МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Запорізька політехніка»

Факультет інформаційної безпеки та електронних комунікацій
(повне найменування факультету)

Кафедра «Інформаційна безпека та наноелектроніка»
(повне найменування кафедри)

Пояснювальна записка

до дипломного проєкту (роботи)
магістр
(ступінь вищої освіти)

на тему Дослідження методів OSINT при розслідуванні
(назва теми)
кіберінцидентів

Виконала: студентка 6 курсу, групи БКз-813м

Спеціальності 125 Кібербезпека та захист
(код і найменування спеціальності)
інформації

Освітня програма (спеціалізація)
безпека інформаційних і комунікаційних систем
ПІКІВЕЦЬ Г.М.
(ПРІЗВИЩЕ та ініціали)
Керівник КОРОЛЬКОВ Р.Ю.
(ПРІЗВИЩЕ та ініціали)
Рецензент ЛИТВИЦЬКИЙ О. П.
(ПРІЗВИЩЕ та ініціали)

2024

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Запорізька політехніка»

Факультет Інформаційної безпеки та електронних комунікацій
Кафедра Інформаційна безпека та наноелектроніка
Ступінь вищої освіти магістр
Спеціальність 125 Кібербезпека та захист інформації
(код і найменування)
Освітня програма (спеціалізація) Безпека інформаційних і комунікаційних
(назва освітньої програми (спеціалізації)
систем

ЗАТВЕРДЖУЮ
Завідувач кафедри ІБтаН
_____ Андрій КОРОТУН
«_____» _____2024 року

З А В Д А Н Н Я
НА ДИПЛОМНИЙ ПРОЄКТ (РОБОТУ) СТУДЕНТКИ

ПІКІВЕЦЬ Ганни Миколаївни
(ПРІЗВИЩЕ, ім'я, по батькові)

1. Тема проєкту (роботи) Дослідження методів OSINT при розслідуванні кіберінцидентів Research on OSINT methods in cyber incident investigation

керівник проєкту (роботи) к.т.н., доцент, КОРОЛЬКОВ Роман Юрійович
(науковий ступінь, вчене звання, ПРІЗВИЩЕ, ім'я, по батькові)
затверджені наказом закладу вищої освіти від « 05 » грудня 20 24 року №507
2. Строк подання студентом проєкту (роботи)_____
3. Вихідні дані до проєкту (роботи) публічна інформація про OSINT розвідку; персональний комп'ютер; інструменти для проведення OSINT розвідки; науково-технічна література

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити) аналітичний огляд методів OSINT; огляд інструментів та законодавче регулювання; дослідження застосування OSINT у кіберрозслідуваннях; перспектив розвитку OSINT у сфері кібербезпеки; впровадження інструментів та методів забезпечення безпеки OSINT-розслідувань; висновки; список використаних джерел і додатки

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, кількість слайдів, плакатів)
Презентація PowerPoint (20 слайдів)

6. Консультанти розділів проєкту (роботи)

Розділ	ПРІЗВИЩЕ, ініціали та посада консультанта	Підпис, дата	
		завдання видав	прийняв виконане завдання
1-3	КОРОЛЬКОВ Р.Ю. доцент кафедри ІБтаН	04.09.2024	10.12.2024
Нормконтроль	КОРОЛЬКОВ Р.Ю. доцент кафедри ІБтаН		16.12.2024

7. Дата видачі завдання «_04_» _жовтня_ 2024 року.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проєкту (роботи)	Строк виконання етапів проєкту (роботи)	Примітка
1	Ознайомлення з завданням до кваліфікаційної роботи	07.10.2024 – 09.10.2024	Виконано
2	Підбір джерел про використання методів OSINT при розслідуванні кіберінцидентів	11.10.2024 – 18.10.2024	Виконано
3	Опрацювання джерел про використання методів OSINT при розслідуванні кіберінцидентів	19.10.2024 – 21.10.2024	Виконано
4	Оформлення розділу «Теоретичні основи OSINT»	22.10.2024 – 28.10.2024	Виконано
5	Оформлення розділу «Методи OSINT у розслідуванні кіберзлочинів»	29.10.2024 – 11.11.2024	Виконано
6	Оформлення розділу «Ефективне розслідування кіберінцидентів за допомогою методів OSINT: практичні інструменти»	12.11.2024 – 02.12.2024	Виконано
7	Висновки	03.12.2024 – 10.12.2024	Виконано
8	Оформлення кваліфікаційної роботи	11.12.2024 – 15.12.2024	Виконано
9	Нормоконтроль	16.12.2024	Виконано
10	Перевірка на плагіат	23.12.2024	Виконано
11	Захист кваліфікаційної роботи	24.12.2024	

Студентка _____ Ганна ПІКІВЕЦЬ
(підпис) (Ім'я ПРІЗВИЩЕ)

Керівник проєкту (роботи) _____ Роман КОРОЛЬКОВ
(підпис) (Ім'я ПРІЗВИЩЕ)

АНОТАЦІЯ

Пояснювальна записка до дипломного проєкту: 130 с., 39 рис., 2 дод., 59 джерела.

OSINT, КІБЕРІНЦИДЕНТ, РОЗСЛІДУВАННЯ, ІНФОРМАЦІЯ З ВІДКРИТИХ ДЖЕРЕЛ, РОЗВІДКА.

Об’єктом дослідження є процес розслідування кіберінцидентів із використанням методів OSINT.

Предметом дослідження є інструменти та методи OSINT, що використовуються для збору, аналізу інформації при розслідування кіберінцидентів, а також їх впровадження для забезпечення безпечного проведення OSINT-розслідувань.

Метою роботи є аналіз застосування інструментів OSINT у процесі розслідування кіберінцидентів та розробка рекомендацій щодо їх безпечного використання.

Практична цінність результатів дослідження полягає у можливості застосування методів і інструментів OSINT для ефективного розслідування кіберінцидентів та підвищення рівня інформаційної безпеки.

У магістерській роботі було досліджено сучасний стан використання методів OSINT для розслідування кіберзагроз. Розглянуто популярні інструменти, такі як Shodan, Maltego, Recon-ng та інші, практичні аспекти їх застосування для збору та аналізу даних. Особливу увагу приділено правовим аспектам використання OSINT, включаючи обробку персональних даних і дотримання нормативно-правових вимог.

На основі практичних прикладів продемонстровано ефективність інструментів OSINT при розслідуванні кіберінцидентів. Запропоновано підходи до впровадження інструментів безпеки для проведення OSINT-

розслідувань, таких як анонімізація, створення захищеного середовища, використання спеціалізованих веббраузерів, віртуальних приватних мереж (VPN), а також впровадження заходів із захисту та зберігання даних, таких як резервне копіювання і шифрування. Це сприяє забезпеченню конфіденційності розслідувань та мінімізації ризиків витоку даних.

Використання запропонованих рішень забезпечує зменшення ризиків, пов'язаних із обробкою конфіденційної інформації, та підвищення ефективності аналізу відкритих джерел. Результати роботи можуть бути впроваджені у практику при розслідуванні кіберінцидентів організаціями різних масштабів, а також використовуватися для навчання фахівців у галузі інформаційної безпеки.

ABSTRACT

Explanatory note to the diploma project: 130 p, 39 fig., 2 app., 59 references.

OSINT, CYBER INCIDENT, INVESTIGATION, OPEN SOURCE INFORMATION, INTELLIGENCE.

The object of research is the process of investigating cyber incidents using OSINT methods.

The subject of the study is the OSINT tools and methods used to collect and analyse information during the investigation of cyber incidents, as well as their implementation to ensure the safe conduct of OSINT investigations.

The purpose of this paper is to analyse the use of OSINT tools in the process of investigating cyber incidents and to develop recommendations for their safe use.

The practical value of the research results lies in the possibility of using OSINT methods and tools to effectively investigate cyber incidents and improve information security.

The master's thesis investigated the current state of the art of using OSINT methods to investigate cyber threats. Popular tools, such as Shodan, Maltego, Recon-ng and others, the practical aspects of their application for data collection and analysis are considered. Particular attention is paid to the legal aspects of using OSINT, including the processing of personal data and compliance with regulatory requirements.

Based on practical examples, the article demonstrates the effectiveness of OSINT tools in investigating cyber incidents. Approaches to the implementation of security tools for OSINT investigations, such as anonymisation, creation of a secure environment, use of specialised web browsers, virtual private networks (VPNs), and implementation of data protection and storage measures, such as backup and

encryption, are proposed. This helps to ensure the confidentiality of investigations and minimise the risk of data leakage.

The use of the proposed solutions reduces the risks associated with the processing of confidential information and increases the efficiency of open source analysis. The results of the work can be implemented in practice when investigating cyber incidents by organisations of various sizes, and can also be used to train information security professionals.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

ІТ - Інформаційні технології

ПЗ - Програмне забезпечення

ШПЗ - Шкідливе програмне забезпечення

ACOUSTINT (Acoustic Intelligence)- акустична розвідка

API (application programming interface) - прикладний програмний інтерфейс

CMS (Content Management System) - система керування вмістом

COMINT (Communications Intelligence) - комунікаційна розвідка

DNS (Domain Name System) - система доменних імен

ELINT (Electronic Intelligence) - електронна розвідка

FISINT (Foreign Instrumentation Signature INTelligence) - розвідувальні сигнали іноземних приладів

GEOINT (Geospatial Intelligence) - геопросторова розвідка

HUMINT (Human Intelligence) - агентурна розвідка

IMINT (Imagery Intelligence) - видова розвідка

IoT (internet of things) - інтернет речей

IP (Internet Protocol) - інтернет протокол

IRINT (Infrared Intelligence) - інфрачервона розвідка

MASINT (Measurement and Signature Intelligence) - вимірювально-сигнатурна розвідка

NUCINT (Nuclear Intelligence) - ядерна розвідка

OSIF (Open Source InFormation) - інформація з відкритих джерел (у вільно доступних медіаканалах)

OSINT (Open Source Intelligence) - розвідка на основі відкритих джерел

RADINT (Radar Intelligence) - радіолокаційна розвідка

SIGINT (Signals Intelligence) - сигнальна розвідка

SOCMINT (Social media intelligence) - розвідка соціальних мереж

SSL (Secure Sockets Layer) - рівень захищених сокетів

TELINT (Telemetric Intelligence) - телеметрична розвідка

URL (Uniform Resource Locator) - єдиний вказівник на ресурс

VPN (Virtual Private Network) - віртуальна приватна мережа

ВСТУП

Сучасний розвиток інформаційних технологій та глобальна цифровізація всіх аспектів життя сприяли значному зростанню кількості кіберінцидентів, які становлять серйозну загрозу для організацій, урядових структур та окремих користувачів. Захист від кіберзагроз став критично важливим завданням, що вимагає ефективних підходів до виявлення та розслідування інцидентів у кіберпросторі. Одним із таких підходів є використання методів відкритої розвідки (OSINT, Open Source Intelligence), які ґрунтуються на аналізі відкритих джерел інформації.

Методи OSINT дозволяють отримувати та аналізувати інформацію з доступних публічних ресурсів, таких як веб-сайти, соціальні мережі, форуми, бази даних та інші публікації, що можуть містити важливі дані для розслідування кіберінцидентів. Використання таких методів у процесі розслідувань є ефективним підходом для збору необхідної інформації про потенційні загрози, шкідливі дії зловмисників, їхні тактики і методи.

З огляду на зростання складності кіберзлочинів та масштабність проблем, які виникають у цій сфері, важливо досліджувати методи OSINT з метою визначення їх ефективності та практичної значущості у розслідуванні кіберінцидентів. Вивчення доступних інструментів OSINT, а також їх застосування у реальних сценаріях кіберзагроз може суттєво підвищити рівень інформаційної безпеки та забезпечити якісне реагування на загрози.

1 ТЕОРЕТИЧНІ ОСНОВИ OSINT

1.1 Визначення та значення OSINT

OSINT (Open Source Intelligence) - це розвідка з відкритих джерел, яка передбачає збір, аналіз та використання інформації, доступної з публічно відкритих джерел для отримання розвідувальних даних. OSINT включає інформацію, що отримується з інтернету, соціальних мереж, медіа, публічних баз даних, звітів, блогів, форумів, супутникових зображень та інших відкритих джерел [1].

OSINT включає процеси пошуку, реєстрації, обліку й аналізу інформації, її аналітико-синтетичної обробки, зберігання, поширення, захисту та презентації результатів досліджень. Дані з відкритих джерел після їх аналітико-синтетичної обробки можуть перетворитися на цінні знання, які, залежно від свого характеру, можуть набути статусу секретної інформації, якщо вони не належать до категорій, що виключають можливість державної таємниці.

Варто розрізняти OSINT (Open Source INTelligence) та OSIF (Open Source InFormation). OSIF — це дані та відомості, які поширюються у відкритих медіаканалах, тоді як OSINT — це спеціально зібрана й структурована інформація, призначена для відповіді на конкретні питання [2]. Основна відмінність полягає в тому, що завдання агентури полягає у здобутті інформації з джерел, які зазвичай не прагнуть її розкривати, тоді як завдання розвідки з відкритих джерел — це точний аналіз та обробка доступної для всіх інформації.

OSINT знаходить застосування в багатьох галузях, зокрема в розвідці, кібербезпеці, журналістиці та бізнесі. У сфері кібербезпеки OSINT допомагає виявляти кіберзагрози, такі як фішингові атаки, зломи та діяльність, пов’язана з розвідкою.

Розвідка з відкритих джерел складається з загальнодоступної інформації, збирається, аналізується та своєчасно розповсюджується серед відповідної аудиторії та відповідає конкретній розвідувальній потребі [3].

Термін «відкрите джерело» стосується конкретно інформації, яка доступна для загального використання. Якщо для доступу до частини інформації потрібні будь-які спеціальні навички, інструменти чи методи, її не можна обґрунтовано вважати відкритою.

Понад 99% Інтернету неможливо знайти за допомогою звичайних пошукових систем. Ця частина, відома як «глибинна мережа», складається з безлічі веб-сайтів, баз даних, файлів і т.д., які з різних причин (включаючи сторінки для входу або платні системи), не піддаються індексації Google, Bing, Yahoo або будь-якою іншою пошуковою системою [4]. Однак більшу частину контенту глибокої мережі можна вважати відкритим, оскільки він легко доступний для загального використання.

OSINT активно використовується різними сферами для вирішення широкого спектра завдань: правоохоронні органи, спецслужби та армія застосовують OSINT для збору даних про потенційні загрози, терористичну діяльність, злочинців, прогнозування конфліктів і аналізу ризиків у кібербезпеці.

Бізнес-середовище використовує OSINT для моніторингу конкурентів, управління репутацією, аналізу ринкових тенденцій, виявлення загроз та підвищення рівня захисту даних.

Журналісти і медіаорганізації застосовують OSINT для збору, перевірки інформації, проведення розслідувань та пошуку новин.

Соціальні мережі і загальнодоступні платформи аналізуються за допомогою OSINT для виявлення ботів, оцінки громадської думки, створення споживчих профілів, а також для дослідження суспільних трендів і прогнозування.

Кібербезпека використовує OSINT для виявлення загроз, аналізу інтернет-ресурсів з метою виявлення слабких місць у захисті, а також моніторингу активності хакерських угруповань.

Моніторинг глобальних явищ включає вивчення ситуації з правами людини, аналіз діяльності режимів та спостереження за міжнародними конфліктами.

Інструменти OSINT можна використовувати для доступу та аналізу інформації з джерел поза традиційними пошуковими системами. Ці інструменти, такі як Spiderfoot, searchcode, Searx, Twint і Metagoofil, збирають і аналізують значні обсяги даних із відкритих джерел, включаючи мережі соціальних медіа та глибоку мережу, щоб виявляти та зберігати великі обсяги даних, знаходити посилання та закономірності між різними фрагментами інформації та зіставляти виявлену інформацію в дієві дані.

Крім того, в Інтернеті є багато вільнодоступної інформації, яку можна знайти за допомогою онлайн-інструментів, відмінних від традиційних пошукових систем.

1.2 Історія та еволюція OSINT

Важливим завданням є дослідити історію виникнення та становлення OSINTу. Точна дата і передумови створення цієї технології залишаються невідомими, але науковці виділяють декілька етапів. Зокрема:

У 1941 році в США була створена Служба моніторингу закордонних трансляцій (Foreign Broadcast Monitoring Service, FBMS), яка займалася аналізом радіопрограм для збору й оцінки інформації з новин країн Осі (нацистська Німеччина, фашистська Італія, Японська імперія) та їх союзників. У роботі служби використовувалися матеріали з газет, журналів та радіопередач [5].

Обробляючи значні обсяги хаотичних даних, аналітики виявляли окремі факти, як-от інформацію про наслідки бомбардувань на основі змін цін на продукти, аналізували пропаганду, щоб зрозуміти реакцію населення на прихід військ, або оцінювали економічне становище країн-супротивників. Ці дані служили як для перевірки інших джерел, так і як самостійні джерела інформації.

Згідно зі звітом директора FBMS президенту Рузвельту, агентство забезпечувало 95% інформації про економічний та психологічний стан Японії. Голова відділу ЗМІ FBMS зазначив: «Ми слухаємо, що люди говорять своїм родичам за кордоном, нейтральним країнам і світу загалом... Наші аналітики — це фахівці, які розуміють психологію, мову, культуру, економіку та традиції ворожої країни. Завдяки пропаганді, адресованій їхнім громадянам, ми отримуємо уявлення про дипломатичні та військові тенденції противника».

Одним із результатів досліджень стало відкриття зв’язку між підвищенням цін на апельсини в Парижі та успішними бомбардуваннями залізничних мостів.

У 1947 році аналітик ЦРУ Кен Шерман заявив, що близько 80% інформації держава отримує з відкритих джерел. Згодом генерал-лейтенант Самуель Уілсон, керівник Розвідувального управління Міністерства оборони США, зазначив, що 90% усіх розвідувальних даних надходить саме з відкритих джерел, тоді як лише 10% припадає на агентурну роботу [6].

Під час Холодної війни діяльність FBMS забезпечила американське керівництво важливою інформацією, зокрема про радянські атомні ракети на Кубі, участь СРСР у конфлікті в Афганістані, а також про кризи в Угорщині та Чехословаччині. У підсумку близько 80% даних про становище Радянського Союзу перед його розпадом було зібрано з відкритих джерел [7].

З часів Другої світової війни і до сьогодення для опису OSINT використовувалися різні терміни [8]:

- public information – загальнодоступна публічна інформація;
- non-secret/ unclassified information – несекретна інформація;

- overt intelligence – відкрита розвідка;

- open/overt information – відкрита інформація;

- white intelligence – «біла» розвідка.

Події 11 вересня 2001 року змусили керівництво США переглянути значення відкритих джерел у системі інформаційно-аналітичної роботи ключових державних установ. У 2004 році американська розвідка розпочала новий етап масштабного реформування. Того ж року президент Джордж Буш підписав закон «Про реформування розвідки та протидію терористичній загрозі» (Intelligence Reform and Terrorism Prevention Act of 2004). Цей закон передбачав інтеграцію OSINT як важливого та рівноправного напрямку діяльності розвідувального співтовариства, а також створення національного центру розвідки, який базуватиметься на аналізі відкритих джерел [9].

2005-2009 рр. – у США був створений центр аналізу розвідувальних матеріалів з відкритих джерел. Це стало наслідком значного збільшення обсягу інформації, яка стала доступною в Інтернеті;

2009 р. - рік «Зеленої революції», що стала визначальною подією в історії OSINTу. Мільйони молодих іранців ввійшли в інтернет, щоб координати свою діяльність, ділилися вірусним контентом; кожен користувач інтернету зміг видобувати інформацію, аналізувати і робити прогнози;

2009-2016 рр. – стрімкий розвиток інтернету, його ролі та впливу на людське життя;

2017 р. – сьогодення – поступове впровадження концепції OSINT не обмежувалося лише сферою оборони, але й поширювалося на інші сфери життєдіяльності людини.

