3.3 буде відображен результат. Далі Чехія. Незважаючи на те, що там також було небагато автобусів, схожих на той, що на картинці, одна фотографія виділялася. Після її перегляду з'явилося багато схожих зображень, на яких було видно, що трамваї та автобуси в Празі також мають червоно-біле забарвлення, подібне до зображеного на картинці. Результат перегляду буде на Рис. 3.4.

Рис. 3.3. Автобус Словенії

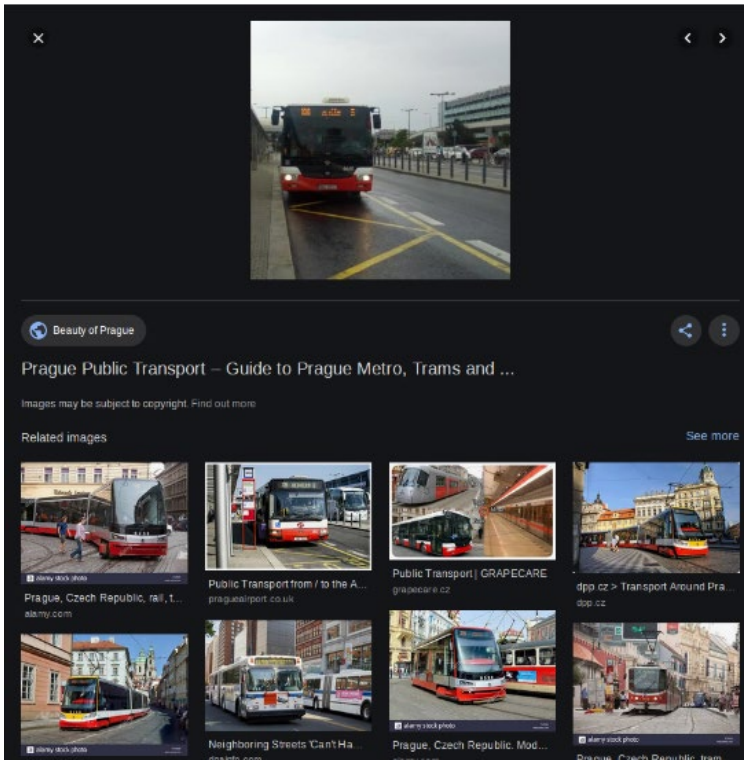

Рис. 3.4. Громадський транспорт Чехії

Знак автомагістралі був використаний для виключення Брно з можливих варіантів. Знак показував однозначний номер автомагістралі, тоді як у Брно є лише частина автомагістралі №2 – єдиної з однозначним номером. Через Братиславу теж проходила та сама автомагістраль №2, але поблизу не було знайдено нічого схожого на потрібне місце. Якщо подивитися на Google Карти міста Прага, то можна побачити, що вона оточена шосе 0, 1, 2, 4, 6 і 7, і всі вони могли бути тією самою автомагістраллю.

Одним із глобальних індикаторів є висока жовта будівля. Як і в випадку з автобусами, була використана формула “Глобальний індикатор” + “Місто” .

Таким чином було знайдено схожу будівлю – готель Opatov в Празі. На Рис. 3.5 і 3.6 буде показана будівля з початкової фотографії та результат запиту у Google картинках відповідно.