З огляду на досвід використання OSINT, можна стверджувати, що для отримання якісної та актуальної інформації необхідно обробляти велику кількість інформаційних джерел. Для ефективного застосування цього методу недостатньо лише знаходити дані; їх потрібно ретельно обробляти, аналізувати та підтверджувати факти, події та явища, оскільки багато з них створюються з метою дезінформації. Сьогодні в провідних країнах світу

OSINT активно використовують інформаційно-аналітичні підрозділи. Дані про ефективність відкритих джерел підтверджують важливість використання досвіду США та країн Європи для вирішення оперативних, тактичних і стратегічних завдань силових структур [10].

1.3 Огляд інших дисциплін збору розвідданих

У розвідувальному товаристві США є п'ять основних дисциплін збору розвідувальної інформації, до яких відноситься і OSINT. Ці дисципліни використовуються для отримання даних з різних джерел з метою забезпечення національної безпеки, підтримки урядових рішень та виконання інших стратегічних завдань.

OSINT (Open Source Intelligence) є методом збору інформації з відкритих джерел, таких як Інтернет, ЗМІ, офіційні публікації та соціальні мережі. При цьому, існує так званий SOCMINT (Social media intelligence) розвідка соціальних мереж, який застосовується для моніторингу вмісту таких платформ, як Instagram, Facebook. SOCMINT можна розглядати як піддисципліну OSINT, що спеціалізується на аналізі даних із соціальних мереж [11].

HUMINT (Human Intelligence) – це метод збору інформації, що включає агентурну розвідку, спрямовану на отримання інформації різного характеру, такого як військовий, політичний, науково-технічний тощо. Для цього залучаються спеціально завербовані особи (агенти) або розвідники, які працюють під прикриттям. Основна мета такого типу розвідки полягає у здобутті секретних відомостей та документів, які зазвичай неможливо отримати іншими методами [12]. HUMINT — одна з найстаріших дисциплін збору розвідувальної інформації, яка в двадцятому столітті стала основним

інструментом збору даних для урядів, залишаючись таким до кінця століття [11].

SIGINT (Signals Intelligence) - це збір і аналіз інформації з електронних комунікацій, радіочастот і інших сигналів, бере свій початок у 1850-х роках. Це один з найважливіших методів розвідки, що включає перехоплення і дешифрування передач даних. Вона базується на перехопленні сигналів противника та їх обробці, що здійснюється з використанням різних платформ, таких як наземні об’єкти, літаки та кораблі. Цей вид розвідки здебільшого став можливим завдяки винаходу телеграфії. Водночас для запобігання перехопленню повідомлень противником використовуються шифрування навіть для неворожих повідомлень.

У SIGINT здійснюється підключення до каналів передачі сигналів та мереж зв’язку з метою перехоплення електронних комунікацій ворога, а також шифрування та дешифрування повідомлень. Теоретично SIGINT поділяється на три піддисципліни:

- комунікаційна розвідка (COMINT): ця піддисципліна зосереджена на перехопленні комунікаційних сигналів, таких як трафік телепринтерів, азбука Морзе, текстові та голосові повідомлення різних форматів. Основним завданням є перехоплення комунікацій з подальшою їх обробкою та передачею між пристроями, із застосуванням криптографічних методів;

- електронна розвідка (ELINT): фокусується на перехопленні та аналізі некомунікаційних сигналів, які надходять через радіолокаційні системи чи інші джерела електромагнітного випромінювання. В цій сфері зазвичай використовуються інструменти, що є власністю урядів, що зумовлює високий рівень засекреченості та захищеності даних;

- розвідка сигналів іноземних приладів (FISINT): передбачає перехоплення телеметрії космічних апаратів чи систем озброєння. Отримані розвіддані дозволяють проаналізувати основні характеристики цих пристроїв і систем, що може бути критично важливим для розуміння їх потенційних можливостей.

SIGINT - це ключовий компонент сучасних розвідувальних операцій, що забезпечує детальну інформацію про комунікаційні та електронні активності, дозволяючи аналітикам розробляти стратегічні рішення на основі перехоплених даних.

GEOINT (Geospatial Intelligence), відома як геопросторова розвідка, заснована на інтеграції розвідувальних даних із геопросторовою інформацією та зображеннями. Ця дисципліна забезпечує моніторинг людської діяльності, прив'язаної до певної географічної місцевості та її умов, шляхом аналізу частотних, часових і статичних зображень. GEOINT використовується як у військових, так і в цивільних цілях.

Однією з піддисциплін геопросторової розвідки є IMINT (Imagery Intelligence), що фокусується на зборі даних із джерел інфрачервоного випромінювання, лазерів, радіолокаційних датчиків, а також візуальних і супутникових фотографій. У наш час значно зросла кількість космічних апаратів, які здійснюють зйомку, тому все більше урядів отримують доступ до таких розвідданих. Проте питання якості залишається актуальним, і її покращенню сприяє використання високотехнологічних рішень для боротьби з наслідками несприятливих природних явищ.

Існують комерційні рішення, які пропонують знімки з високою роздільною здатністю, такі як Terra Bella, Orthecast, Planet Labs, BlackSky Global, XpressSAR. Завдяки цьому, деякі недержавні суб'єкти, гуманітарні організації та бізнеси мають можливість впроваджувати GEOINT у свою діяльність.

MASINT (Measurement and Signature Intelligence), або вимірювально-сигнатурна розвідка, є загальним терміном, який описує спектр високотехнологічних методів виявлення для вимірювання різних типів сигнатур. Це можуть бути біологічні, хімічні, радіочастотні, акустичні, радіаційні, інфрачервоні, спектроскопічні сигнатури. MASINT використовує технології дистанційного зондування для збору просторових, метричних,

модульних та кутових даних. Цей тип розвідки дозволяє ідентифікувати інформаційні закономірності, які використовуються в інших системах [13].

MASINT поділяється на п’ять основних піддисциплін:

TELINT (Telemetric Intelligence) – телеметрична розвідка, яка фокусується на перехопленні і аналізі телеметричних даних, які зазвичай передаються під час випробувань ракет і космічних апаратів. Це дозволяє збирати дані про роботу системи та її характеристики.

RADINT (Radar Intelligence) – радіолокаційна розвідка, яка спеціалізується на аналізі радіолокаційних сигналів для виявлення та відстеження об'єктів, таких як літаки, кораблі та транспортні засоби.

NUCINT (Nuclear Intelligence) – ядерна розвідка, що займається виявленням і аналізом ядерних випромінювань та інших сигнатур, пов'язаних з ядерною активністю.

IRINT (Infrared Intelligence) – інфрачервона розвідка, яка використовує інфрачервоне випромінювання для збору даних про теплові сигнатури об'єктів, дозволяючи виявляти та ідентифікувати їх навіть у темний час доби.

ACOUSTINT (Acoustic Intelligence) – акустична розвідка, яка аналізує звукові хвилі і вібрації для виявлення та класифікації об'єктів за їх акустичними сигнатурами, таких як підводні човни або інші транспортні засоби.

MASINT застосовується в різних інформаційних середовищах і відіграє важливу роль у багатьох галузях, включаючи:

- виявлення літаків і безпілотників: MASINT здатний ідентифікувати та відстежувати літаки і безпілотні літальні апарати, використовуючи різні сенсори та методи аналізу сигнатур;

- виявлення та відстеження ракет: MASINT може виявляти запуск ракет і відстежувати їх політ, аналізуючи теплові та інші сигнатури;

- оцінка природних ресурсів: Дистанційне зондування допомагає виявляти та оцінювати поклади корисних копалин, ґрунти, водні ресурси та інші природні об'єкти;

- ліквідація наслідків стихійних лих: MASINT використовується для оцінки та моніторингу наслідків природних катастроф, таких як землетруси, урагани, повені, для забезпечення ефективного реагування та ліквідації наслідків;

- моніторинг і контроль надання допомоги біженцям: MASINT допомагає відстежувати та контролювати потоки біженців, забезпечуючи координацію та ефективне надання гуманітарної допомоги.

Завдяки широкому спектру застосувань MASINT є важливим інструментом для урядів і організацій у зборі та аналізі інформації з різних джерел.

1.4 Основи правового використання методів OSINT

Збір та аналіз інформації з відкритих джерел як сфера діяльності повинні здійснюватися в межах нормативно-правового поля держави. Це забезпечується через дотримання конституційних прав у сфері пошуку, збору, передачі та використання інформації в усіх демократичних країнах. Законодавство різних країн світу активно підтримує впровадження систем розвідки з відкритих джерел. Наприклад, у 1996 році в США було прийнято Закон про свободу інформації зобов'язує федеральні відомства забезпечувати громадянам вільний доступ до інформації, що знаходиться в їхньому розпорядженні. Закон містить обмеження, що стосуються матеріалів, пов'язаних з національною обороною, фінансовими та особистими документами, а також документацією правоохоронних органів держави. Водночас, у деяких країнах законодавство накладає обмеження на таку діяльність, фактично забороняючи проведення розвідки з відкритих джерел.

В Україні згідно з Конституцією, "кожен має право вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово або в

інший спосіб – на свій вибір" (Розділ 2, ст. 34). Правове регулювання в інформаційній сфері в Україні ґрунтується на таких принципах:

- свобода законно шукати, отримувати, передавати, виробляти та поширювати інформацію: кожен громадянин має право законно займатися інформаційною діяльністю без будь-яких перешкод;

- встановлення обмежень на доступ до інформації лише законами держави: обмеження на доступ до інформації можуть встановлюватися виключно законодавчими актами;

- відкритість інформації про діяльність державних органів та органів місцевого самоврядування та вільний доступ до такої інформації, за винятком випадків, визначених законодавством: громадяни мають право отримувати інформацію про діяльність державних органів, за умови, що вона не підлягає законодавчим обмеженням;

- поділ інформації за категорією доступу: інформація класифікується як відкрита (загальнодоступна) та з обмеженим доступом. Відкрита інформація доступна для всіх, тоді як до інформації з обмеженим доступом мають доступ лише уповноважені особи чи організації, згідно із законодавством.

Незважаючи на те, що в Україні на сьогодні не існує узаконеного поняття "OSINT" (відкритої розвідки), діяльність зі збирання, зберігання, обробки та розповсюдження інформації регулюється низкою законодавчих та нормативних актів. Основними з них є:

- Закон України “Про інформацію” від 02.10.92 р. № 2657-XII: цей закон встановлює загальні принципи інформаційної діяльності в Україні, включаючи права та обов'язки громадян і організацій у сфері інформації[14].

- Закон України «Про медіа» від 31 березня 2023 року № 2849-IX регулює діяльність у сфері медіа в Україні. Він визначає правові основи функціонування суб'єктів медіа, а також засади державного управління, регулювання та нагляду в цій сфері [15]. Закон вводить низку нових понять для українського законодавства: аудіовізуальне медіа, європейська студія-виробник, багатоканальна електронна комунікаційна мережа, європейський

продукт, медіаграмотність, медіа, користувацьке відео, національний продукт, онлайн-медіа, пакет телеканалів та радіоканалів, незалежна студія-виробник, платформа спільного доступу до відео, платформа спільного доступу до інформації, система умовного доступу, пошукова система, універсальний медіа-сервіс та формат [16].

- Закон України “Про охоронну діяльність” від 22.03.12 р. № 4616-VI: закон регламентує правила ведення охоронної діяльності, включаючи питання захисту інформації та доступу до неї [17].

- Закон України “Про захист персональних даних” від 01.06.10 р. № 2297-VI: він визначає правові основи для захисту персональних даних, встановлюючи правила збору, зберігання та обробки такої інформації [18].

Цивільний кодекс України (ст. 505), Кодекс України про адміністративні правопорушення (ст. 163, ст. 164), Кримінальний кодекс України (ст. 231, 232): ці кодекси містять положення щодо відповідальності за порушення законів в інформаційній сфері, включаючи несанкціонований доступ до інформації та її неправомірне використання.

Варто зауважити, що у певних випадках діяльність з забезпечення безпеки підприємництва в рамках розвідки з відкритих джерел може трактуватися як оперативно-розшукова діяльність. Відповідно до Закону України "Про оперативно-розшукову діяльність" № 2135-XII від 18.02.1992 р. [19], таку діяльність мають право здійснювати лише суб'єкти, згадані у відповідних статтях цього закону.

У Стратегії кібербезпеки України, затвердженій Указом Президента України від 15.03.16 р. № 96/2016 [20], декларуються ключові завдання для силових органів. Серед них передбачено "створення системи своєчасного виявлення, протидії та нейтралізації кіберзагроз, в тому числі із залученням волонтерських організацій". Це безумовно стосується застосування засобів конкурентної розвідки в сфері кібербезпеки.

Чинним Кримінальним кодексом України передбачена кримінальна відповідальність за незаконне збирання та використання відомостей, що

становлять комерційну таємницю, а також за розголошення комерційної таємниці. Однак ця інформація виходить за рамки розвідки з відкритих джерел.

Через досить широке та неоднозначне тлумачення законодавчих норм процедури збору, обробки та зберігання інформації про конкурентів, з одного боку, фактично набувають безкарного статусу, тобто стають легітимними, а з іншого – залишаються малодоступними для громадян. В українській практиці фактично закритий доступ до великого обсягу інформації, яка в інших демократичних країнах є вільно доступною, наприклад, щодо земельних ділянок, нерухомості (наявної і закладеної), наявності банківських рахунків тощо. Більшу частину таких відомостей можна отримати лише через консультації з спеціальними експертами.

Наразі особливо актуальною є проблема криміналізації окремих державних служб, які у своїй діяльності застосовують розвідку з відкритих джерел. Чимало підрозділів служб безпеки як державного, так і приватного секторів використовують бази даних, що містять інформацію про осіб, зокрема персональні дані. Такі інформаційні ресурси застосовуються з позитивною метою, наприклад, для перевірки даних про співробітників, конкурентів чи партнерів. Ймовірно, ці бази даних і надалі будуть використовуватися бізнес-структурами та окремими громадянами, але вони змушені будуть порушувати законодавство, "йти в підпілля". Технічну можливість використання та підтримки подібних баз даних забезпечують численні системи, такі як "Cronos" (оболонки, що легально реалізуються). Завдяки таким інструментам будь-який зацікавлений користувач Інтернету може отримати доступ до численних баз даних, які функціонують на основі цих оболонок [19].

Сьогодні одними з основних цінностей людства є особиста приватність, право на захист життя та свобода слова. Інформація про людей, або персональні дані, стає все більш цінним товаром, за який готові платити значні суми. У руках зловмисників ці дані можуть стати потужною зброєю. Державні органи, банки та великі бізнес-компанії не завжди здатні забезпечити

належний захист баз персональних даних, що зберігаються у них, в результаті чого значний обсяг конфіденційної інформації потрапляє на ринок. Тому захист персональних даних є надзвичайно важливим.

Основними європейськими стандартами у сфері 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 [21]. Ці документи є обов'язковими для всіх держав-членів Європейського Союзу і служать моделями для законодавства, зокрема й для нашої країни. Держави ЄС повинні адаптувати своє законодавство відповідно до цих правових стандартів.

Конституцією України гарантується право на приватність. Стаття 28 забороняє піддавати особу медичним, науковим чи іншим дослідженням без її вільної згоди (захист фізичної приватності), стаття 30 захищає недоторканність житла (територіальну приватність), стаття 31 захищає таємницю листування, телефонних розмов, телеграфної та іншої кореспонденції (комунікаційну приватність), стаття 32 забороняє збір, зберігання, використання та поширення конфіденційної інформації про особу без її згоди (інформаційну приватність).

Конвенція Ради Європи від 28 січня 1981 року “Про захист осіб у зв’язку з автоматичною обробкою персональних даних” (ратифікована Україною 6 липня 2010 року) визначає положення передачі персональних даних через національні кордони у випадках, коли ці дані обробляються автоматизовано або були зібрані для такої обробки.

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

- повне ім'я та прізвище;
- ідентифікаційний номер;
- IP-адреса (в деяких випадках);
- номер посвідчення водія;

- номери кредитних карток;
- цифровий підпис;
- дата народження;
- місце народження;
- генетична інформація [22].

Українське законодавство передбачає, що обробка персональних даних є інформаційною за своєю суттю і регулюється цілою низкою правових актів.

Обробка персональних даних здійснюється за згодою суб'єкта персональних даних, що підтверджується роз'ясненням Уповноваженого Верховної Ради України з прав людини від 8 січня 2014 року ("Роз'яснення до Типового порядку обробки персональних даних"). Це означає, що фізична особа добровільно висловлює свою згоду на обробку її персональних даних, за умови поінформованості, відповідно до визначеної мети обробки. Згода може надаватися у письмовій формі, у формі, що дозволяє зробити висновок про її надання, або в порядку, передбаченому законами України.

Особливу увагу слід приділяти обробці "чутливих" персональних даних, таких як інформація про здоров'я та біометричні дані, оскільки вони становлять особливий ризик для прав суб'єктів. Для обробки таких даних організаціям необхідно дотримуватися суворіших підстав, повідомляти регулятору про їх використання та призначати відповідальну особу за їх захист. Організації повинні оцінювати ризики та доцільність обробки таких даних заздалегідь [23].

Персональні дані мають оброблятися відкрито і прозоро. Суб'єкти даних повинні бути проінформовані про те, хто обробляє їхні дані, які саме дані використовуються, з якою метою, та які у них є права. Якщо дані збираються безпосередньо в особи, повідомлення надається негайно, або ж протягом 30 робочих днів, якщо дані отримані іншим шляхом. Спосіб інформування залежить від конкретного випадку обробки, наприклад, рекрутинг або електронна комерція.

Обробка даних можлива лише в межах, дозволених наданою згодою або іншою підставою. Якщо мета обробки змінюється на несумісну з початковою, як наприклад, дані використовувалися для рекрутингу, а потім для маркетингу, необхідно отримати повторну згоду особи.

Організація повинна чітко визначити, хто має доступ до персональних даних, і надавати його тільки тим, хто потребує цього для виконання професійних обов'язків. Працівники з доступом зобов'язані дотримуватися конфіденційності, що регулюється трудовими договорами або угодами про нерозголошення.

Строки зберігання даних та їх захист залишаються на розсуд організації, але законодавство вимагає, щоб обробка даних тривала не довше, ніж необхідно для цілей, для яких вони були зібрані. Подальша обробка можлива лише в статистичних чи архівних цілях. Організації самостійно визначають терміни зберігання, враховуючи правила документообігу, волю суб'єкта та досягнення цілей обробки.

Захист даних включає технічні та організаційні заходи, такі як тренінги для працівників, процедури доступу до даних та інше. Головне – запобігти несанкціонованому доступу або втраті даних. Політики зберігання даних (data retention policies) повинні документувати строки зберігання та дії після їх закінчення, наприклад, знищення або анонімізація даних.

Передача даних іншим особам також вимагає належної підстави, такої як згода суб'єкта, що дозволяє таку передачу. При передачі даних з України до країн, що не забезпечують належний захист, повинні виконуватись додаткові умови, наприклад, наявність однозначної згоди особи.

При залученні третьої сторони до обробки даних, між організацією та підрядником має бути укладений письмовий договір, що визначає обсяг та мету обробки. В Україні немає вимоги укладати окремі договори про обробку даних, але для важливих партнерів доцільно розглянути комплексний підхід до документування взаємодії.

На розгляді Парламенту перебуває проєкт Закону № 8153 від 25 жовтня 2022 року [24], що має на меті привести українське законодавство у відповідність до норм ЄС. Цей документ пропонує значні зміни в розподілі прав та обов'язків між володільцем (контролером) і розпорядником (оператором) персональних даних, регламентує підстави та порядок транскордонної передачі даних, визначає обов'язки та алгоритми дій у разі витоку даних, а також підсилює відповідальність за порушення у сфері захисту персональних даних.

1.5 Реалізація OSINT-технологій

OSINT (відкрита розвідка) відіграє важливу роль у розслідуванні кіберзлочинів, дозволяючи фахівцям отримувати цінну інформацію з відкритих джерел для ідентифікації злочинців та аналізу атак. Декілька відомих випадків демонструють ефективність OSINT у виявленні деталей кібератак:

- Атака NotPetya (2017 р.)

NotPetya - одна з найбільших кібератак у світі, яка почалася в Україні, але швидко поширилася глобально паралізуючи роботу сотень організацій [25]. OSINT допоміг у виявленні деталей цієї атаки через аналіз технічної інфраструктури, яку використовували зловмисники. Вивчивши відкриті дані, фахівці змогли встановити, що IP-адреси та сервери, які брали участь в атаці, також використовувалися в попередніх операціях Sandworm. Це дало можливість простежити загальну стратегію і почерк цієї групи. Використовуючи відкриті джерела, дослідники ідентифікували шляхи, якими шкідливий код поширювався через компрометовані оновлення українського бухгалтерського ПЗ M.E.Doc.

- DarkHotel (2014 р.)

Угруповання DarkHotel стало відомим завдяки складним кібершпигунським атакам, які були націлені на керівників високого рівня, що зупинялися в готелях. Зловмисники використовували Wi-Fi-мережі готелів для компрометації пристроїв жертв і викрадення конфіденційної інформації, включаючи бізнес-документи, паролі, та інші важливі дані [26]. Одним із ключових моментів у розслідуванні діяльності DarkHotel була ефективність OSINT-розвідки. Досліджуючи діяльність угруповання, аналітики звернули увагу на сертифікати SSL, які використовувалися для забезпечення захищеного з'єднання на вебсайтах та серверах, контрольованих DarkHotel. Ці сертифікати містили інформацію про доменні імена та інші метадані, що дало можливість ідентифікувати пов'язані сервери та визначити, які вебресурси використовувалися для атак. Також були застосовувані інструменти для аналізу доменів, пов'язаних із злочинцями. Вивчаючи, які доменні імена використовувалися для командно-контрольних серверів, експерти змогли виявити зв'язок між різними атаками, що вказували на централізовану інфраструктуру. Хакери часто маскували свою діяльність через VPN та інші засоби, але аналітики змогли виявити декілька фіксованих IP-адрес, які використовувалися для обслуговування командно-контрольної інфраструктури. На основі отриманих даних (сертифікати SSL, домени, IP-адреси) аналітики змогли створити карту взаємопов'язаних серверів, які використовувалися для контролю атак та викрадення даних. Використовуючи OSINT-інструменти для збору інформації з відкритих джерел, таких як інтернет-форуми, реєстри доменів, та сервіси аналізу мережевого трафіку, розслідувачі змогли простежити зв'язки між інфраструктурою атак у різних країнах.

- WannaCry (2017р.)

Атака вірусу-вимагача WannaCry (2017р.) стала однією з най масштабніших кіберінцидентів у світі, уразивши понад 200 000 комп'ютерів у 150 країнах у травні 2017 року. WannaCry поширювався через уразливість у

системі Windows (експлойт EternalBlue, розроблений АНБ США), що дозволило зловмисникам швидко інфікувати тисячі пристроїв [27]. Одним із ключових елементів OSINT-розслідування стало відстеження доменів та IP-адрес, які використовувалися для комунікації з Command & Control серверами, що контролювали поширення вірусу. Британський дослідник Маркус Гатчінс (MalwareTech) виявив прихований механізм зупинки атаки — "kill-switch", який активувався при зверненні вірусу до певного незареєстрованого домену. За допомогою OSINT-методів він знайшов цей домен, зареєстрував його, що дозволило зупинити подальше поширення вірусу. За результатами аналізу, дослідники з'ясували, що за атакою стояло угруповання Lazarus, яке асоціюється з Північною Кореєю. З допомогою OSINT вдалося простежити зв'язок між схожими атаками цього угруповання і використаними методами у WannaCry, що стало основою для приписування атаки цьому угрупованню. Аналіз відкритих джерел, таких як історія доменів, використаних хакерами раніше, IP-адреси, а також аналіз криптовалютних гаманців, до яких вірус надсилав викуп, дозволив створити повну картину атаки та зв'язків між хакерськими групами.

- Атака на «Укрзалізницю» (2022р.)

Атака на «Укрзалізницю» в 2022 році була однією з ключових кібератак, які мали на меті порушити критично важливу інфраструктуру України. Під час цієї атаки постраждала система продажу квитків, що спричинило значні перебої в роботі залізничних перевезень. Одним із перших кроків, який застосовували фахівці кібербезпеки, було використання OSINT-інструментів для аналізу трафіку в мережах «Укрзалізниці». Це дозволило виявити підозрілу активність, яка вказувала на несанкціонований доступ до системи. Фахівці аналізували аномальну поведінку в трафіку, такі як різке збільшення запитів на сервери або спроби з'єднання з невідомими IP-адресами. Використовуючи інструменти, такі як WHOIS та IP-регістри, експерти змогли ідентифікувати IP-адреси, з яких здійснювалася атака. Це дало можливість швидко ідентифікувати хакерське угруповання, яке стояло за цією операцією.

Одним із ключових завдань було встановлення зв'язків між атакуючими IP-адресами та відомими хакерськими угрупованнями. Використовуючи OSINT, аналітики зібрали інформацію про доменні реєстрації, минулі атаки та публікації в темних веб-форумах, що дозволило пов'язати атаку на «Укрзалізницю» з групою, яка раніше здійснювала кібератаки проти українських та інших міжнародних цілей. Через активний моніторинг соціальних мереж і темних веб-ресурсів фахівці змогли виявити, що деякі зловмисники хизувалися своєю участю в атаці. Відкриті дані з таких платформ, як Telegram та інші форуми, дозволили вивчити додаткову інформацію про учасників атаки, що значно допомогло розширити картину подій.

- DDoS-атака на Україну (2022р.)

15 лютого 2022 року Україна зазнала потужної DDoS-атаки (Distributed Denial of Service), яка призвела до тимчасового виведення з ладу важливих державних вебресурсів. Під удар потрапили сайти Міністерства оборони, Збройних сил України, а також двох найбільших банків країни — ПриватБанку та Ощадбанку [28]. Так як DDoS-атаки полягають у перевантаженні сервера величезною кількістю запитів з метою його виведення з ладу.То у випадку з українськими сайтами, атакуючі використовували ботнети для генерації трафіку, що призвело до неможливості доступу до ресурсів. Ця атака не лише вплинула на державні структури, але й викликала занепокоєння серед громадян, оскільки доступ до фінансових послуг був ускладнений. У відповідь на цю кібератаку, були застосовані методи OSINT (Open Source Intelligence) для аналізу та розслідування її походження. Кіберексперти та аналітики використовували відкриті джерела, щоб виявити характер атакуючих, відстежити IP-адреси та аналізувати маршрути трафіку. Це дозволило встановити, які сервери були скомпрометовані і звідки надходив атакуючий трафік. Також через моніторинг соціальних мереж, форумів і новинних ресурсів аналітики могли визначити, чи були ознаки підготовки до атаки, а також виявити можливі зв'язки з відомими хакерськими угрупованнями.

Приклади таких атак, як NotPetya, DarkHotel, WannaCry, атака на «Укрзалізницю» та DDoS-атака на Україну, демонструють, як відкриті джерела інформації можуть бути використані для виявлення злочинців, встановлення зв'язків між ними та розкриття їхніх методів дії. Фахівці з кібербезпеки використовують методи OSINT для збору даних, таких як домени, IP-адреси та SSL-сертифікати, що допомагає ідентифікувати атакуючих та аналізувати їхню інфраструктуру. Цей підхід не лише дозволяє розкрити деталі атак, але й сприяє запобіганню майбутніх злочинів, зміцнюючи загальну безпеку в кіберпросторі.

1.6 Висновки до розділу 1

У цьому розділі були розглянуті теоретичні основи OSINT, що охоплюють визначення, значення та еволюцію цієї дисципліни, а також правові аспекти її застосування. Відкриті джерела розвідки (OSINT) відіграють ключову роль у зборі, аналізі та використанні інформації з доступних публічних ресурсів, що є важливим для ефективного розслідування кіберінцидентів.

Аналіз історії та еволюції OSINT показав, що з розвитком технологій та зростанням обсягів інформації в інтернеті методи відкритої розвідки значно вдосконалилися. Зараз вони є важливим елементом сучасної кіберрозвідки та активно застосовуються як урядовими структурами, так і приватними організаціями для моніторингу, розслідування та запобігання кіберзагрозам.

Порівняння OSINT з іншими дисциплінами збору розвідданих, такими як HUMINT чи SIGINT, показало, що OSINT має унікальні переваги, зокрема доступність, низьку вартість та можливість швидкої обробки великих обсягів даних. Однак, разом з цим, відкриті джерела вимагають ретельної перевірки та

верифікації, оскільки інформація може бути недостовірною або маніпулятивною.

Важливим аспектом OSINT є правове регулювання його використання. Хоча в Україні поки що немає узаконеного поняття "OSINT", діяльність у цій сфері регулюється низкою правових актів, таких як Закон України "Про інформацію", "Про медіа" та "Про захист персональних даних". Однак практичний доступ до інформації в Україні часто обмежений у порівнянні з демократичними країнами, де певні дані є відкритими. Усе більше значення в сучасному світі набуває захист персональних даних, які вважаються цінним товаром. Європейські стандарти, такі як Конвенція Ради Європи та інші міжнародні акти, слугують зразком для розвитку українського законодавства в цій сфері, що стає дедалі актуальнішим у контексті інтеграції до ЄС. Зважаючи на зростання кіберзагроз та недоліки в захисті конфіденційної інформації, важливо продовжувати реформування нормативно-правової бази, спрямованої на забезпечення безпеки інформації та прав громадян на приватність.

Використання OSINT у кібербезпеці відіграє важливу роль у розслідуванні та запобіганні кіберзлочинів. Випадки кібератак, таких як NotPetya, DarkHotel, WannaCry та багато інших, демонструють, як відкриті джерела інформації можуть надати цінні дані для ідентифікації зловмисників, аналізу їх інфраструктури та виявлення їхніх методів дій.

Таким чином, OSINT є невід'ємною частиною сучасної розвідки та кібербезпеки, а його впровадження та розвиток потребують як технічної, так і правової обізнаності. Це забезпечує високий рівень адаптивності до нових загроз у цифровому середовищі.

2 МЕТОДИ OSINT У РОЗСЛІДУВАННІ КІБЕРЗЛОЧИНІВ

2.1 OSINT в життєвому циклі кібератаки

Кібератака починається з вибору зловмисником цілі – компанії або особи, яка стане об'єктом атаки, і збору інформації про неї. Для зловмисників якісна розвідка є ключовою для успішності атаки, тоді як для пентестерів вона важлива для ефективного проведення тестів на проникнення. Це включає відпрацювання різних векторів атак, таких як соціальна інженерія, брутфорс, атаки на Web-додатки, що допомагає виявити вразливості та впровадити контрзаходи для покращення захисту системи [29].

У кібербезпеці OSINT часто використовується для збору публічних даних про компанію з відкритих джерел. Ці дані включають не тільки електронну пошту співробітників, а й IP-адреси, DNS-імена, домени та субдомени, відкриті порти та сервіси, публічні експлойти, механізми безпеки, факти компрометації, конфіденційні документи тощо.

Зі зростанням кількості кіберінцидентів, від яких страждають як організації, так і індивідуальні користувачі Інтернету, стають доступнішими послуги типу Ransomware-as-a-Service (RaaS) або Phishing-as-a-Service (PaaS). Це збільшує число кіберпорушників, оскільки для їх використання не потрібні значні технічні знання. Доступність OSINT-інструментів дозволяє злочинцям непомітно накопичувати інформацію про ціль та планувати атаки, створюючи загрозу для організацій, які часто не підозрюють про кількість доступної про них інформації в мережі.

Важливо розуміти роль OSINT у життєвому циклі кібератаки та досліджувати інструменти для пошуку інформації з відкритих джерел. Це є ефективним способом запобігання потенційним атакам завдяки своєчасному виявленню вразливостей за допомогою тестів на проникнення.

Термін «життєвий цикл кібератаки» (або «cyber kill chain») описує послідовність етапів, які проходить зловмисник під час здійснення кібератаки

— від початкової розвідки до досягнення мети, наприклад, крадіжки даних чи запуску шкідливого програмного забезпечення. Вперше цей термін був запропонований у рамках моделі Intelligence Driven Defense, яка спрямована на виявлення та запобігання кібервторгненням. Модель ідентифікує ключові кроки, які необхідно виконати для успішної реалізації атаки [30].

Завдяки цій моделі можна зрозуміти, що для того, щоб зупинити кібератаку, достатньо порушити діяльність зловмисника на будь-якому з етапів. Оскільки для успішної атаки він має пройти всі кроки, блокування на одному з них може зупинити процес. Основні етапи кібератаки в цій моделі включають: розвідку, підготовку, доставку, експлуатацію, закріплення, отримання управління та виконання дій у системі жертви (рис. 2.1).

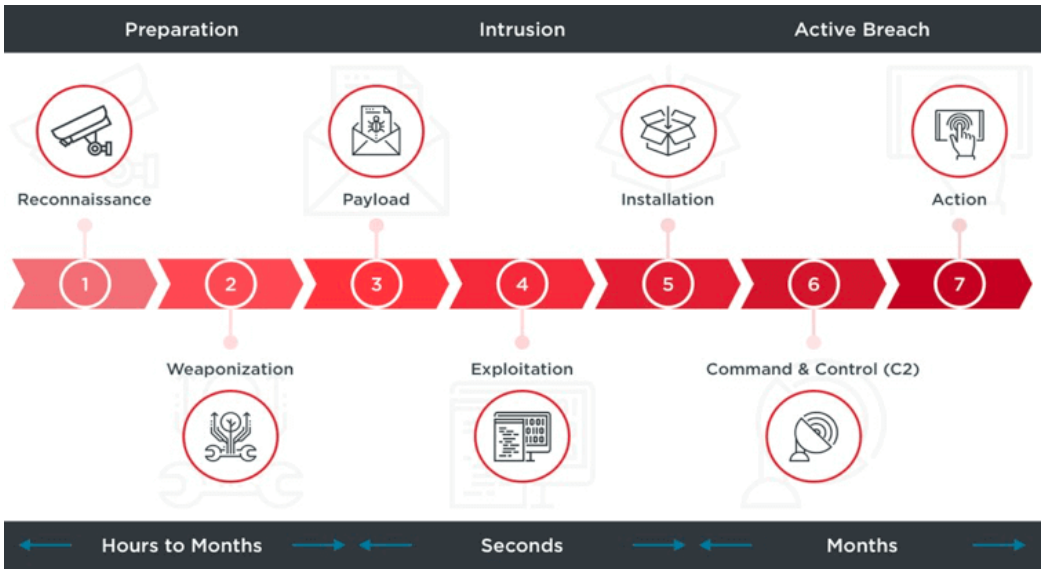


Рисунок 2.1 - Життєвий цикл кібератаки [30]

Перші етапи моделі переважно включають підготовчі дії. Наприклад, етап розвідки може охоплювати різноманітні методи, з яких найпоширенішим є сканування. Метою сканування є виявлення відомих вразливостей, неправильних налаштувань програмного та апаратного забезпечення, застарілого програмного забезпечення та інших слабких місць, що можуть сприяти здійсненню кібератаки. Збирається вся доступна інформація про ціль, включаючи специфіку організації, вимоги до галузі, до якої вона належить,

використовувані технології, а також аналізується активність компанії та її співробітників у соціальних мережах, блогах, форумах тощо. Метою збору такої інформації є виявлення найбільш уразливих точок системи захисту організації, визначення найбільш ймовірних методів атаки та вибір оптимальних з них з огляду на необхідні ресурси та інвестиції для реалізації кібератаки [31].

На другому етапі здійснюється вибір або створення інструментів для атаки. Сучасна кіберзлочинність значно спрощує цей процес для зловмисників. Якщо раніше успішна реалізація атаки вимагала від них глибоких знань для написання шкідливого коду, його впровадження в інформаційну систему організації та викрадення даних, то нині всі необхідні засоби — готові ботнети, набори експлойтів, утиліти для модифікації шкідливих програм, модулі шифрування та інші інструменти — доступні для придбання в даркнеті. Це означає, що навіть особа без спеціальних технічних навичок може скористатися такими послугами. Існує навіть явище, відоме як "вимагання як послуга" (RaaS), коли шкідливе програмне забезпечення потрапляє на комп'ютер жертви, шифрує дані, а потім вимагає викуп за їхнє розшифрування. Використовуючи таку послугу, зловмисник отримує готовий продукт і не потребує розробки власних інструментів.

Ймовірність успішного злому також підвищується через те, що хакери стежать за оновленнями програмного забезпечення і одними з перших отримують патчі, які виправляють вразливості. За допомогою реверс-інжинірингу вони можуть визначити, де розробниками була виявлена проблема, вивчити цю вразливість і створити новий експлойт або модифікувати вже існуючий. Оскільки корпоративні та приватні користувачі часто затримуються з оновленням програмного забезпечення, зловмисники мають час на вивчення оновлень, розробку експлойтів та проведення атак на системи із застарілим програмним забезпеченням.

Третій етап — доставка шкідливого програмного забезпечення в мережу організації. Найчастіше для цього використовують шкідливі електронні листи,

застосовуючи прийоми соціальної інженерії, щоб змусити співробітників відкрити прикріплений файл чи архів, перейти за посиланням або виконати певні дії, зазначені в листі. Ефективна розвідка значно підвищує ймовірність успіху, оскільки дозволяє замаскувати лист так, що навіть підготовлений співробітник повірить, що він надійшов від легітимного джерела.

Під час створення шкідливого електронного листа можуть використовуватися різноманітні дані про ціль, зокрема імена друзів і колег, робочі завдання, якими займається співробітник, улюблені ЗМІ, назва банку, де він обслуговується, а також його хобі та інтереси. Чим більше інформації зібрано про конкретного співробітника, тим більш переконливим і правдоподібним можна зробити текст листа.

Четвертий етап життєвого циклу кібератаки — це злом. На цьому етапі співробітник компанії або приватний користувач відкриває файл, програму чи архів з електронного листа або переходить за шкідливим посиланням, активуючи шкідливе програмне забезпечення. У результаті цього дії зловмисник отримує доступ до зараженого пристрою.

П'ятий етап полягає у встановленні та розгортанні шкідливого програмного забезпечення на вже контрольованому зловмисником пристрої. На цьому етапі завантажуються відсутні модулі та забезпечується постійна присутність в мережі. Виявити таку активність складно, адже шкідливі файли можуть бути замасковані під легітимні, імітуючи звичайну активність користувачів.

Шостий етап — це отримання повного контролю над зараженими машинами та можливість управління ними: відправка команд, завантаження нових модулів для атак, отримання інформації про комп’ютери та встановлене на них програмне забезпечення. Зловмисник, залежно від своїх цілей, може залишатися в мережі тривалий час, щоб визначити подальші вектори атак, такі як зараження інших пристроїв, доступ до інтернет-банкінгу, промислових систем або крадіжка даних.

На сьомому етапі зловмисник реалізує свої наміри: завантажує потрібну інформацію, шифрує дані, шантажує користувача чи організацію, вимагаючи викуп за відновлення доступу, або формує ботнети.

Успішна реалізація атаки, яка охоплює всі сім етапів життєвого циклу кібератаки, потребує ретельної підготовки. Вона включає розвідку, підготовку та доставку шкідливого програмного забезпечення із використанням різноманітних методів та інструментів OSINT. Зловмиснику недостатньо просто знайти вебсайт компанії чи профілі її співробітників у соціальних мережах. Він повинен задіяти повний арсенал розвідувальних навичок, зокрема комунікацію для маніпулювання співробітниками організації або окремими користувачами. Це часто включає застосування технік соціальної інженерії [30].

Проте ефективність OSINT не обмежується тільки збором інформації. Для успішного планування та реалізації атаки зловмисники повинні також вміти аналізувати отримані дані, визначати найбільш ймовірні точки входу і слабкі місця в системі безпеки. Це вимагає глибоких знань у галузі кібербезпеки та постійного відстеження нових уразливостей і методів атак. Використання OSINT дозволяє зловмисникам не лише знаходити інформацію про технічні аспекти системи, але й вивчати людський фактор, що є критичним для успішного виконання атак.

Окрім того, методи OSINT грають важливу роль у розслідуванні кіберінцидентів. Після атаки, ефективне використання OSINT може допомогти в ідентифікації джерела атаки, аналізі її шляхів і виявленні вразливостей, які були використані. Це може включати збір і аналіз інформації з відкритих джерел, таких як публічні звіти про зломи, соціальні медіа, форуми, а також технічні дані, які можуть допомогти відстежити діяльність зловмисника.