Рис. 3.5. Будівля з початкової фотографії

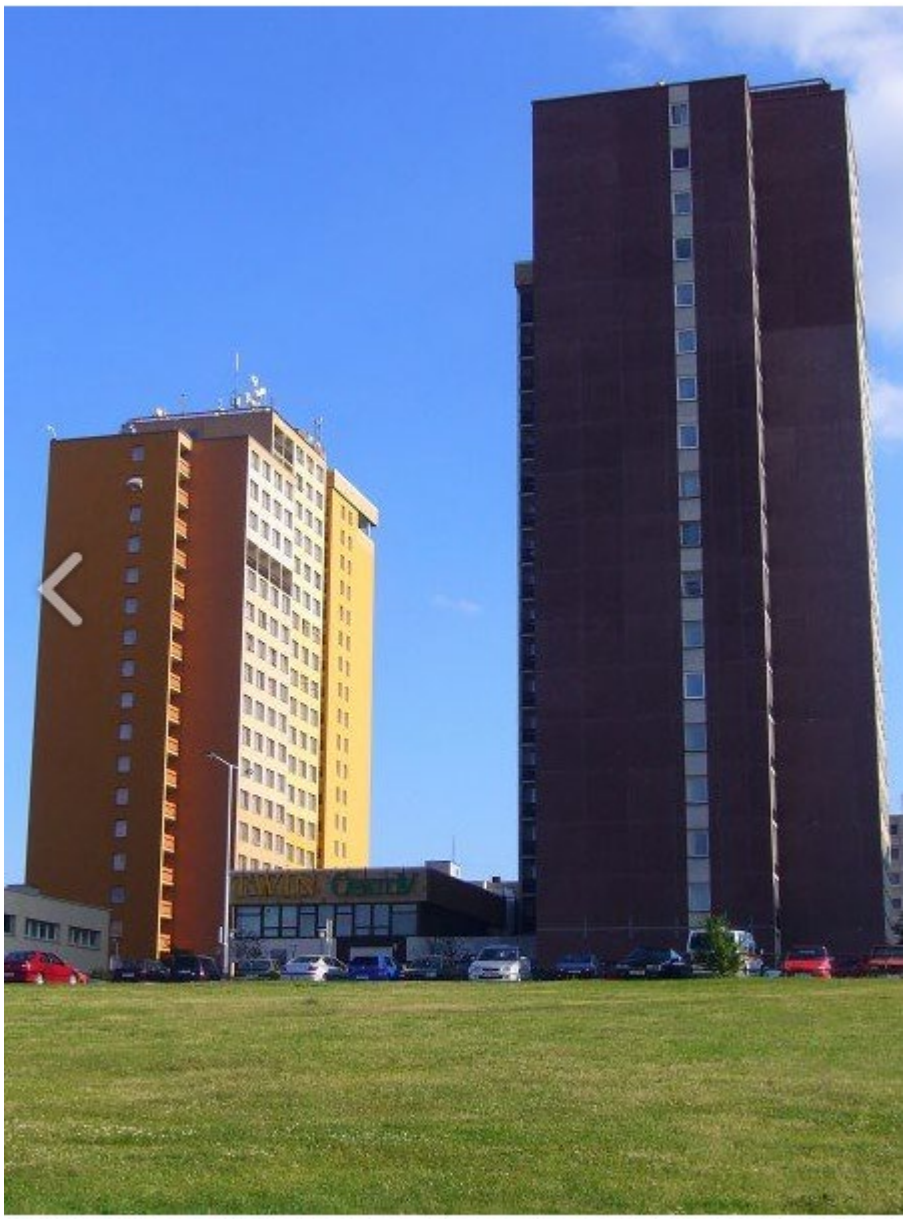

Рис. 3.6. Результат запиту у картинках Google

Якщо звернутись до Google Карт, то можна побачити, що поруч знаходиться автомагістраль.

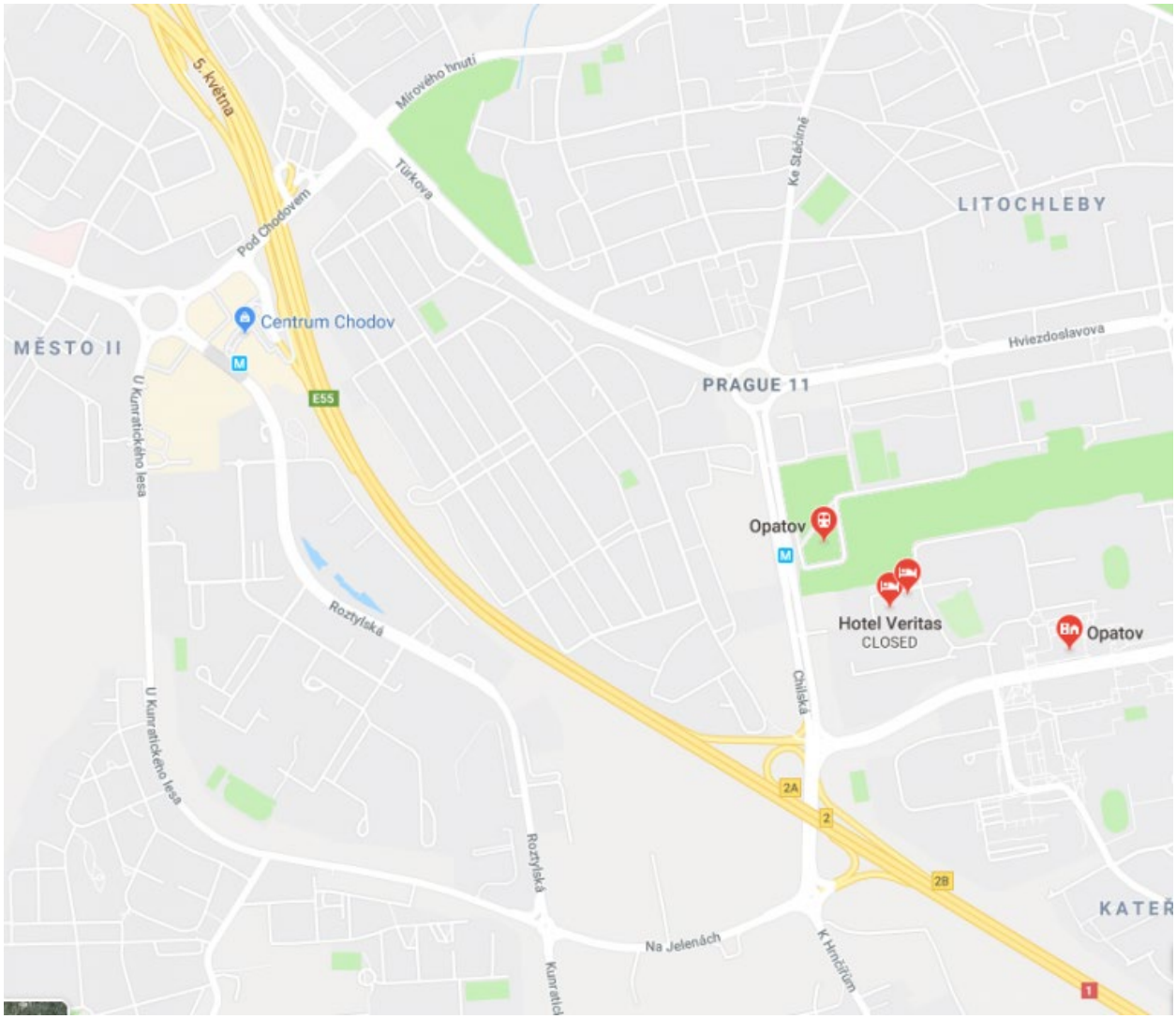

Рис. 3.7. Готель Opatov на Google Maps

Для того щоб знайти точне розташування, потрібно використати місцеві індикатори. Поряд з мостом через автомагістраль був дивний намет. «Намет» – це дах для автовокзалу. З більш детальною інформацією про місцеві індикатори допоможе сервіс Google Street view, щоб знайти фотографію автобусів і побачити, як вони насправді виглядають великим планом.

На Рис. 3.8 буде показана місцевість на 3D карті, а на Рис. 3.9 - припарковані в тому самому місці та у тій же кольоровій гамі автобуси, що й на оригінальному фото.