У сучасному світі, де технології постійно розвиваються, і кіберзагрози стають все складнішими, важливо не лише виявляти і запобігати атакам, але й постійно удосконалювати свої навички в використанні OSINT. Це дозволяє не

тільки забезпечити більш ефективний захист від потенційних загроз, але й підвищити загальний рівень безпеки інформаційних систем і організацій, а також оперативно реагувати на кіберінциденти і проводити їх детальне розслідування.

2.2 Методи та інструменти збору інформації OSINT

У кібербезпеці OSINT зазвичай використовується для збору публічних даних про компанію, причому це стосується не лише інформації про електронні адреси її співробітників, а також дозволяє збирати широкий спектр даних:

- інформація про DNS-імена та IP-адреси;
- дані про домени та субдомени, зареєстровані на компанію;
- факти компрометації електронних адрес;
- відкриті порти та сервіси на них;
- публічно доступні експлойти для виявлених сервісів;
- конфіденційні документи;
- існуючі механізми безпеки,

які потім використовуються для оцінки ризиків, планування атак або захисту від них [32].

Методи OSINT умовно поділяються на дві категорії: пасивні та активні. До пасивних належать методи, які передбачають пошук інформації виключно у відкритих джерелах без прямої взаємодії з об’єктом атаки. Приклади таких методів:

- збір інформації про діяльність, структуру компанії, її співробітників, керівництво, підрядників із відкритих пошукових систем;
- пошук відкритих персональних даних співробітників компанії у соціальних мережах, месенджерах або інших відкритих джерелах;

- перегляд збережених копій сайтів у пошукових системах для аналізу змін порівняно з поточною інформацією;

- аналіз активності об’єкта у соціальних мережах, на форумах, блогах та інших віртуальних платформах;

- отримання геолокаційних даних за допомогою загальнодоступних сервісів, таких як Google Maps;

- перегляд збережених копій сайтів у пошукових системах для аналізу змін порівняно з поточною інформацією.

Перелічені методи становлять лише невелику частину пасивних методів збору інформації. Проте навіть у такому вигляді, якщо атакуючий володіє відповідними знаннями та вміннями, вони можуть значно полегшити підготовку до кібератаки

Активні методи OSINT передбачають більш детальне дослідження й аналіз інформації. Вони часто вимагають взаємодії з цільовою компанією або особою, що несе певні ризики: у разі підозр з боку цілі, вся підготовка до атаки може бути припинена ще на етапі розвідки. Якщо пасивні методи дозволяють зібрати загальнодоступну інформацію про об’єкт із відкритих джерел, то під час використання активних методів необхідно самостійно ініціювати отримання додаткових даних. Ці методи потребують більше часу, ресурсів та зусиль, але й забезпечують глибше розуміння об’єкта.

До активних методів розвідки належать:

- збір даних із закритих або платних ресурсів;

- використання спеціалізованих сервісів і програм, що здійснюють активну взаємодію з об’єктом (наприклад, автоматичну реєстрацію на сайті);

- застосування інструментів для аналізу файлів, програм чи сайтів на наявність шкідливого коду;

- створення фальшивих сайтів, сторінок або каналів у месенджерах для збору даних про користувачів;

- безпосередній контакт із ціллю.

Отже, пасивні методи є простішими та менш ризикованими для збору інформації, тоді як активні методи — більш складні, але й потенційно ефективніші, хоч і з підвищеним ризиком бути виявленими.

Кожна група методів розвідки передбачає використання певного набору інструментів. Серед найбільш популярних можна виділити такі, як Shodan, Maltego, Google Dorks та Metagoofil. Для досягнення максимальної ефективності рекомендується комбінувати ці інструменти з іншими доступними засобами, адаптуючи їх до конкретних завдань розвідки. Зокрема, розслідування кіберінцидентів також виграє від застосування методів OSINT, оскільки дозволяє відстежувати джерела атаки, аналізувати шляхи компрометації системи та виявляти вразливості, які були використані в атаці. Інструменти OSINT можуть допомогти не тільки в зборі даних до атаки, але й у ретроспективному аналізі і відновленні після інциденту, що є критичним для покращення безпеки та запобігання майбутнім загрозам.

2.2.1 Shodan

Shodan.io - це інтернет-ресурс, який надає інформацію про підключені до мережі пристрої за їх IP-адресами. Цей ресурс можна розглядати як пошукову систему для підключених до Інтернету серверів, таких як веб-камери, маршрутизатори та інші пристрої [33]. Деякі користувачі описують Shodan як пошукову систему сервісних банерів, тобто метаданих, які сервер надсилає клієнту у відповідь. Ці метадані можуть включати інформацію про програмне забезпечення, підтримувані опції сервісу, вітальне повідомлення тощо, які клієнт повинен з’ясувати перед взаємодією з сервером. Цей інструмент дозволяє ефективно моніторити стан мережі. Команди з кібербезпеки можуть використовувати Shodan для відстеження серверів і пристроїв у своїй мережі, які мають прямий доступ до Інтернету і, відповідно, можуть стати

потенційними об'єктами атак. Крім того, можливості Shodan охоплюють аналіз ринку, виявлення вразливостей та проведення тестів на проникнення, що робить його універсальним інструментом для кіберзахисту та розвідки.

Результати пошуку можна фільтрувати за допомогою таких конструкцій:

- country: країна в форматі UK, RU, US і тощо, наприклад: nginx country: UA

- city: місто, наприклад: nginx city:«Ternopil» country:UA

- os: операційна система, наприклад: microsoft-iis os:«windows 2011»

Shodan збирає дані про веб-сервери HTTP/HTTPS (порти 80, 8080, 443, 8443), FTP (порт 21), SSH (порт 22), Telnet (порт 23), SNMP (порт 161), IMAP (порти 143, 993), SMTP (порт 25), SIP (порт 5060), RTSP (порт 554) та інші (рис.2.2). Протокол RTSP, наприклад, може використовуватися для доступу до веб-камер та відеопотоків.

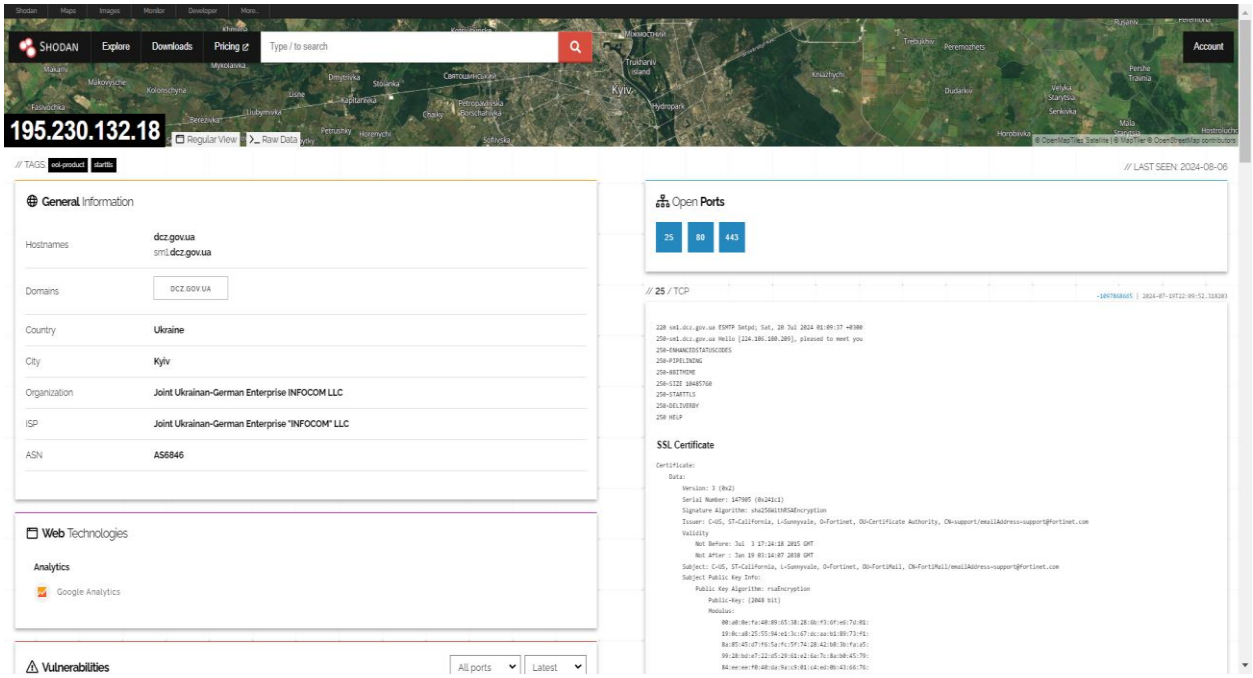


Рисунок 2.2 - Дані зібрані по за допомогою Shodan.io по хосту dcz.gov.ua (Державна служба зайнятості)

Shodan також має функціонал для виявлення вразливостей ресурсів та відображення їх CVE (Common Vulnerabilities and Exposures) (рис. 2.3). Це

дозволяє знаходити методи вирішення проблем, скориставшись загальною базою даних, такою як https://www.cve.org.

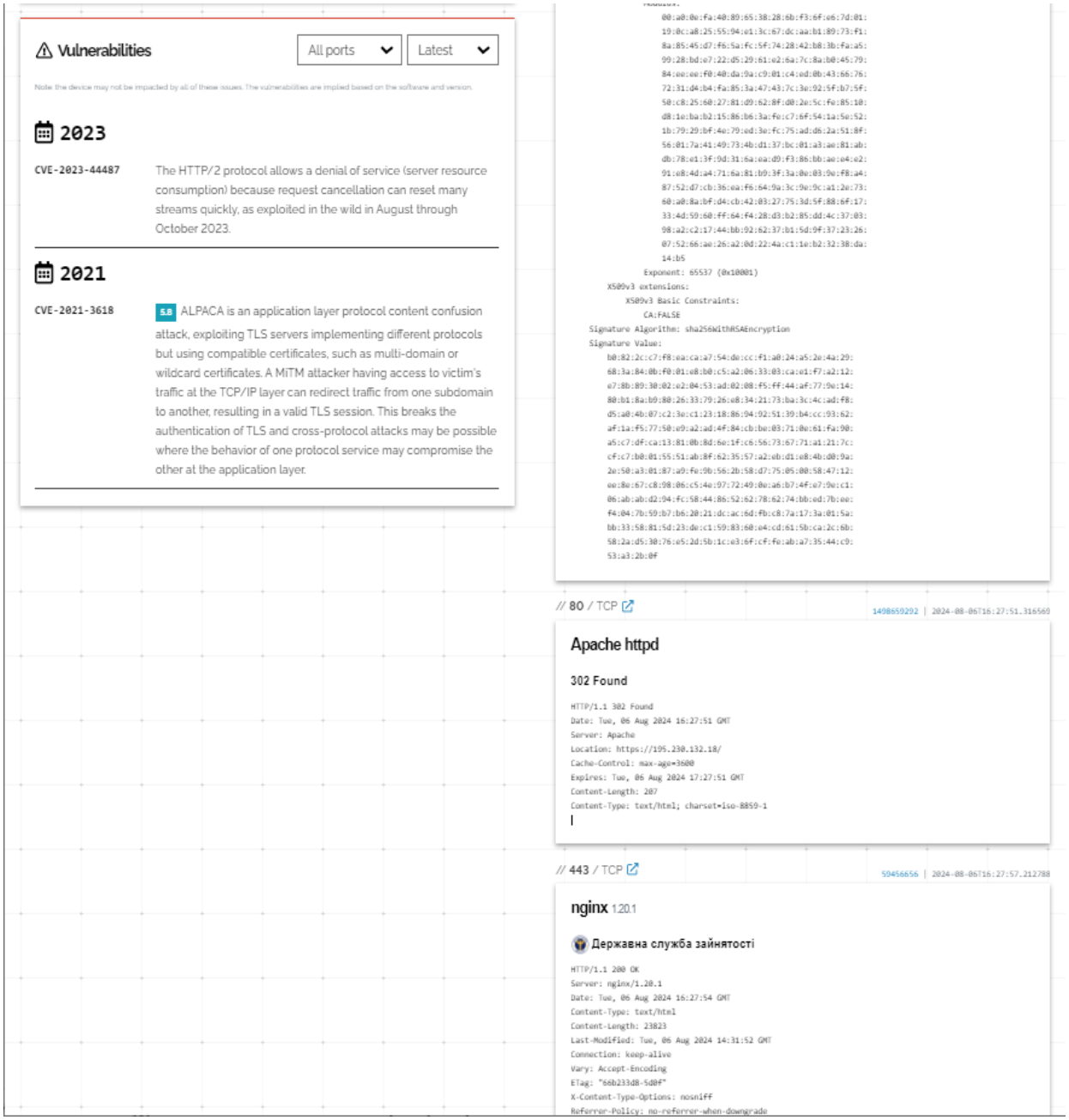


Рисунок 2.3 - Вразливості та SSL сертифікат для сайту dcz.gov.ua

Зібрані дані можна використовувати для аналізу вразливостей, сканування та моніторингу цільових ресурсів або цілих мереж у режимі реального часу. Shodan дозволяє виявляти витоки даних у хмару, фішингові веб-сайти, зламані бази даних тощо. Крім того, він надає інструменти для

моніторингу всіх підключених пристроїв в Інтернеті з можливістю налаштування зручного оповіщення про результати моніторингу та виявлення будь-яких аномалій.

Для доступу до розширеного пошуку необхідно зареєструватися. Платні версії пропонують доступ до більшої кількості пристроїв і необмежену кількість пошуків на день.

Shodan відіграє важливу роль у кібероslідуванні завдяки своїй здатності знаходити сервери, камери відеоспостереження, бази даних, інтернет речей (IoT) та інші підключені пристрої. Shodan дозволяє дослідникам і кіберзлочинцям виявляти уразливі пристрої з відкритими портами, незахищеними інтерфейсами або відомими вразливостями. Це робить його важливим інструментом для моніторингу та аналізу інфраструктури, відстеження змін у мережах організацій або окремих осіб, а також визначення, які сервіси і пристрої підключені до мережі та як вони налаштовані.

У процесі кібероslідувань Shodan допомагає відстежувати джерела атак, знаходити підозрілі активності, а також збирати додаткову інформацію для атрибуції атак. Крім того, Shodan може використовуватись для пошуку витоків конфіденційної інформації, яка може бути випадково виставлена в Інтернет через некоректно налаштовані пристрої.

Shodan також допомагає оцінювати рівень загрози для певної організації чи інфраструктури, виявляючи вразливі точки, які можуть бути використані в кібератаках.

2.2.2 Recon-ng

Recon-ng — це розвідувальний фреймворк на Python, який надає ефективне середовище для швидкого та детального виконання OSINT-розвідки з відкритих джерел [34]. У комплекті поставляються незалежні

модулі, взаємодія з власною базою даних, зручні вбудовані функції, інтерактивна допомога тощо. Встановити всі доступні модулі можна командою: marketplace install all під час першого запуску інструменту, тому що вони можуть спочатку бути відсутніми. Деякі модулі під час роботи взаємодіють з API різних сервісів, як-от: Google, Github, Bing тощо, для них необхідно буде отримати API ключ і вказати його командою keys add.

Подивитися список ключів можна командою keys list, де буде виведена таблиця (рис. 2.4).

Для перегляду основних команд необхідно викликати довідку (рис. 2.5).

Цей інструмент дозволяє користувачам визначати субдомени для конкретного домену та виконувати інші типові операції, такі як взаємодія з базами даних, виконання веб-запитів, керування ключами API та стандартизація вихідного вмісту.

Recon-ng підтримує численні модулі, які дозволяють підключатися до різних сервісів, таких як Shodan, GitHub, Jigsaw, VirusTotal та інших, що розширює можливості інструменту та робить його ще більш ефективним для проведення розвідки.

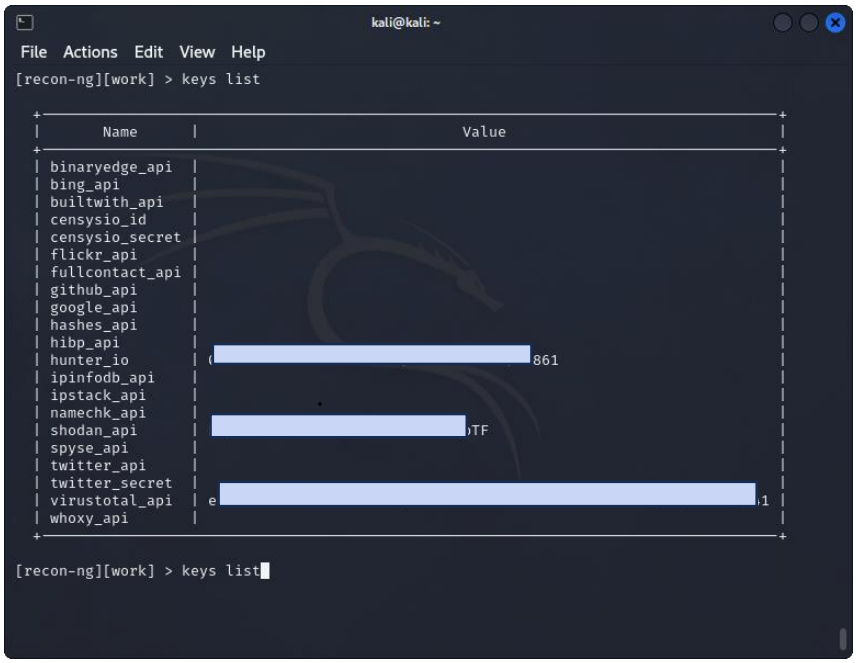


Рисунок 2.4 - Список ключів Recon-ng

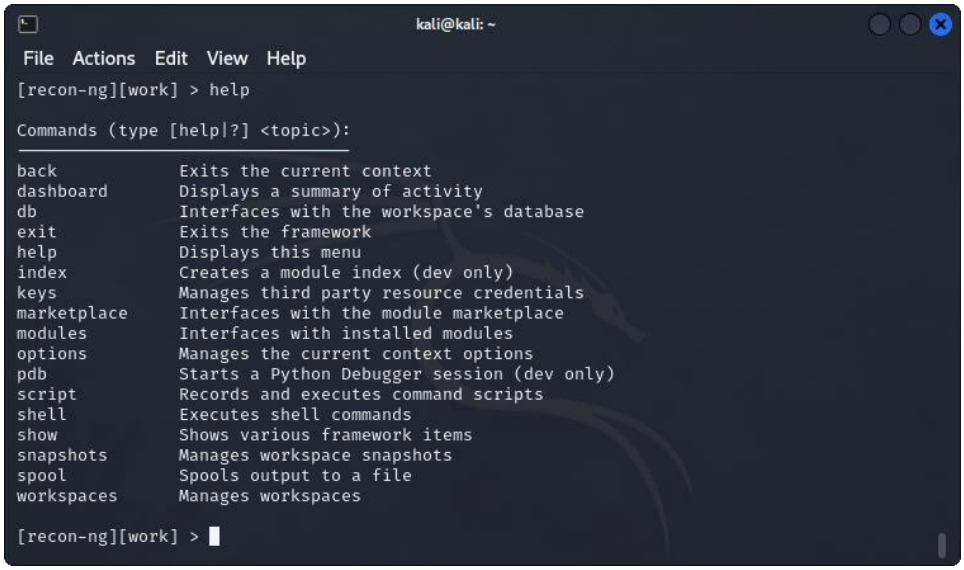


Рисунок. 2.5 - Довідка Recon-ng

Завдяки модульній архітектурі, Recon-ng підтримує численні джерела даних, включаючи пошукові системи, соціальні мережі, бази даних доменів та інші ресурси, що дозволяє отримати широкий спектр даних про цільову систему або організацію. Інструмент дозволяє легко визначати субдомени для конкретного домену, що може допомогти у виявленні додаткових точок входу для потенційних атак. Recon-ng може використовуватися для збору інформації про IP-адреси та їх географічне розташування, що допомагає в ідентифікації джерел загроз або аналізу мережевої інфраструктури. Завдяки підтримці різних модулів, Recon-ng дозволяє інтегруватися з такими сервісами, як Shodan, GitHub, Jigsaw, VirusTotal, що робить збір даних ще більш зручним і ефективним. Інструмент підтримує генерацію звітів, що дозволяє зручно документувати результати розвідки, зберігаючи їх для подальшого аналізу або використання в інших процесах.