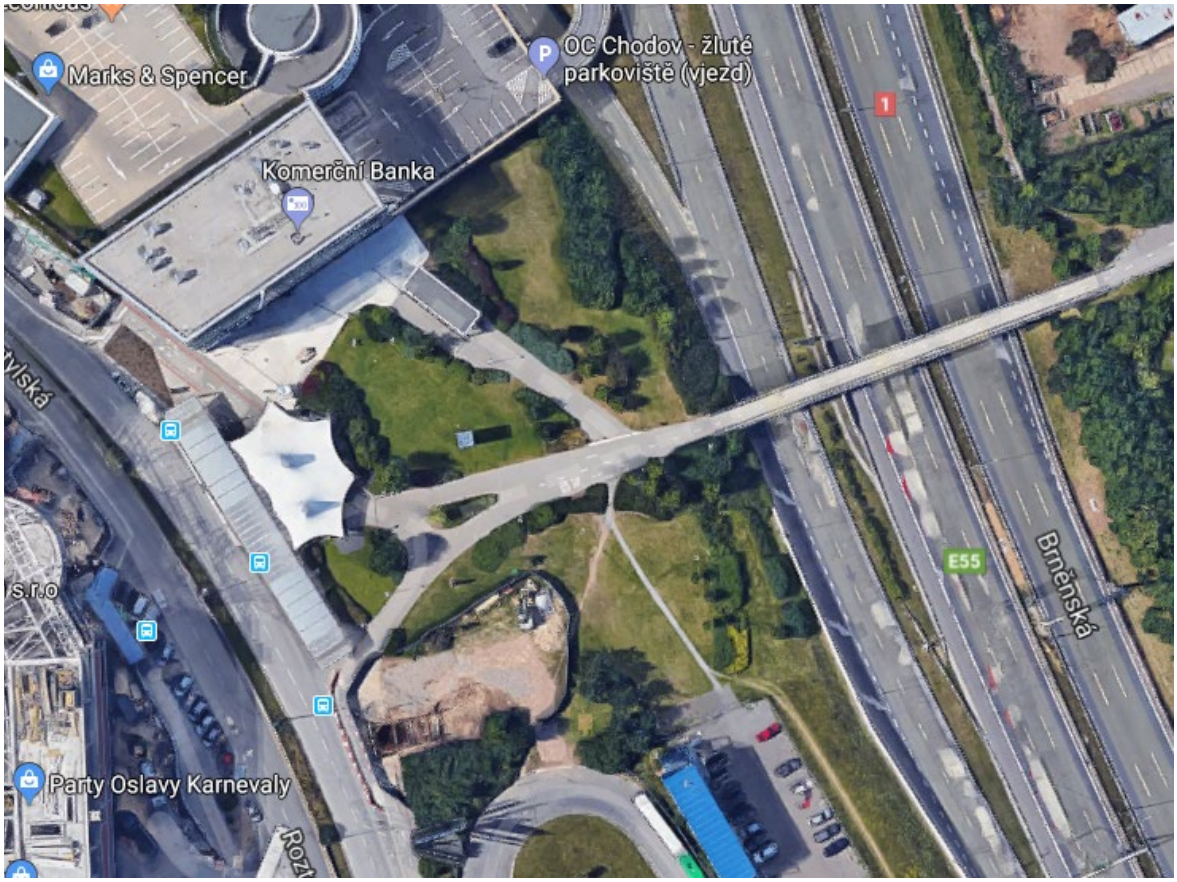

Рис. 3.8. Зображення місцевості на 3D карті.

Рис. 3.9. Фото автовокзалу

Використовуючи Street view, проходячи далі по автомагістралі можна побачити знак який інформує про з’їзд з автомагістралі №2 (Рис. 3.10.)

Рис. 3.10. Знак з’їзду з автомагістралі №2.

Тепер потрібно зрозуміти з якої будівлі був зроблен оригінальний знімок.

Єдиною багатоповерхневою будівлею був торговий центр Centrum Chodov, зображений на Рис. 3.11.