Recon-ng дозволяє, використовуючи простий пошук, знаходити веб-камери, паролі за замовчуванням, маршрутизатори, світлофори та інші пристрої, підключені до Інтернету, що може бути важливим під час проведення кіберослідувань або оцінки рівня загрози.

Recon-ng широко використовується фахівцями з кібербезпеки для збору попередньої інформації перед проведенням тестування на проникнення або під час кіберослідувань. Цей інструмент дозволяє збирати важливі дані, такі як доменні імена, інформацію про сервери, контактні дані та інші метадані, які можуть бути використані для розробки стратегії атаки або оцінки рівня загрози.

Recon-ng також може бути корисним для виявлення вразливих точок в інфраструктурі організації, допомагаючи визначити, які системи або сервіси можуть бути найбільш схильні до атак. Інтеграція з різними сервісами та базами даних дозволяє отримувати актуальну інформацію та швидко реагувати на нові загрози.

2.2.3 TIDoS

TIDoS Framework— це набір інструментів із відкритим вихідним кодом, яким можна користуватися безкоштовно. Цей набір інструментів надає всі основні тести веб-додатків, як-от сканування цілі, процес перерахування, оцінка та аналіз уразливостей [35]. Цей інструмент допомагає в проведенні кіберослідувань, аналізуючи доступні дані та виявляючи потенційні загрози або вразливості. Під час запуску програми необхідно ввести домен, що цікавить, і вказати, чи використовується SSL (рис. 2.6).

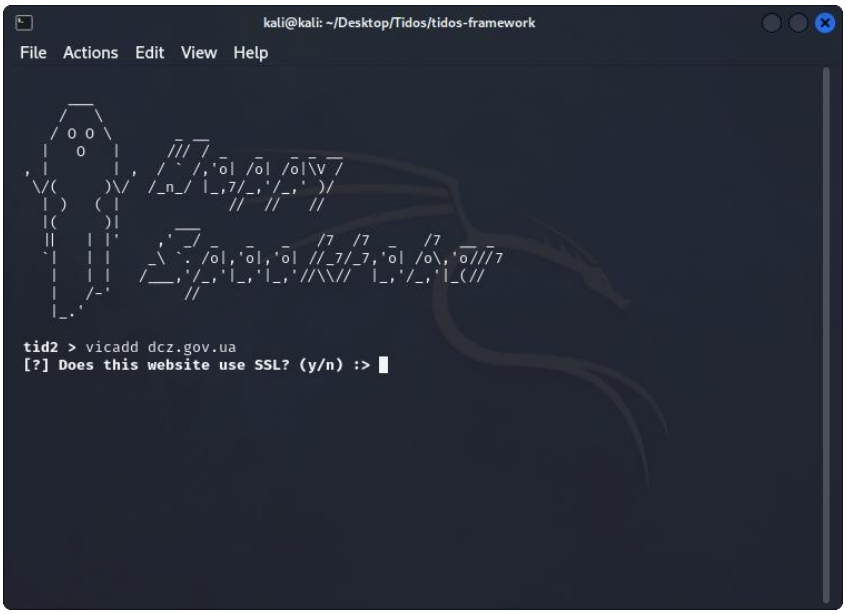


Рисунок 2.6 - Використовується SSL у TIDoS

TIDoS складається з 5 основних етапів, які підрозділяються на 14 підетапів. Загалом TIDoS має 108 модулів, що дозволяють виконувати різні типи збору інформації та виявлення вразливостей. За допомогою команди list можна побачити модулі (рис. 2.7) [36].

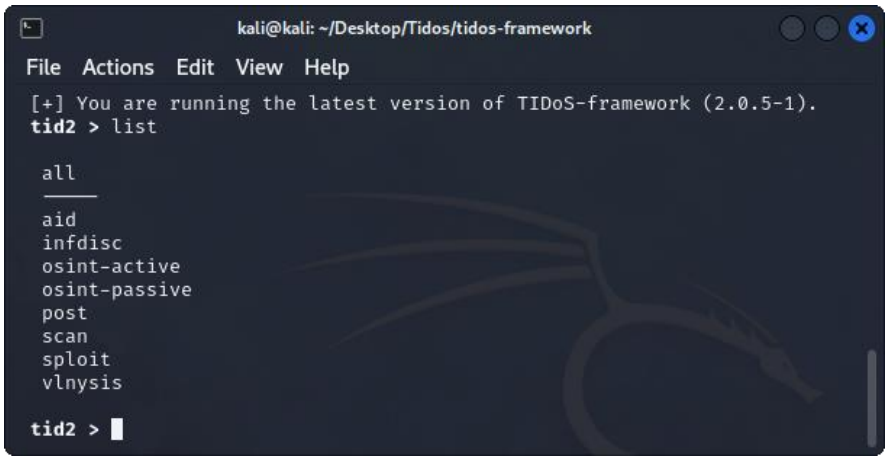


Рисунок 2.7 – Використання команди list у TIDoS

Для при розслідуванні кіберінцидентів за допомогою OSINT використовуються модулі osint-passive і osint-passive, що містить близько 50 модулів. Osint-passive дає змогу проводити пасивний збір даних (рис. 2.8):

Рисунок 2.8 - Список модулів пасивного збору у TIDoS

- пошук email-адрес та іншу контактну інформацію в Інтернеті;
- інформацію про домен (whois-інформація);
- інформацію про конфігурацію DNS;
- список субдоменів;
- список підмереж тощо.

Так і з osint-active можна проводити активний збір даних (рис. 2.9):

- перевірка сертифікатів SSL;
- перевірка файлів robots.txt і sitemap.xml;
- виявлення CMS;
- визначення альтернативних версій сайту шляхом звернення з різним параметром User-Agent;
- пошук файлів типу info.php і його можливих варіацій тощо.

Рисунок 2.9 - Список модулів активного збору у TIDoS

2.2.4 Maltego

Maltego — це потужне програмне забезпечення для збору інформації з відкритих джерел (OSINT), розроблене компанією Paterva [37]. Воно відоме своєю здатністю збирати та аналізувати дані з різноманітних джерел. Maltego дозволяє проводити пошук інформації у профілях соціальних мереж, за електронними адресами, номерами телефонів та іншими параметрами. Ця інформація може бути корисною для приватних осіб, компаній та організацій для вирішення професійних питань.

Maltego широко використовується у судових розслідуваннях та криміналістиці, оскільки він дозволяє визначати геолокацію кіберзлочинців, а

також дізнаватися особисті дані, що можуть бути необхідними для розслідувань. Програма є незамінною для правоохоронних органів та приватних детективів, допомагаючи їм виявляти злочинців, які можуть використовувати різноманітні схеми обману, такі як спам-атаки, реєстрація фішингових доменів та зламування облікових записів.

Це програмне забезпечення також допомагає журналістам під час розслідувань, дозволяючи їм знаходити потрібну інформацію. Maltego працює на всіх основних операційних системах (Windows, Mac, Linux) і виконує аналіз за допомогою запитів до записів DNS, WHOIS, пошукових систем, різноманітних API, а також отриманням метаданих [38].

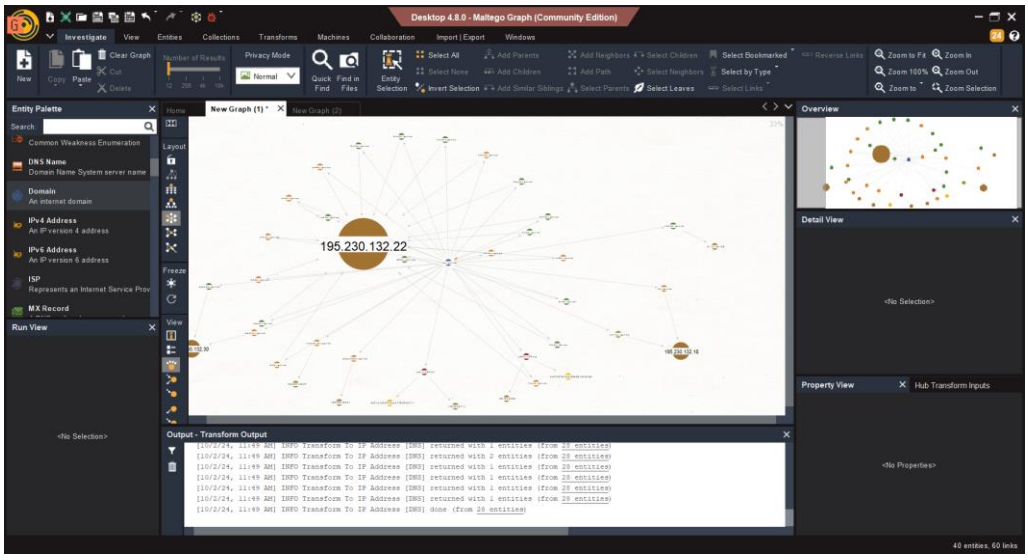


Рисунок 2.10 - Візуалізація зібраних даних у вигляді графів

Однією з головних особливостей Maltego є його здатність візуалізувати зібрані дані у вигляді графів (рис. 2.10), що дозволяє легко розуміти та аналізувати складні зв'язки між різними об'єктами. Програма використовує три основні елементи: Entities (об’єкти), Transforms (процеси) та Links (зв’язки). Об’єктами можуть бути люди, організації, комп'ютери, вебсайти та інше. Всі елементи розміщені на робочій області, а користувачі можуть змінювати візуальне подання графа, щоб краще аналізувати взаємозв’язки між ними.

Завдяки своїм потужним можливостям, Maltego є незамінним інструментом для розслідувань, кібербезпеки та інших сфер, де важливо швидко знаходити, аналізувати та візуалізувати інформацію.

2.2.5 theHarvester

theHarvester (навмисно пишеться з малої літери «t» на початку) — це інструмент на основі командного рядка, розроблений командою Edge-Security. Розроблений на основі Python, він призначений для збору розвідувальних даних із відкритих джерел (OSINT) на початкових етапах розслідування. Його основною метою є допомога у визначенні зовнішніх загроз, з якими може стикатися компанія в Інтернеті.

theHarvester дозволяє збирати такі важливі дані, як електронні адреси, імена, субдомени, IP-адреси та URL-адреси, використовуючи численні відкриті джерела, такі як пошукові системи (Google, Bing, Baidu, Yahoo), сервери ключів PGP і соціальні мережі (LinkedIn, Twitter). Однією з важливих функцій є можливість пошуку віртуальних хостів за допомогою DNS-запитів, що дозволяє перевіряти кількість імен хостів, пов’язаних з певною IP-адресою.

Ось кілька пасивних і активних джерел розвідувальних даних, які використовує theHarvester [39]:

Пасивний:

- Baidu
- Bing
- dnsdumpster
- Duckduckgo
- Google
- Hunter
- Qwant

- SecurityTrails
- Shodan
- Trello
- Twitter

Активний:

- DNS Bruteforcing: перерахування словника брутфорсом
- Screenshots: зробіть знімки екрана знайдених субдоменів

Завдяки своїй ефективності та можливості працювати з широким спектром джерел даних, theHarvester є цінним інструментом у сфері кібербезпеки, допомагаючи як у визначенні потенційних загроз, так і в зборі критично важливої інформації про цільові системи та мережі.

2.2.6 Metagoofil

Metagoofil - це безкоштовна програма з відкритим вихідним кодом на GitHub для збору метаданих з публічних документів, що особливо корисно на етапі збору інформації під час тестування на проникнення (рис. 2.11).

Основна функція Metagoofil полягає у вилученні даних з файлів різних форматів, таких як PDF, DOC, XLS, PPT, та інших, розміщених на веб-сайтах цільових компаній [32].

Інструмент використовує бібліотеки Hachoir та PdfMiner для обробки та аналізу метаданих. Ці метадані можуть містити важливу інформацію, таку як імена користувачів, версії програмного забезпечення, а також дані про сервери або машини, що можуть бути використані під час планування атак.

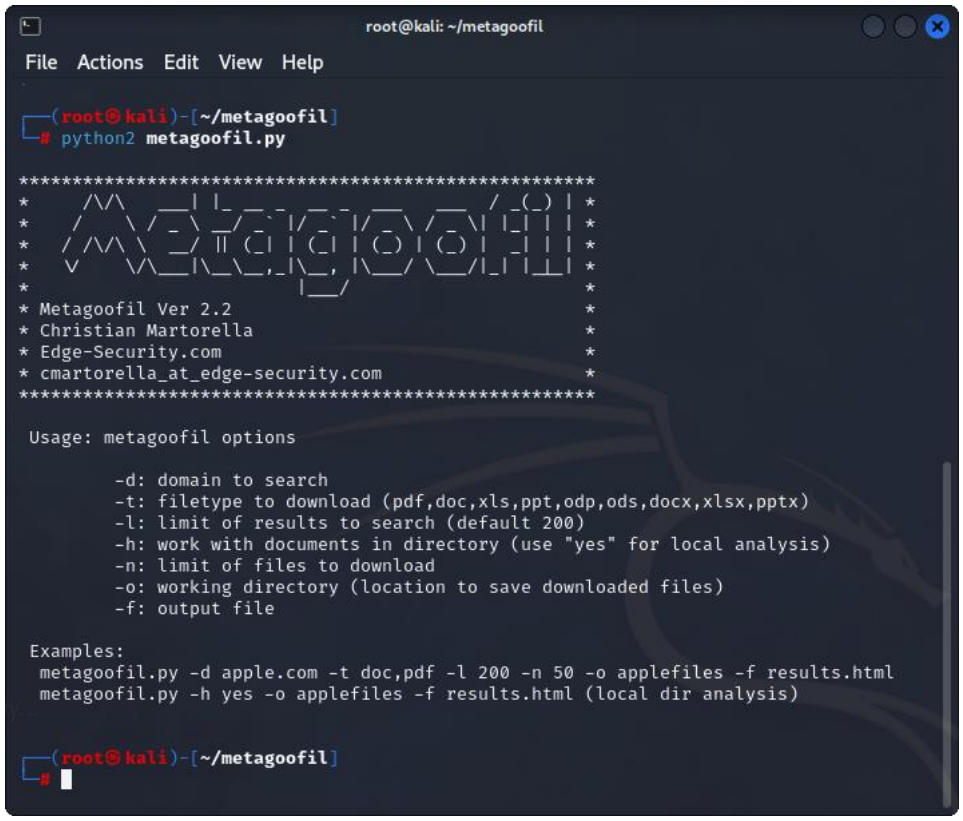


Рисунок 2.11 – Metagoofil

Крім того, Metagoofil може вилучати MAC-адреси з документів Microsoft Office та надавати відомості про апаратне забезпечення системи, яка використовувалася для створення документів. Це робить його незамінним інструментом для тестувальників, які займаються кібербезпекою.

2.2.7 SpiderFoot

SpiderFoot — це потужний інструмент збору даних з відкритим кодом, доступний для Linux та Windows. Розроблений на мові Python, він є високо конфігурованим і може працювати на практично будь-якій платформі. SpiderFoot автоматично запитує понад 100 відкритих джерел даних (OSINT) для збору інформації про IP-адреси, доменні імена, адреси електронної пошти, імена та інші деталі.

Щоб скористатися SpiderFoot, потрібно просто вказати ціль дослідження та вибрати модулі, які потрібно активувати [32]. Інструмент збирає дані, створюючи розуміння всіх сутностей та їх взаємозв'язків. Він спрощує процес компіляції OSINT шляхом автоматизації збору інформації.

SpiderFoot підтримує широкий спектр типів запитів, зокрема доменне ім'я, IP-адресу, хост чи субдомен, підмережу, біткойн-адресу, електронну пошту, номер телефону, ім'я користувача або людини, а також номер автономної системи мережі. Якщо хтось завантажує зображення в загальнодоступні соціальні мережі з активованою функцією геолокації, SpiderFoot може отримати повну інформацію про місцезнаходження цієї особи, що може бути корисним для розслідування кіберінцидентів та інших завдань, що потребують детального аналізу зібраних даних.

2.2.8 OSINT Framework

OSINT Framework — це потужний і цінний ресурс для збору розвідувальної інформації з відкритих джерел, створений і підтримуваний Джастіном Нордіном. Цей проєкт із відкритим кодом надає доступ до великої кількості безкоштовних інструментів і ресурсів, що допомагають користувачам знаходити та використовувати OSINT-ресурси для онлайн-розслідувань, зокрема розслідувань кіберінцидентів.

Фреймворк містить понад 150 інструментів і ресурсів (рис. 2.12), кожен із яких має власний набір функцій і можливостей [40]. Наприклад, Shodan використовується для виявлення пристроїв і мереж, Maltego — для візуалізації даних, а theHarvester — для розвідки електронної пошти та імен користувачів. У контексті розслідувань кіберінцидентів ці інструменти можуть бути особливо корисними для виявлення вразливих пристроїв, аналізу загроз та ідентифікації зловмисників.

Однією з головних переваг OSINT Framework є те, що він є повністю безкоштовним і відкритим, що дозволяє кожному завантажити та використовувати його без обмежень. Крім того, активна спільнота користувачів постійно розширює його функціональність, додаючи нові інструменти та ресурси, що робить його ефективним рішенням для розслідування кіберінцидентів.

Фреймворк розроблений так, щоб бути зручним навіть для тих, хто не має технічного досвіду, оскільки його інструменти прості для навігації, а структура організована таким чином, що полегшує пошук потрібного інструменту. Це робить OSINT Framework ідеальним вибором для дослідників, журналістів та інших фахівців, які покладаються на інформацію з відкритих джерел у своїй роботі, зокрема для фахівців з кібербезпеки, які розслідують кіберінциденти.

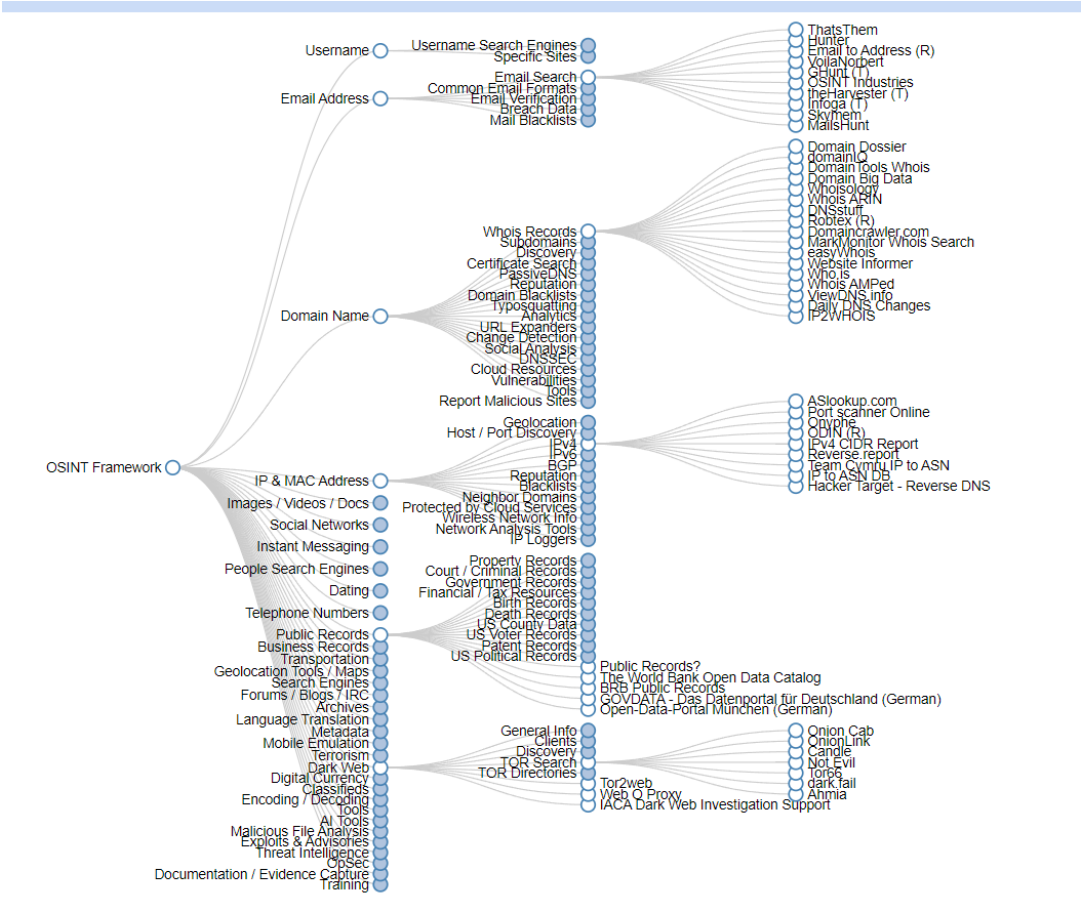


Рисунок 2.12 - OSINT Framework

Під час розслідування кіберінцидентів OSINT Framework допомагає користувачам ефективно організовувати та обробляти велику кількість інформації з різних публічних платформ, таких як новини, зображення та соціальні мережі. Це дозволяє виявляти та аналізувати загрози, відслідковувати активність зловмисників, знаходити витоки даних та здійснювати інші важливі завдання, пов'язані з кібербезпекою.