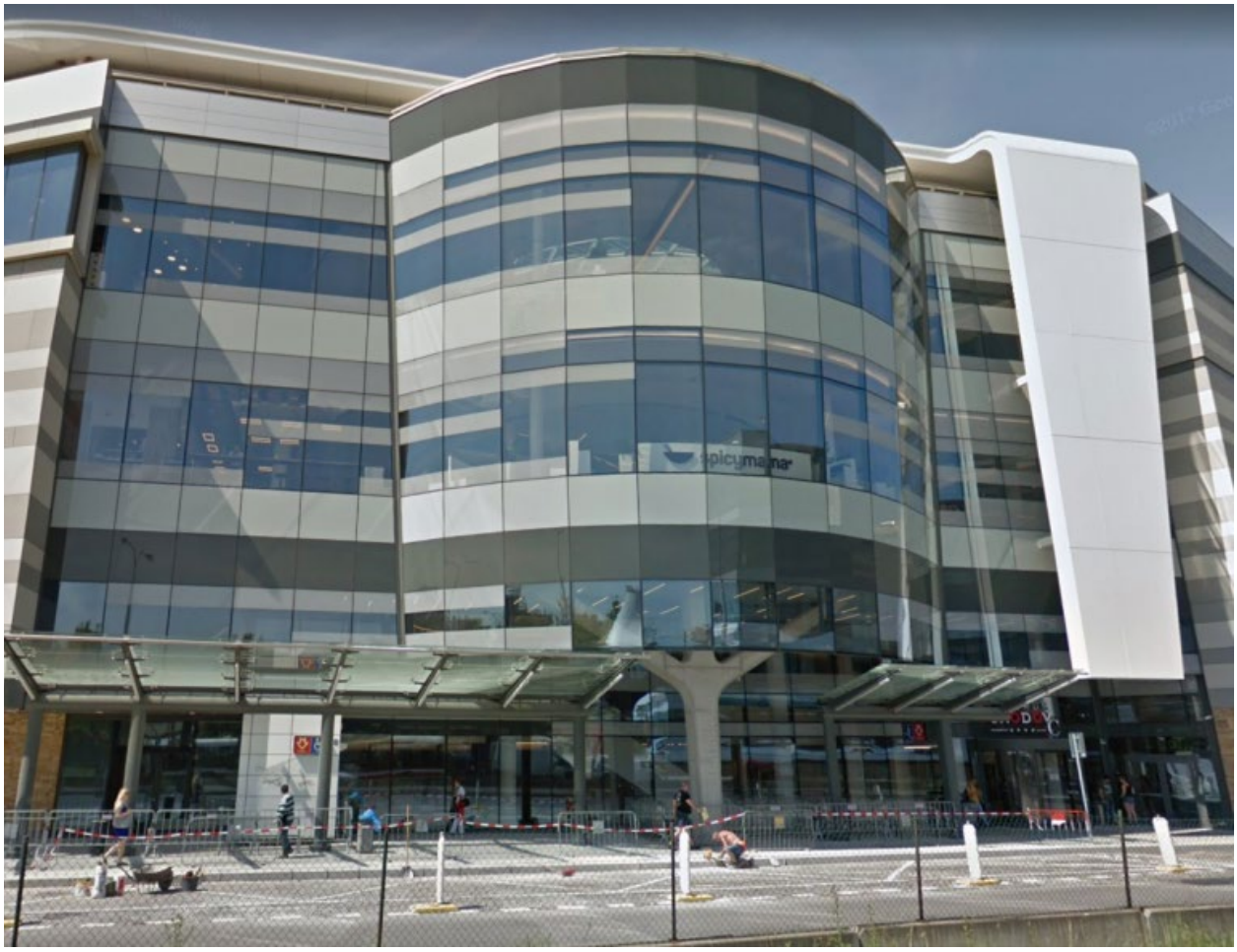

Рис. 3.11. Зображення торгового центру Centrum Chodov

Найкращим способом знайти точне розташування – знайти план будівлі торгового цетру, а потім спробувати знайти фотографії інтер’єру за назвою можливих місць. Дивлячись на план (Рис. 3.12.) , можна припустити що це місце було або Spicymama, або дуже близько до нього. Інтерактивний план поверху показав, що на першому та другому поверхах були лише кафе, тож вибору було замало.

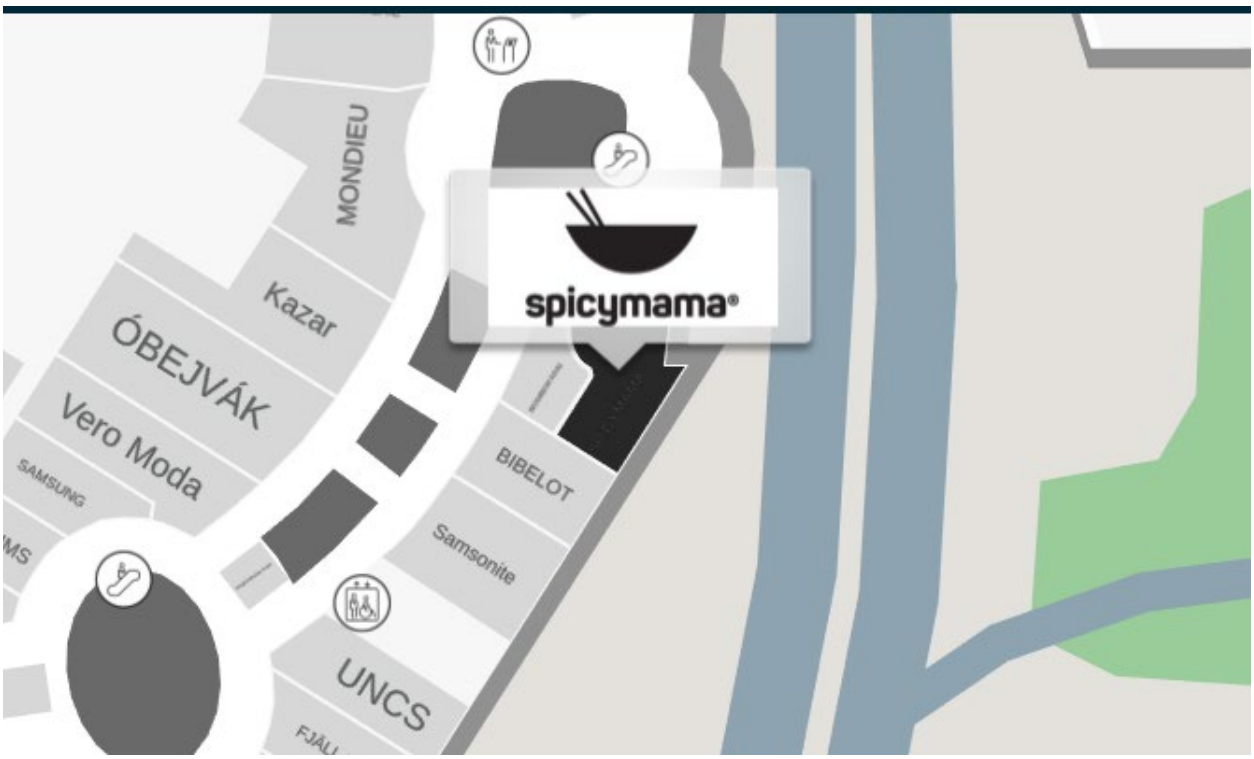

Рис. 3.12. План торгового центру Centrum Chodov

Інтер’єр Spicymama не відповідав початковому зображенню. Після перевірки сусіднього місце, де продавалися продукти – Page Cafe. Швидкий пошук по Facebook фотографій “Page Cafe Centrum Chodov” повернув збіг наведений на Рис. 3.13.