Завдяки феномену сегрегації — розділення або відокремлення інформації - інструменти OSINT Framework спрощують процес збору та аналізу даних, що дозволяє досягати оптимальних результатів у розслідуванні кіберінцидентів. Це робить OSINT Framework незамінним інструментом для фахівців з кібербезпеки, які прагнуть забезпечити надійний захист своїх систем та мереж від кіберзагроз.

OSINT Framework надає каталог джерел даних та корисних посилань на ефективні інструменти, що спрощує процес пошуку інформації. Це включає різні публічні платформи, такі як новини, зображення, соціальні мережі тощо. Завдяки цьому, OSINT Framework допомагає організувати і обробити велику кількість інформації, що робить її більш актуальною та цінною.

Інструменти OSINT, представлені у фреймворку, полегшують процес збору та аналізу даних завдяки феномену сегрегації – розділення або відокремлення інформації. Цей фреймворк використовується в різних галузях для досягнення оптимальних результатів, надаючи ефективні рішення для збору, організації та аналізу розвідувальної інформації.

2.2.9 Cobwebs

Компанія Cobwebs розробила потужне рішення для веб-аналітики з використанням штучного інтелекту, яке активно застосовується для розслідувань у цифровому середовищі, включаючи даркнет. Це рішення

використовує передові алгоритми машинного навчання для збору та аналізу даних з різних джерел в Інтернеті. На тлі стрімкого зростання темного інтернету потреба в веб-розслідуваннях також зросла, що зробило веб-дослідження від Cobwebs особливо популярними.

Платформа Cobwebs побудована на основі штучного інтелекту, що дозволяє проводити розширені автоматизовані веб-розслідування. Дані з мережі витягуються за допомогою комплексної технології OSINT, що дозволяє аналітикам швидко виявляти нові загрози і знаходити приховану інформацію. Це досягається за допомогою автоматизованих і детальних можливостей пошуку, що значно підвищує ефективність роботи [41].

Переваги платформи від Cobwebs для розслідування:

- отримання важливої інформації в режимі реального часу за різними критеріями;
- доступ до всіх джерел даних у Мережі;
- повна автоматизація;
- візуалізація розслідувань – перегляд даних на інтерактивному графіку.

Програмне рішення Cobwebs використовується як приватними, так і державними компаніями. Воно знайшло застосування в кримінальних розслідуваннях, у сфері кібербезпеки, а також у фінансових установах, де критично важливо швидко і точно ідентифікувати загрози та аналізувати дані.

2.2.10 Використання пошукових сервісів

Під час розслідування кіберінцидентів важливо використовувати різні пошукові сервіси, такі як Google, Yahoo та інші, для збору інформації. Щоб прискорити та полегшити процес пошуку, можна застосовувати оператори пошуку. Без них знайти необхідну інформацію може бути складно або майже неможливо.

Пошукові оператори та техніка Google Dorking, також відомий як Google Hacking [42], є потужними інструментами для розслідування кіберінцидентів, дозволяючи знаходити вразливі фрагменти тексту на веб-сторінках, які можуть свідчити про наявність уразливих версій веб-додатків та значно розширити можливості пошуку та збору інформації. Одна з найбільших баз Google-дорків доступна на сайті ExploitDB (рис. 2.13).

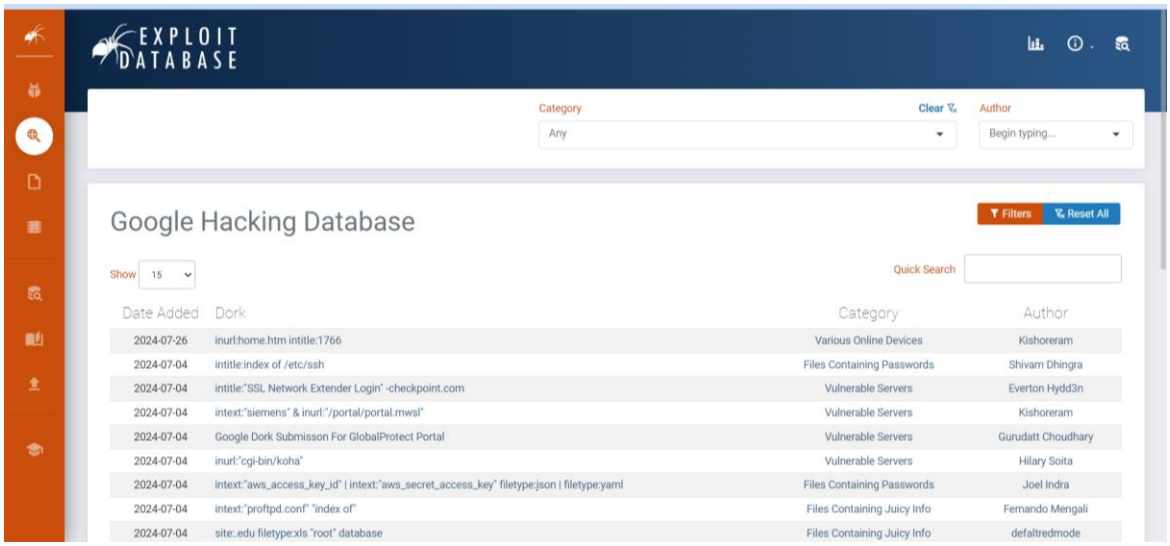


Рисунок 2.13 - Головна сторінка сайту Exploit Database

Більшість пошукових систем підтримують використання команд у пошуковому рядку, які називаються операторами. Зазвичай оператори складаються з двох частин: вид оператора (наприклад, site: для вказування веб-сайту або filetype: для типу файлу) і відповідного правила для оператора (наприклад, цільовий домен або тип файлу). Використання операторів пошуку, таких як site:, filetype:, inurl:, і intitle:, допомагає фільтрувати результати пошуку, дозволяючи отримати лише релевантну інформацію. Наприклад, використання оператора site: dcz.gov.ua обмежує результати пошуку сторінками з одного сайту, а filetype:pdf допомагає знайти документи певного типу на цьому сайті.

Наприклад, на запит "dcz.gov.ua" Google видає близько 327 000 результатів. Але за допомогою оператора site: кількість результатів можна

скоротити до 124 000, а додавши оператор filetype:pdf, отримати всього 1 860 результатів (рис.2.14). Це дозволяє відфільтрувати зайву інформацію та знайти саме те, що потрібно.

Ця техніка також дозволяє знайти документи та інші файли, які можуть бути не індексовані стандартними пошуковими запитами, але доступні в Інтернеті. Методи Google Dorking, такі як allintitle:, intext:, inurl:, filetype:, і cache:, допомагають знайти специфічні дані, наприклад, звіти або податкові декларації, які можуть не бути відразу видимими при звичайному пошуку [43].

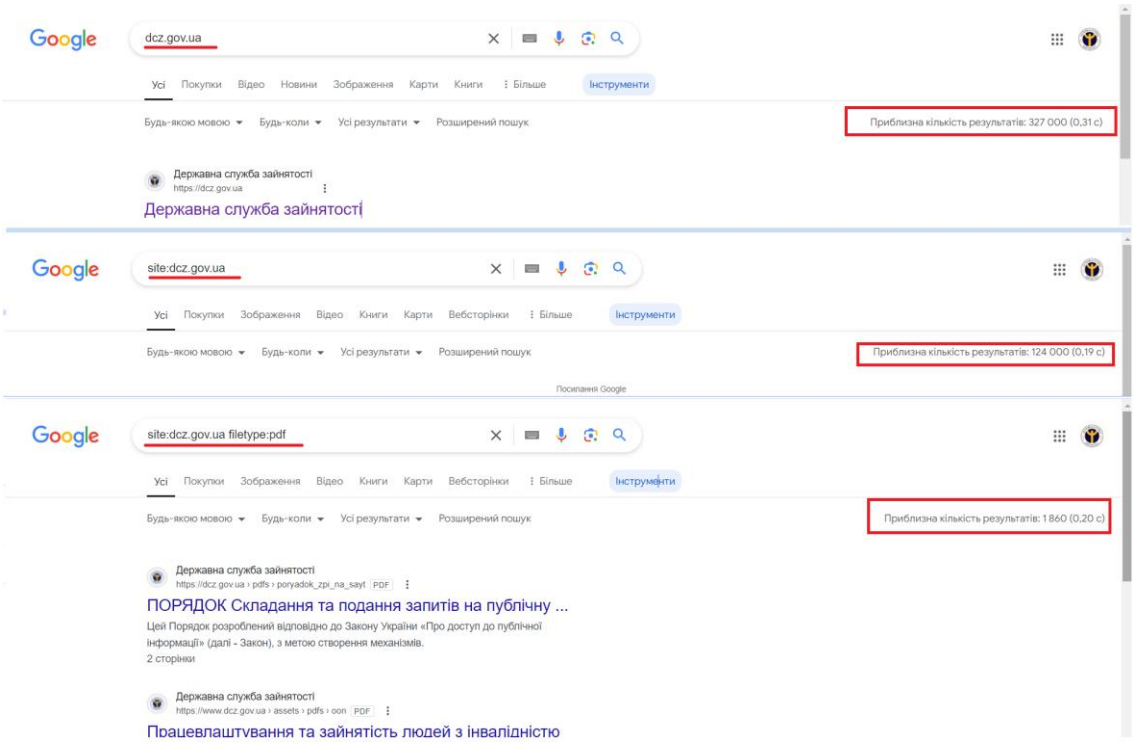


Рисунок 2.14 - Використання операторів пошуку

Припустимо, ви розслідуєте можливий витік інформації на певному веб-сайті. Ви можете використати Google Dorking, щоб знайти файли, які були випадково опубліковані або залишені доступними на сервері. Наприклад, використання запиту site:example.com filetype:xls inurl:password може показати електронні таблиці на сайті "example.com", у яких згадується слово "password" у URL. Це може виявити важливі документи, які містять конфіденційну інформацію. Аналогічно, запит intitle:"index of" "backup" може допомогти

знайти відкриті каталоги з резервними копіями файлів, що може свідчити про наявність уразливих даних [44].

Щоб знайти інформацію, яку організація спочатку публікувала в Інтернеті, а потім видалила (наприклад, через допуск помилки або втрату актуальності), можна скористатися сервісом Archive.org. Це архів Інтернету, що функціонує з 1996 року і надає можливість переглядати збережені копії веб-сторінок, графічних матеріалів, відео- та аудіозаписів, а також програмного забезпечення. Archive.org автоматично створює резервні копії веб-сайтів і зберігає їх у своєму архіві, що дозволяє користувачам відновлювати інформацію, яка була видалена або змінена на оригінальних ресурсах.

Сервіс підтримує широкий спектр медіа-форматів і надає доступ до величезної кількості інформації. Це корисно не тільки для осіб, які шукають видалені веб-сторінки, але й для дослідників, які хочуть переглядати історію розвитку веб-контенту або перевіряти зміни на сайтах з часом. Archive.org забезпечує довгострокове архівування даних і надає безкоштовний доступ до своїх ресурсів для всіх користувачів, що робить його важливим інструментом для збору та аналізу інформації.

Однією з головних переваг Google є її здатність виконувати масштабний та всебічний пошук. Завдяки індексації мільярдів веб-сторінок, Google надає доступ до великого обсягу даних із різноманітних джерел, забезпечуючи можливість глибокого аналізу доступної інформації.

Додаткові сервіси Google, такі як Google Maps, Google Images, Google News тощо, можуть стати важливими інструментами в OSINT-дослідженнях. Вони надають географічні дані, зображення, актуальні новини та інші відомості для аналізу. Крім того, Google дозволяє знаходити інформацію у соціальних мережах, які є цінним джерелом публічних даних для OSINT. Результати пошуку можуть включати профілі користувачів, публікації, коментарі, фотографії, що дає можливість виявляти зв’язки між особами та формувати повну картину подій чи діяльності.

Інструменти моніторингу, такі як Google Alerts, дозволяють автоматично отримувати сповіщення про нові результати пошуку або зміни за заданими ключовими словами. Це сприяє постійному оновленню інформації щодо обраних тем. Додаткові інструменти, як Google Trends, Google Public Data Explorer та Google Scholar, забезпечують можливості візуалізації даних, аналізу популярності запитів і пошуку наукових публікацій. Загалом Google є надзвичайно ефективним інструментом для збору та аналізу відкритої інформації, надаючи широкі можливості для OSINT-розвідки.

Ще одним ефективним інструментом для пасивного збору інформації є сервіс «Have I Been Pwned?». Цей ресурс дозволяє перевіряти, чи були скомпрометовані облікові дані певної електронної пошти. Сервіс архівує і використовує численні відомі витоки баз даних, що дозволяє перевіряти, чи потрапила введена електронна адреса до списку постраждалих у цих витоках.

Витоки даних, які фіксує «Have I Been Pwned?», походять з різних джерел і містять різноманітні набори даних: адреси електронної пошти, паролі, імена користувачів, хеші паролів, платіжні дані, номери телефонів, фізичні адреси та іншу інформацію. Серед найбільших витоків даних, включених до бази сервісу, можна відзначити:

- Collection #1 (772,904,991 записів): один з найбільших витоків даних, що містить величезну кількість записів електронних адрес і паролів;

- Verifications.io (763,117,241 записів): витік, який охоплює велику кількість електронних адрес і супутніх даних;

- Onliner Spambot (711,477,622 записів): значний набір даних, що включає електронні адреси, паролі та інші чутливі дані.

Крім того, сервіс включає витоки даних з популярних платформ, таких як Facebook, LinkedIn, Adobe, VK, Dropbox та інших. Це дозволяє користувачам перевіряти, чи їхні облікові дані потрапили до зламаних баз даних, що може бути важливим для запобігання подальшим атакам або зловживанням [43].

В розслідуваннях кіберінцидентів «Have I Been Pwned?» може бути корисним для виявлення скомпрометованих облікових записів, що допомагає

дослідникам зрозуміти обсяг потенційного впливу інциденту. Перевірка наявності уражених облікових даних може допомогти в ідентифікації скомпрометованих систем або користувачів, а також у виявленні потенційних вразливостей. Виявлення витоків даних допомагає визначити, які особисті дані були скомпрометовані, що в свою чергу дозволяє розробити ефективні стратегії для захисту та відновлення інформації.

2.3 OSINT як метод попередження кіберзагроз

OSINT (Open Source Intelligence) є важливим методом попередження кіберзагроз завдяки своїй здатності виявляти потенційні загрози на ранніх стадіях. Використання OSINT дозволяє організаціям і фахівцям з кібербезпеки ефективно збирати, аналізувати та інтерпретувати дані з відкритих джерел, що допомагає вчасно вжити заходів для захисту інформаційних систем.

Фахівці з безпеки активно використовують OSINT для швидкого пошуку загальнодоступної інформації про внутрішню діяльність фізичних осіб або компаній, а також про їхню взаємодію із зовнішнім середовищем. Часто конфіденційні дані виявляються в метаданих, які фізичні чи юридичні особи випадково публікують. До таких даних можуть належати незахищені з'єднання, відкриті порти пристроїв, застаріле програмне забезпечення, назви пристроїв, версії ПЗ, інформація про мережі та IP-адреси, а також витоки, наприклад, власний код, опублікований на GitHub.

Більшість кіберзагроз починається з точок входу до корпоративної мережі, які включають інформаційні системи на периметрі, доступні з інтернету (сервери, робочі станції, адміністративні панелі спеціалізованого обладнання), мобільні пристрої, що використовуються співробітниками як у межах периметра, так і за його межами, а також облікові записи в хмарних сервісах. Останній пункт часто вимагає інтерактиву з жертвою, наприклад, під

час фішингових атак, що підвищує ризик виявлення. Однак у деяких випадках перевага надається вразливим точкам входу, розташованим на периметрі.

Мережевий периметр, з розвитком технологій і впровадженням хмарних рішень, поступово зникає. Модель Bring Your Own Device (BYOD) дозволяє співробітникам використовувати особисті пристрої для бізнес-процесів, що розмиває периметр і ускладнює контроль потоків даних між корпоративною мережею та зовнішнім світом. Це збільшує різноманітність варіантів проникнення для зловмисників.

Соціальні мережі та веб-сайти є цінними джерелами інформації, особливо щодо співробітників компанії. Постачальники та партнери часто ненавмисно відкривають доступ до деталей IT-інфраструктури компанії, які варто було б залишити конфіденційними. Також існує безліч неіндексованих файлів і веб-ресурсів, що належать до "глибокої мережі" (deep web) і залишаються технічно доступними для публічного доступу.

Таким чином, методи OSINT можуть бути використані для попередження кіберзагроз у відповідь на кіберінциденти. Завчасно проведена розвідка відкритих джерел інформації про підприємство дозволяє запобігти витоку даних або повноцінній кібератаці. Аналізуючи інформацію з точки зору хакера, можна виявити, яка інформація знаходиться у відкритому доступі, що допомагає захистити компанію від можливих загроз.

OSINT є відносно недорогим методом захисту, що вимагає мінімальних затрат, але може запобігти значним матеріальним втратам, захищаючи конфіденційну інформацію та бюджет організації. Використання OSINT як превентивного заходу дозволяє значно знизити ризик успішної атаки на організацію.

2.4 Використання OSINT на початкових етапах розслідування кіберінцидентів

Сьогодні часто трапляються випадки несанкціонованого доступу до систем, крадіжки інформації та інших порушень через комп'ютерні мережі. Тому важливо чітко визначити, що таке кіберінцидент (Cyber incident).

Законом України «Про основні засади кібербезпеки України» (№ 2163-VIII, прийнятий 5 жовтня 2017 року) кіберінцидент визначається як інцидент кібербезпеки (далі - кіберінцидент) - подія або ряд несприятливих подій ненавмисного характеру (природного, технічного, технологічного, помилкового, у тому числі внаслідок дії людського фактора) та/або таких, що мають ознаки можливої (потенційної) кібератаки, які становлять загрозу безпеці систем електронних комунікацій, систем управління технологічними процесами, створюють імовірність порушення штатного режиму функціонування таких систем (у тому числі зриву та/або блокування роботи системи, та/або несанкціонованого управління її ресурсами), ставлять під загрозу безпеку (захищеність) електронних інформаційних ресурсів [45].

На засіданні Національного координаційного центру кібербезпеки при Раді національної безпеки і оборони України (Протокол № 18 від 25.10.2021, № 16/320/21дск від 28.10.2021) було затверджено перелік категорій кіберінцидентів (далі – Перелік). Цей документ розроблено з урахуванням рекомендацій Європейської агенції з кібербезпеки (ENISA Reference Incident Classification Taxonomy, січень 2018 року), а також на основі спільного документа ENISA та Європейського центру боротьби з кіберзлочинністю Європолу (Common Taxonomy for Law Enforcement and The National Network of CSIRTs). [46].

У Конвенції Ради Європи про кіберзлочинність [47], прийнятій у Будапешті 23 листопада 2001 року (до якої Україна приєдналася шляхом ратифікації 7 вересня 2005 року), наведено класифікацію діянь, за які

пропонується встановити кримінальну відповідальність на національному рівні. Класифікація кіберзлочинів у Конвенції базується на об'єкті, проти якого спрямоване правопорушення, зокрема це комп'ютерні дані та системи, або на використанні комп'ютерних систем у механізмі вчинення злочину [49].