Рис. 3.13. Інтер’єр з оригінальною фотографії

3.3. Розслідування кіберзлочину за допомогою крипто гаманця

При розслідувані кіберзлочину, в якому фігурує крипто гаманець можливо здійснити ідентифікацію особи власника гаманця. Засоби OSINT дозволяють здійснити аналіз інформації по крипто гаманцю. Крім цього, технологія Блокчейн дозволяє всім бажаючим переглянути стан гаманця та транзакції, які відбувалися із його використанням, знаючи лише адресу гаманця. Технології OSINT дозволяють більш комплексно підійти до питання пошуку такої інформації. Данні про власника крипто-гаманця стали не виключенням. Один із інструментів OSINT для здійснення пошуку інформації є Maltego, який був раніше згаданий в роботі, дає змогу здійснювати аналіз крипто-гаманців та встановлювати зв'язки між ними, як це показано на рис. та рис.

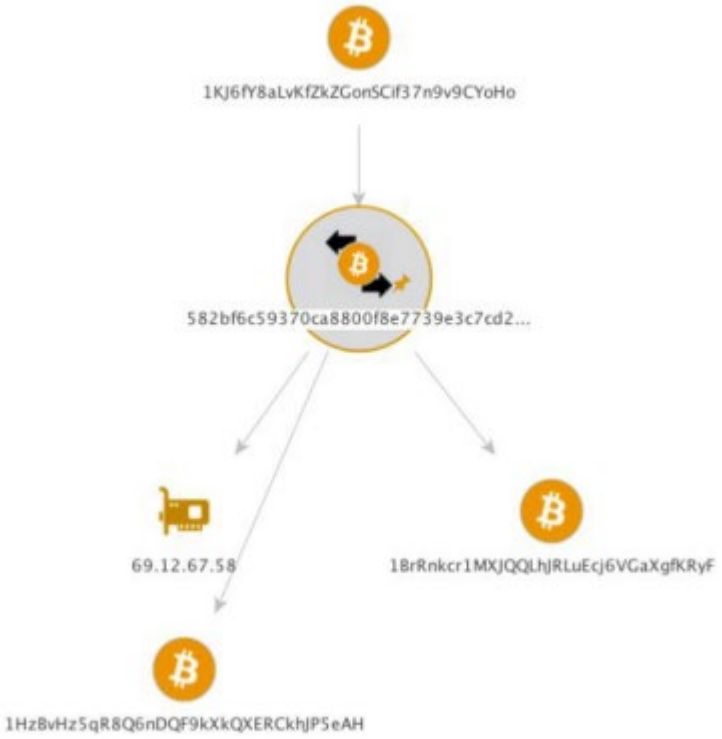

Рис.3.14 Maltego

Крім того, можна спробувати шукати гаманці в пошукових системах, таких як Google, Yandex, Bing і Boardreader.Такі гаманці часто можна зустріти на одному з форумів в Інтернеті. Тому що пошукові системи можуть проіндексувати таку сторінку, навіть якщо це так званий «хакерський форум».Існує також багато веб-ресурсів для пошуку криптовалютних гаманців. Найвідоміші включають "blockchain.com/explorer", "blockchair.com/", "etherchain.org" і "etherscan.io".Технологія OSINT, завдяки своїй універсальності та відсутності структури в пошуку інформації, дозволяє підходити до проблеми з різних сторін і в поєднанні з іншими техніками та методами розслідування надає повну та об’єктивну інформацію про інцидент.

ВИСНОВКИ

У кваліфікаційній роботі Проведено аналіз шляхів та розроблення рекомендацій щодо розслідування кіберзлочинів за допомогою OSINT. Досліджено сучасний стан використання технології OSINT, а також популярні інструменти для збору та аналізу інформації. Показано, що OSINT Framework є незамінним інструментом для проведення розвідки, оскільки забезпечує доступ до широкого спектра ресурсів для збору та аналізу відкритої інформації, включаючи пошук даних, аналіз соціальних мереж, перевірку доменних імен, пошук витоків даних тощо. Виявлено, що Google, як найпопулярніша пошукова система, володіє широкими можливостями для здійснення ефективного пошуку інформації з відкритих джерел, що дозволяє проводити глибокий аналіз даних.