Згідно з Конвенцією, до кіберзлочинів віднесено такі групи посягань:

1) правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних та систем.

Ця група охоплює злочини, які спрямовані на підрив або порушення безпеки комп'ютерних систем та інформації, що зберігається, обробляється або передається за їх допомогою. До цієї групи входять такі правопорушення:

- незаконний доступ (hacking): несанкціоноване проникнення в комп'ютерні системи, мережі або програми з метою отримання доступу до інформації чи ресурсів

- нелегальне перехоплення: перехоплення даних, які передаються через комп'ютерні мережі або системи, включаючи електронну пошту та інші форми електронного зв'язку, без дозволу власника інформації;

- втручання в дані: навмисна зміна, знищення, пошкодження або погіршення якості комп'ютерних даних, що впливає на їхню цілісність та достовірність;

- втручання в роботу системи: дії, що спрямовані на порушення роботи комп'ютерних систем, у тому числі через віруси, трояни або інші шкідливі програми, які зупиняють або сповільнюють роботу системи.

2) правопорушення, пов'язані з використанням комп'ютерів.

Сюди входять злочини, такі як комп'ютерне підроблення або шахрайство, де комп'ютер використовується для вчинення протиправних дій, що мають економічний чи інший мотив:

- комп'ютерне підроблення: створення або зміна комп'ютерних даних з метою введення в оману інших осіб, що може бути використано, наприклад, для шахрайства або інтернет-шахрайства;

- комп'ютерне шахрайство: використання комп'ютерних систем або мереж для обману з метою отримання фінансової вигоди або майнової переваги, наприклад, шляхом фальсифікації електронних підписів або документів.

3) правопорушення, пов'язані зі змістом.

Ця категорія включає злочини, пов'язані з розповсюдженням забороненого або доступом до незаконного або забороненого контенту через комп'ютерні системи та мережі:

- дитяча порнографія. Створення, зберігання, розповсюдження або демонстрація матеріалів, що зображають сексуальне насильство над дітьми, через інтернет або інші цифрові канали;

- расизм і ксенофобія. Використання комп'ютерних систем для поширення матеріалів, які пропагують ненависть або насильство на основі раси, національності, етнічної приналежності або релігії.

4) правопорушення, пов'язані з порушенням авторських і суміжних прав. Ця група стосується злочинів, де комп'ютерні системи використовуються для порушення авторських прав та прав, що охороняються відповідно до законодавства про інтелектуальну власність:

- порушення авторських прав. Незаконне розповсюдження, копіювання або використання матеріалів, захищених авторськими правами, таких як музика, фільми, програмне забезпечення, без дозволу власника прав;

- порушення суміжних прав. Незаконне використання записів виконання, звукових записів, радіо- і телепередач або інших матеріалів, які охороняються суміжними правами.

Перша група кіберзлочинів виділяється за об'єктом, на який спрямовані дії злочинця, тоді як інші три групи визначаються тим, що винуваті застосовують комп'ютерні системи у процесі вчинення злочину.

Згідно зі Статистичним звітом Державного центру кіберзахисту (рис. 2.15), за підсумками роботи Системи виявлення вразливостей і

Рисунок 2.15 - Статистика виявлення вразливостей і реагування на кіберінциденти та кібератаки в 2023 році [48]

реагування на кіберінциденти та кібератаки у 2023 році було оброблено близько 18 мільярдів подій. Ці події були отримані за допомогою засобів моніторингу, аналізу та передачі телеметричної інформації про кіберінциденти та кібератаки. У ході первинного аналізу було зафіксовано 133 мільйони підозрілих подій інформаційної безпеки, з яких 148 тисяч були класифіковані як критичні події (потенційні кіберінциденти), визначені шляхом фільтрації підозрілих подій і проведення вторинного аналізу [48].

Також, відповідно до цього звіту за 2023 рік (рис. 2.16) згідно переліку категорій кіберінцедентів схваленого Національним координаційним центром кібербезпеки при Раді національної безпеки та оборони України найпоширеніші інциденти це шкідливий програмний код та збір інформації зловмисником, безпосередньо аналітиками безпеки було зафіксовано та оброблено 1105 кіберінцидентів, що на 62,5% більше, ніж за результатами 2022 року. Найпоширеніші інциденти подій ІБ (більше 100 000 подій):

- 02.04 Шкідливе підключення;
- 03.01 Сканування;
- 02.02 Розповсюдження ШПЗ;
- 08.01 Шахрайський сайт;

- 05.02 Компрометація системи;
- 09.02 Некоректна конфігурація;
- 04.01 Спроба експлуатації вразливості;
- 03.03 Фішинг;
- 02.03 Командно-контрольний центр;
- 06.03 Збій.

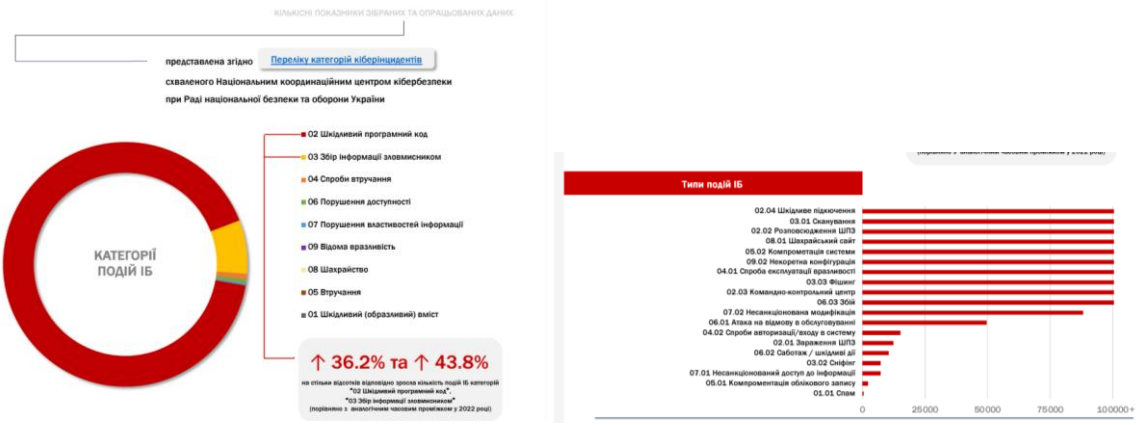


Рисунок 2.16 - Статистика подій ІБ за 2023 рік [48]

Законодавство України визначає кібератаки як навмисні дії в кіберпросторі, що здійснюються за допомогою електронних комунікаційних засобів (зокрема, інформаційно-комунікаційних технологій, програмного забезпечення, програмно-апаратних засобів, інших технічних і технологічних пристроїв) і спрямовані на досягнення однієї чи кількох з наступних цілей: порушення конфіденційності, цілісності або доступності електронних інформаційних ресурсів, що обробляються, передаються чи зберігаються в комунікаційних або технологічних системах; здобуття несанкціонованого доступу до цих ресурсів; порушення безпеки, стабільності та нормальної роботи комунікаційних чи технологічних систем; використання цих систем, їхніх ресурсів та засобів електронних комунікацій для атак на інші об’єкти кіберзахисту [45].

Зовнішній кіберінцидент — це інцидент, пов'язаний з кіберзагрозами, які виникають внаслідок дій зловмисників, що діють з-за меж організації. Такі

інциденти зазвичай пов'язані з атакуючими, які діють ззовні організації, як правило, через Інтернет або інші зовнішні мережі. Це можуть бути фішингові атаки, коли співробітникам надсилають електронні листи з метою отримати доступ до їхніх облікових записів; DDoS-атаки, коли зловмисники перевантажують сервери організації, що призводить до відмови в обслуговуванні; спроби злому або інші способи несанкціонованого доступу до систем. У законодавстві України поняття зовнішнього кіберінциденту не визначено як окрема категорія, але може бути охарактеризований як будь-який кіберінцидент, спричинений діями зловмисників з-за меж організації, що впливає на інформаційні системи, мережі або дані. Основні документи, що регулюють кібербезпеку та кіберінциденти в Україні:

- Закон України "Про основні засади забезпечення кібербезпеки України" від 05.10.2017 № 2163-VIII. У ньому визначаються загальні принципи забезпечення кібербезпеки, зокрема у випадках кіберінцидентів, які можуть включати як внутрішні, так і зовнішні загрози;

- Постанова Кабінету Міністрів України від 23.12.2020 № 1295 "Деякі питання забезпечення функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки" [50]. Ця постанова визначає порядок функціонування системи виявлення та реагування на кіберінциденти, які можуть мати зовнішнє джерело;

- Наказ Адміністрації Держспецзв’язку від 03.07.2023 № 570 "Про затвердження Методичних рекомендацій щодо реагування суб’єктами забезпечення кібербезпеки на різні види подій у кіберпросторі"[51]. Він включає методичні рекомендації щодо реагування на кіберінциденти, враховуючи різні типи загроз, зокрема і зовнішні.

У випадку зовнішніх кіберзагроз відповідні органи, як-от Національний координаційний центр кібербезпеки, можуть здійснювати моніторинг, аналіз та реагування для запобігання або мінімізації впливу таких інцидентів.

Останніми роками кібератаки зазнали суттєвих змін, які стосуються не лише їхніх об’єктів та суб’єктів, але й цілей та завдань. Від простих атак на

конкурентів до масштабних міжнародних конфліктів у кіберпросторі, ці зміни ставлять серйозні виклики перед військовим та політичним керівництвом провідних країн. Ефективність реагування на ці виклики визначатиме майбутні перспективи світової спільноти.

З огляду на нові загрози в кіберпросторі, необхідно проводити ретельний аналіз останніх кіберінцидентів для розробки єдиної стратегії контрзаходів. Хоча універсального підходу до розслідування кіберінцидентів не існує, є кілька основних етапів, яких слід дотримуватися. Це включає збір інформації про інцидент, її перетворення у формат, придатний для аналізу, зіставлення отриманих даних із відомими фактами, а також збагачення інформації новими знахідками з IT-інфраструктури та відкритих джерел. Процес є ітеративним і триває доти, доки не буде проведено всебічний аналіз усіх зібраних даних.

Збір даних відбувається з різних джерел, таких як жорсткі диски, оперативна пам'ять та мережевий трафік. Важливо зібрати структуровану інформацію, що формується програмними засобами, такими як компоненти операційної системи, системні додатки, спеціалізоване ПЗ та засоби захисту. Перетворення інформації може здійснюватися як із використанням загальнодоступних інструментів, так і внутрішніх розробок.

Якщо мета – з'ясувати причини конкретного інциденту, важливо детально дослідити компанію, ознайомитися з її керівництвом, співробітниками та зібрати всі можливі дані. Часто свідчення можуть бути суперечливими або неточними, що ускладнює розслідування.

Наступні етапи включають аналіз зібраних даних, образів систем і лог-файлів. З великого масиву інформації необхідно виділити ключові дані, розсортувати їх за часом, провести статистичний аналіз і відновити хронологію подій – від моменту проникнення в інфраструктуру до витоку даних або інших дій, що загрожують цілісності, конфіденційності чи доступності інформації.

Зазвичай ці дії потребують прямого втручання в систему чи інфраструктуру компанії, що потребує значних ресурсів і часу. Для

оперативного розслідування кіберінцидентів доцільно використовувати методи OSINT (Open Source Intelligence) поряд із традиційними методами. Включення OSINT у комплексне розслідування дозволяє досягти кращих результатів і підвищити ефективність процесу.

При цьому важливо враховувати нормативно-правову базу України, що регулює реагування на кіберінциденти та кібератаки. На сайті Державної служби спеціального зв'язку та захисту інформації України розміщені документи Реагування на кіберінциденти/кібератаки [52]:

- Постанова Кабінету Міністрів України від 23.12.2020 № 1295 "Деякі питання забезпечення функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки"[50]. Ця постанова встановлює основи для створення і функціонування системи виявлення вразливостей та реагування на кіберінциденти і кібератаки в Україні. Вона регулює організацію роботи цієї системи, визначає її функціональні можливості, і забезпечує належний рівень захисту інформаційних систем. Постанова також може охоплювати питання про підключення та взаємодію з іншими національними та міжнародними системами кібербезпеки.

- Наказ Адміністрації Держспецзв’язку від 24.06.2022 № 284 "Про затвердження Порядку передачі комплектів обладнання підсистеми збору телеметрії інформаційно-комунікаційних систем (активні сенсори) системи виявлення вразливостей і реагування на кіберінциденти та кібератаки до об’єктів кіберзахисту" [53]. Наказ визначає порядок передачі комплектів обладнання, які є частиною підсистеми збору телеметрії для системи виявлення вразливостей і реагування на кіберінциденти. Це обладнання, відоме як активні сенсори, використовується для моніторингу та збору даних з інформаційно-комунікаційних систем. Наказ регулює технічні та організаційні аспекти передачі цього обладнання до об’єктів кіберзахисту, що сприяє підвищенню ефективності виявлення та реагування на кіберзагрози.

- Постанова Кабінету Міністрів України від 04.04.2023 № 299 "Деякі питання реагування суб’єктами забезпечення кібербезпеки на різні види подій

у кіберпросторі" [54]. Постанова регулює порядок реагування на різні види подій у кіберпросторі, які можуть впливати на безпеку інформаційних систем. Вона визначає обов'язки суб'єктів забезпечення кібербезпеки, процедури реагування та координації між різними організаціями. Мета постанови – забезпечити швидке та ефективне реагування на кіберінциденти, що можуть загрожувати національній кібербезпеці.

- Наказ Адміністрації Держспецзв'язку від 03.07.2023 № 570 "Про затвердження Методичних рекомендацій щодо реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі" [51]. Цей наказ затверджує методичні рекомендації для суб'єктів забезпечення кібербезпеки щодо реагування на різні події у кіберпросторі. Методичні рекомендації включають детальні інструкції та практичні поради для управління та реагування на кіберінциденти. Наказ має на меті забезпечити стандартизований підхід до реагування, полегшити інтеграцію та координацію між різними кібербезпековими структурами, а також підвищити загальну ефективність боротьби з кіберзагрозами.

2.5 Висновки до розділу 2

У розділі було розглянуто ключові аспекти застосування відкритої розвідки для протидії кіберзагрозам і проведення розслідувань.

По-перше, було досліджено роль OSINT на різних етапах життєвого циклу кібератаки. Зростання кількості кіберінцидентів і доступність інструментів, таких як Ransomware-as-a-Service, підвищують ризики для організацій. Розуміння, як відкриті дані можуть бути використані як нападниками, так і захисниками, дозволяє ефективніше протидіяти загрозам і запобігати кібератакам. Тому OSINT є не лише ефективним засобом для

попередження атак, але й важливим інструментом у розслідуванні кіберінцидентів, що допомагає виявляти вразливості та джерела атак..

По-друге, було розглянуто основні методи та інструменти для збору інформації в межах OSINT. Такі інструменти, як Shodan, Recon-ng, TIDoS, Maltego, theHarvester, Metagoofil, SpiderFoot, OSINT Framework і Cobwebs, дозволяють фахівцям збирати критичні дані про інфраструктуру та потенційні вразливості. Особливу увагу приділено пошуковим сервісам (Google, Yahoo) та методам, зокрема Google Dorking, що допомагають знаходити специфічну інформацію в мережі. Окрім того, було розглянуто два основні типи здобування інформації: пасивний і активний, із зазначенням їх відмінностей та відповідних ризиків і переваг. Використання цих методів дозволяє ідентифікувати потенційні ризики ще до того, як вони призведуть до інцидентів, що надає компаніям можливість заздалегідь підготуватися до атак.

Було встановлено, що використання OSINT є важливим методом попередження кіберзагроз, що допомагає не лише виявляти потенційні атаки, але й запобігати витоку інформації. Розвідка з відкритих джерел дозволяє оцінити, яку інформацію про організацію можна знайти у відкритому доступі, і вчасно вжити заходів для її захисту.

Було розкрито важливість OSINT на початкових етапах розслідування кіберінцидентів. Відкриті джерела інформації допомагають виявляти початкові вектори атак, встановлювати потенційних учасників та з'ясовувати обставини інциденту.

Також зазначено, що проведення OSINT не є затратною процедурою, що робить її доступною як для малих, так і для великих компаній. Використання безкоштовних інструментів OSINT додатково сприяє зниженню витрат на безпеку.

Загалом, OSINT є потужним інструментом для виявлення, запобігання та розслідування кіберзлочинів завдяки своїй доступності та широкому спектру методів і інструментів для збору інформації.

3 ЕФЕКТИВНЕ РОЗСЛІДУВАННЯ КІБЕРІНЦИДЕНТІВ ЗА ДОПОМОГОЮ МЕТОДІВ OSINT: ПРАКТИЧНІ ІНСТРУМЕНТИ

3.1 Використання методів OSINT у розслідуванні кіберінцидентів

Безсумнівно, OSINT — це технологія, яка має значний потенціал і сьогодні, і в майбутньому. Ті, хто володіє знаннями про її інструменти та принципи роботи, завжди матимуть перевагу у питаннях конкуренції, особистої, корпоративної та національної безпеки. В Україні з 2014 року активно намагаються застосовувати OSINT у військових операціях, однак його повноцінне використання у сфері державного управління та захисту національних інтересів ще перебуває на етапі розвитку та наукових досліджень.

Розслідування кіберінцидентів — це тривалий процес, що вимагає уважного аналізу всіх деталей. Перш за все, необхідно визначити тип інциденту, його тривалість та які дії були здійснені під час події. Лише після отримання цих базових даних можна перейти до глибшого аналізу ситуації й обрати відповідні методи для розслідування. Універсального підходу для вирішення кожного кіберінциденту не існує, проте завжди є ключові моменти, від яких можна відштовхуватися під час роботи.

Одним із основних способів використання OSINT при розслідуванні кіберінцидентів є моніторинг відкритих джерел інформації, таких як соціальні мережі, форуми, блоги та інші онлайн-ресурси, де можуть бути опубліковані важливі дані або згадки про подію. Це дозволяє виявити інформацію про можливі атаки, зловмисників або вразливі місця системи.

Ще один ефективний метод — аналіз індикаторів компрометації (IOC), що можуть бути публічно доступними в базах даних, таких як VirusTotal, Hybrid Analysis та інші ресурси. Ці дані можуть допомогти ідентифікувати зловмисне програмне забезпечення або інші шкідливі активності, що були використані під час атаки.

Також важливу роль відіграє геолокаційний аналіз. OSINT може допомогти визначити місце перебування зловмисників через аналіз публічних зображень, метаданих або інших цифрових слідів, що залишаються під час кіберінцидентів. Зокрема, метадані фотографій або файлів, завантажених зловмисниками, можуть містити GPS-координати, що дають змогу відслідкувати їх місцезнаходження.

Пошук зловмисників через аналіз доменних імен та IP-адрес — ще один практичний метод OSINT, що використовується під час розслідування кіберінцидентів. Завдяки даним про реєстрацію доменів, відкритих баз даних про IP-адреси та історію їх використання можна виявити активність або зв'язки, які можуть допомогти у відстеженні кібератак.

Коли відбувається кіберінцидент або кібератака, завжди залишаються сліди події. Збір початкової інформації про інцидент є фундаментом для подальшого розслідування, де OSINT відіграє важливу роль у пошуку і аналізі цих даних.

3.1.1 Використання методів OSINT для пошуку інформації на основі електронної пошти.

Один із прикладів можна навести на основі ситуації, коли на електронну поштову скриньку надходить лист із вкладеним файлом. Вкладенням може бути архів, що містить шкідливе програмне забезпечення. Після розпакування та запуску такий файл починає збирати визначені дані з комп'ютера і передавати їх на віддалений сервер. Такі інциденти є доволі поширеними на сьогоднішній день. Відправниками можуть бути як недосвідчені зловмисники, що лише тестують свої навички, так і досвідчені хакери, що націлені на компрометацію організації та крадіжку її даних.