Виявлено, що використання технології OSINT для збору, узагальнення та аналізу інформації з соціальних мереж стало ключовим аспектом сучасної розвідки, оскільки організації стикаються з дедалі складнішими завданнями у цій сфері. Показано, що OSINT Framework забезпечує комплексне рішення для розвідки, дозволяючи збирати та аналізувати дані в режимі реального часу, автоматизувати процеси збору інформації та спрощувати впровадження найкращих практик безпеки.

Встановлено практичні рекомендації, які включають методи пошуку по фото та криптовалютних гаманцях, що є важливими аспектами сучасних розслідувань кіберзлочинів. Пошук по фото дозволяє ідентифікувати особи та відстежувати їх діяльність у різних мережах, що є критично важливим для збору доказів. Аналіз криптовалютних гаманців допомагає виявляти фінансові транзакції, пов’язані з кіберзлочинами, та відстежувати рух коштів.

Таким чином, встановлено, що правильна реалізація технології OSINT має сприяти ефективному збору та аналізу інформації, забезпечуючи безпеку та

конфіденційність даних у цілому. Обґрунтовано, що у майбутньому, неперервний розвиток цієї технології та її поєднання з іншими інноваційними підходами відкриває шлях до нових можливостей і досягнень у багатьох сферах, включаючи безпеку, розвідку, бізнес-аналітику та громадську діяльність. Важливо також дотримуватись етичних стандартів та законодавства під час проведення OSINT розвідки, розробляючи відповідні політики та процедури для захисту прав і приватності осіб.

ПЕРЕЛІК ПОСИЛАНЬ

1.Жарков Я.М. Наукові підходи щодо визначення суті розвідки з відкритих джерел / Я.М. Жарков, А.О. Васильєв // Вісник Київського національного університету імені Тараса Шевченка. Військово-спеціальні науки.- 2013. - Вип. 30. - С. 38-41. - // URL: http://nbuv.gov.ua/UJRN/VKNU_vsn_2013_30_12

2. NATO Open Source Intelligence Reader (2002). // URL: http://informationretrieval.info/docs/NATO-OSINT.html–

3. Розвідка Відкритих Джерел (OPEN SOURCE INTELLIGENCE)Ржевська Н.Ф., Кожушко О.О. // URL: http://ena.lp.edu.ua/bitstream/ntb/19232/1/53-Rzhevska-257-261.pdf

4. Про інформацію: Закон України від 02.10.92 р. № 2657-XII

5. Про захист персональних даних: Закон України від 01.06.10 р. № 2297-VI.

6. Про оперативно-розшукову діяльність: Закон України від 18.02.92 р. № 2135-XII

7. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року “Про Стратегію кібербезпеки України”: Указ Президента України від 15.03.16 р. № 96/2016.

8. Розвідка відкритих джерел інформації (osint) у розвідувальній практиці США Кожушко Ольга Олегівна URL: http://jrnl.nau.edu.ua/index.php/IMV/article/viewFile/3264/321

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

10. Протокол Берклі з ведення розслідувань з використанням відкритих цифрових даних. Практичний посібник. Нью-Йорк і Женева, 2020. 119 с. URL: https://www.law.berkeley.edu/ wp-content/uploads/2022/03/Berkeley-Protocol-Ukrainian.pdf (Дата звернення: 15.08.2023)

11. OSINT Framework. URL: https://osintframework.com

12. Про друковані засоби масової інформації (пресу) в Україні: Закон України від 16.11.92 р. № 2782-XII.

13. Про охоронну діяльність: Закон України від 22.03.12 р. № 4616-VI.

14. Ланде Д.В. Правові питання конкурентної розвідки // URL: http://ippi.org.ua/sites/default/files/7_16.pdf

15. Розробка системи управління кіберінцидентами в мережах LTE // URL: https://jrnl.nau.edu.ua/index.php/Infosecurity/article/view/13036/18086

16.Електронна енциклопедія Wikipedia. Українськомовна версія // URL: https://uk.m.wikipedia.org/wiki/Персональні_дані/

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ

(Презентація)