Розглянимо приклад коли на електронну поштову скриньку надходять листи із вкладеним файлом. На корпоративну скриньку прийшло 2 листа: один від Чубарь Катерина Олександрівна (fop_chubar@tutamail.com), а другий - Агрокомбінат Радість (gillies@netyp.com) (рис. 3.1).

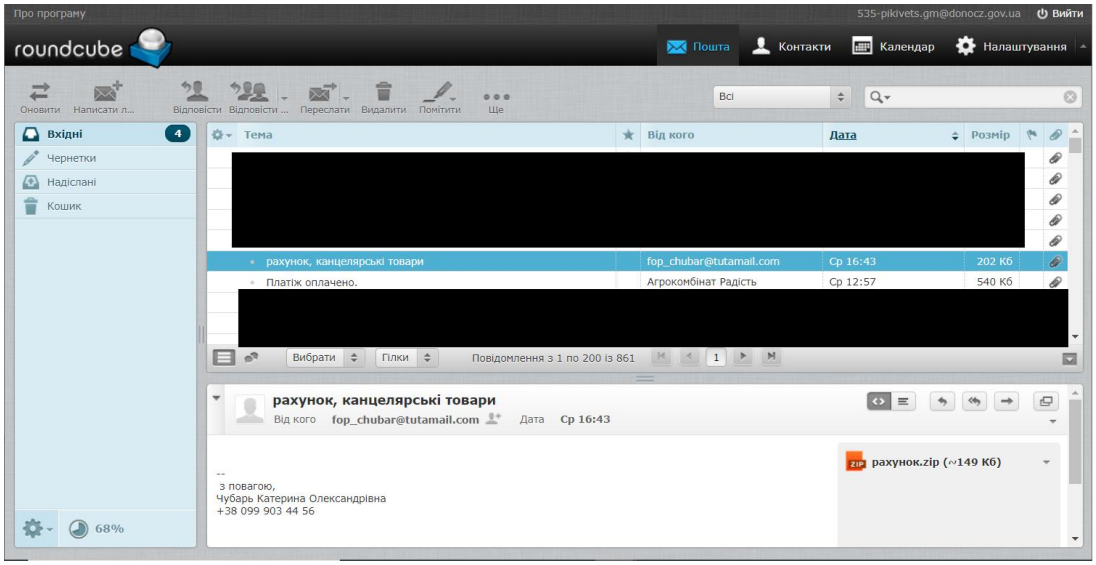


Рисунок 3.1 - Листи із вкладеним файлом

Розглянимо лист від Чубарь Катерина Олександрівна (fop_chubar@tutamail.com). Першим кроком у розслідуванні такого кіберінциденту слід вважати аналіз електронної адреси відправника та його IP-адреси. Скачавши лист на свій персональний комп'ютер і відкривши у текстовому редакторі Notepad++ (рис. 3.2) можна побачити Ip-адресу відправника: 185.205.69.213 та сервер з якого було надіслано лист (mail.w13.tutanota.de). Застосувавши інструмент "whois" через веб-ресурс https://thehost.ua/ua/domains/whois (рис. 3.3) отримали дані реєстру з інформацію про хостинг-провайдера, який надає послуги по цьому Ip-адресу:

organisation: ORG-TG206-RIPE

org-name: Tutao GmbH

country: DE

org-type: LIR

address: Deisterstr. 17a

address: 30449

address: Hannover

address: GERMANY

phone: +49-511-202801-0

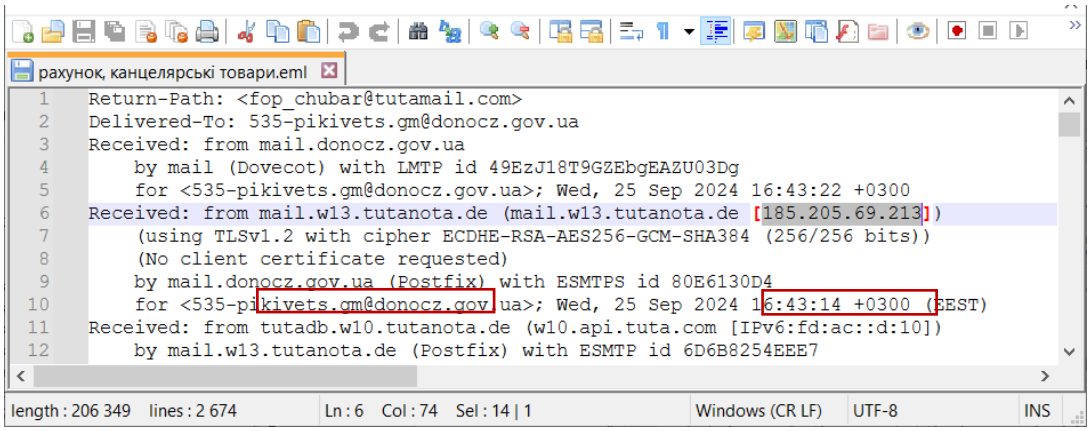


Рисунок 3.2 - Відкритий лист у текстовому редакторі Notepad++

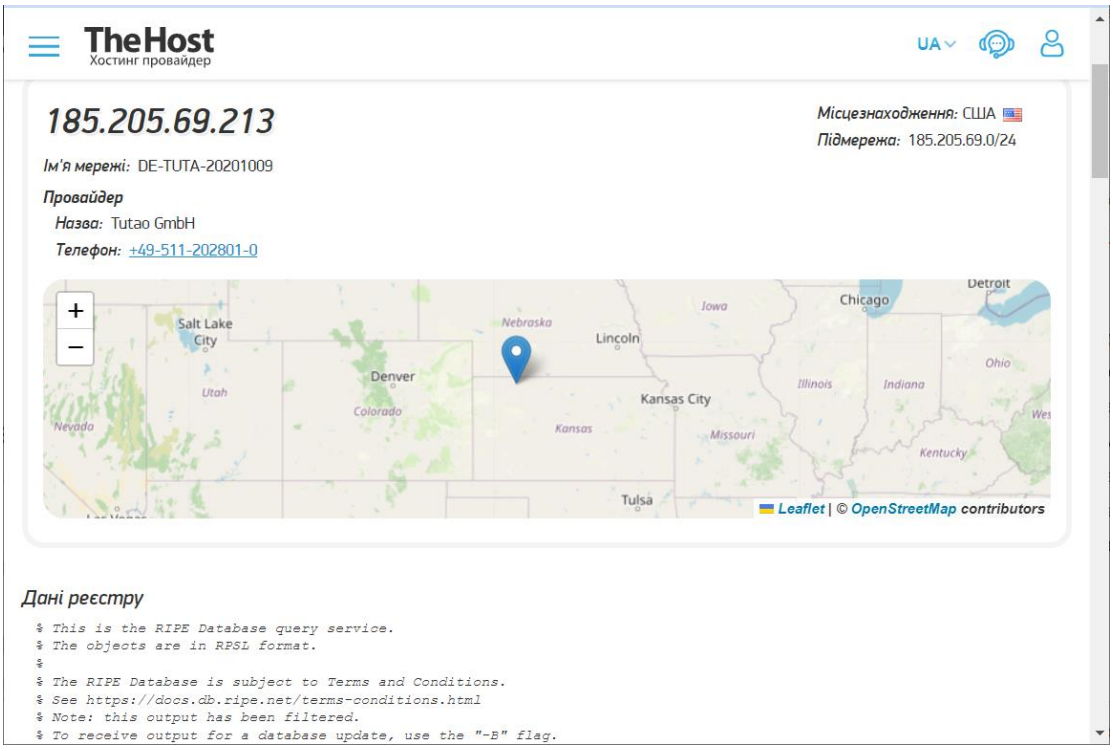


Рисунок 3.3 - Перевірка Whois за Ip185.205.69.213 на сайті TheHost

За допомогою одного з інструментів OSINT Framework - Email Reputation (https://emailrep.io/) можна дізнатися про репутацію поштової скриньки (рис. 3.4).

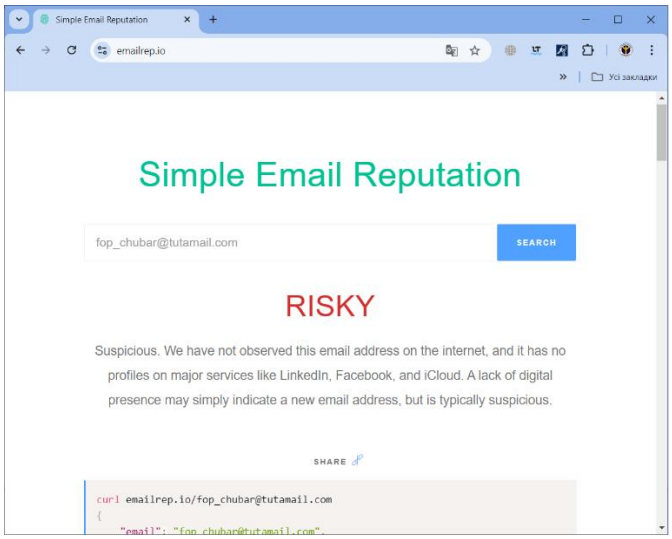


Рисунок 3.4 - Перевірка на репутацію за допомогою Email Reputation

Як бачимо поштова скринька fop_chubar@tutamail.com є підозрілою, тому що її не знайдено в Інтернеті і вона не має профілів у основних службах, таких як LinkedIn, Facebook та iCloud, але це може вказувати на нову адресу електронної пошти. За допомогою сайту https://intelx.io перевіряємо , чи використовувалася ця електронна адреса для реєстрації на вебсайтах або в соціальних мережах, що дозволить отримати додаткові дані про зловмисника. На рис. 3.5 ми бачимо що ця електронна адреса ніде не використовувалася для реєстрації.

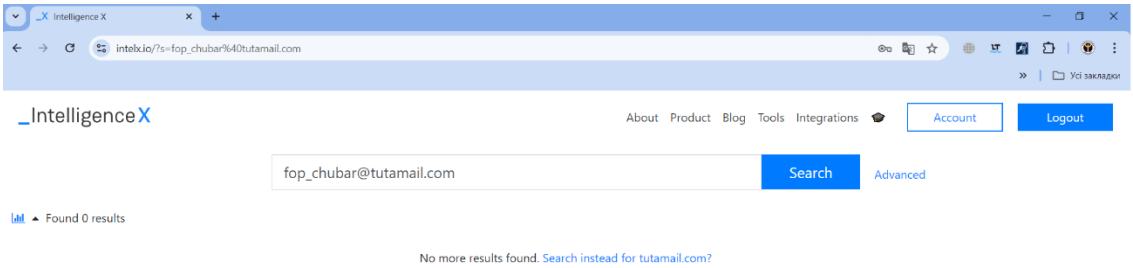


Рисунок 3.5 - Перевірка за допомогою _IntelligenceX

За допомогою сайта міністерства юстиції України можна зробити безкоштовний пошук відомостей по Чубарь Катерина Олександрівна у Єдиному державному реєстрі юридичних осіб, фізичних осіб-підприємців та громадських формувань (далі - ЄДР). Цей пошук здійснюється відповідно до статті 11 Закону України «Про державну реєстрацію юридичних осіб, фізичних осіб-підприємців та громадських формувань». Згідно отриманої інформації ми можемо сказати що є ФОП ЧУБАРЬ КАТЕРИНА ОЛЕКСАНДРІВНА, яка може займатися роздрібною торгівлею газетами та канцелярськими товарами в спеціалізованих магазинах, але її офіційна адреса електронної пошти (isidor_selidovo@ukr.net) відрізняється від той з якої надійшло повідомлення.

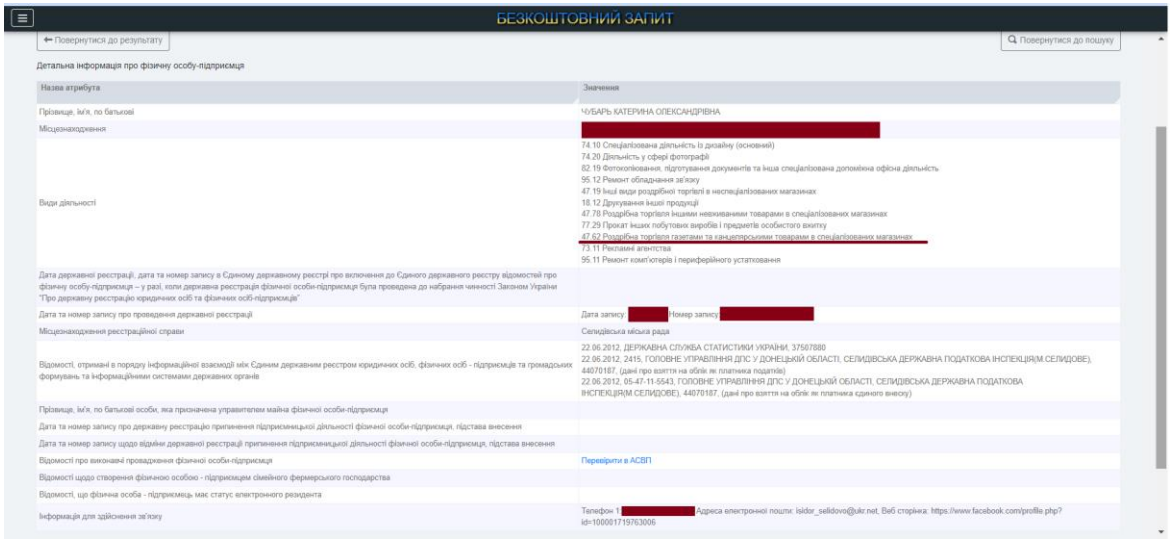


Рисунок 3.6 - Інформація з сайту міністерства юстиції України

Таким чином, використовуючи виключно методи та інструменти OSINT, вдалося визначити, через який сервіс здійснювалася розсилка повідомлень і де зберігаються дані про відправника. Отримана інформація, у разі подальшого звернення до правоохоронних органів, здатна суттєво прискорити розслідування інциденту та забезпечити оперативну реакцію на подібні випадки.

Незважаючи на те, що до повідомлення був прикріплений файл, і його аналіз не було проведено, отримана інформація вже надає базу для подальших досліджень. Однак, без детального аналізу файлу та його функціональних особливостей неможливо скласти повну картину кіберінциденту.

3.1.2 Збір даних, використовуючи адресу криптогаманця

У сучасних умовах, коли криптовалюти стають важливою частиною глобальної економіки, анонімність та децентралізованість блокчейн-технологій викликають інтерес не лише у законного бізнесу, а й у кіберзлочинців. В рамках OSINT-розслідувань, що використовують виключно відкриті джерела інформації, збір даних за адресою криптогаманця стає важливим інструментом для виявлення і аналізу підозрілих фінансових потоків, а також для розслідування кіберзлочинів. Такі дані можуть включати інформацію про транзакції, баланси криптогаманців, зв'язки між гаманцями, а також публічні згадки криптовалютних адрес у форумах, соціальних мережах чи інших онлайн-платформах. Основна мета OSINT-розслідувань полягає у використанні доступних публічних даних для отримання якомога більше інформації без доступу до закритих чи конфіденційних джерел. Технологія блокчейн забезпечує відкритий доступ до перегляду стану гаманця та його транзакцій, знаючи лише його адресу. Дані про власника криптогаманця також можуть бути виявлені за допомогою цих методів OSINT. Одним з інструментів OSINT, що використовується для аналізу криптогаманців і встановлення взаємозв'язків між ними, є Maltego.

Розглянемо збір даних, використовуючи адресу криптогаманця на прикладі фішинг листа, який надійшов до Селидівського міського центру зайнятості (рис. 3.7) з e-mail inlebi@email.changingemail.com. В цьому листі зловмисники стверджують, що володіють компрометуючою інформацією і

погрожують розкрити її, якщо не буде сплачено викуп на криптогаманць: bc1q34vjur6yxxra3mjktr2qu5wrkvelgrw47wf93k.

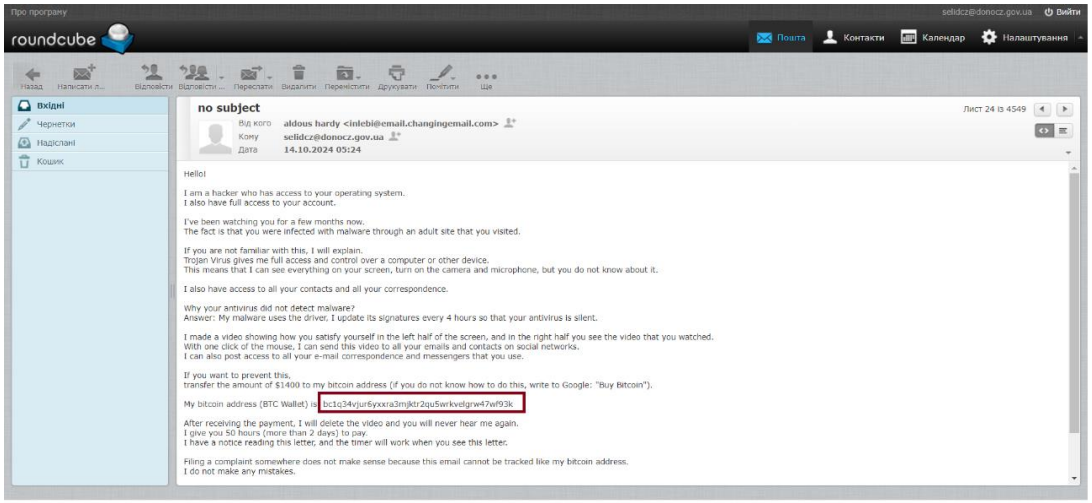


Рисунок 3.6 - Фішинг лист із вимогою викупу

За допомогою інструменту Maltego було побудовано граф, що відображає транзакції, які пройшли через біткоїн-адресу bc1q34vjur6yxxra3mjktr2qu5wrkvelgrw47wf93k (рис. 3.7). Цей граф дозволяє візуалізувати зв'язки між різними адресами, що беруть участь у транзакціях, а також ілюструє шлях руху коштів.

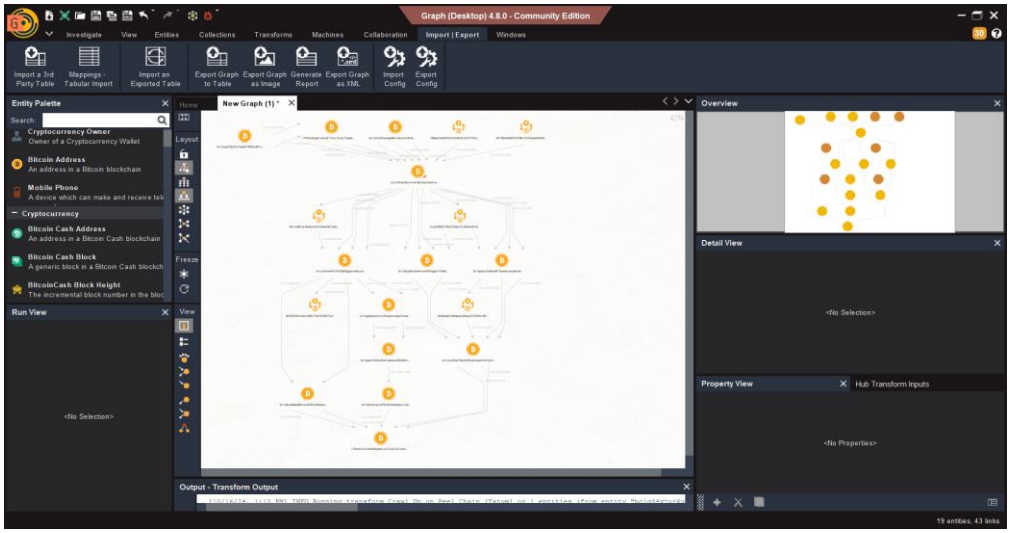


Рисунок 3.7 - Транзакції, які пройшли через біткоїн-адресу

На основі представленого графа можна зробити висновок, що на біткоїн-адресу bc1q34... надійшли певні грошові кошти з адрес 17KNc... та bc1qt... (рис. 3.8). У подальшому всі ці кошти, після проходження через низку проміжних адрес, були перераховані на біткоїн-адресу: 17StnGroPUsNXBq4AVJQ1fqGftoFZh3zva (рис. 3.9).

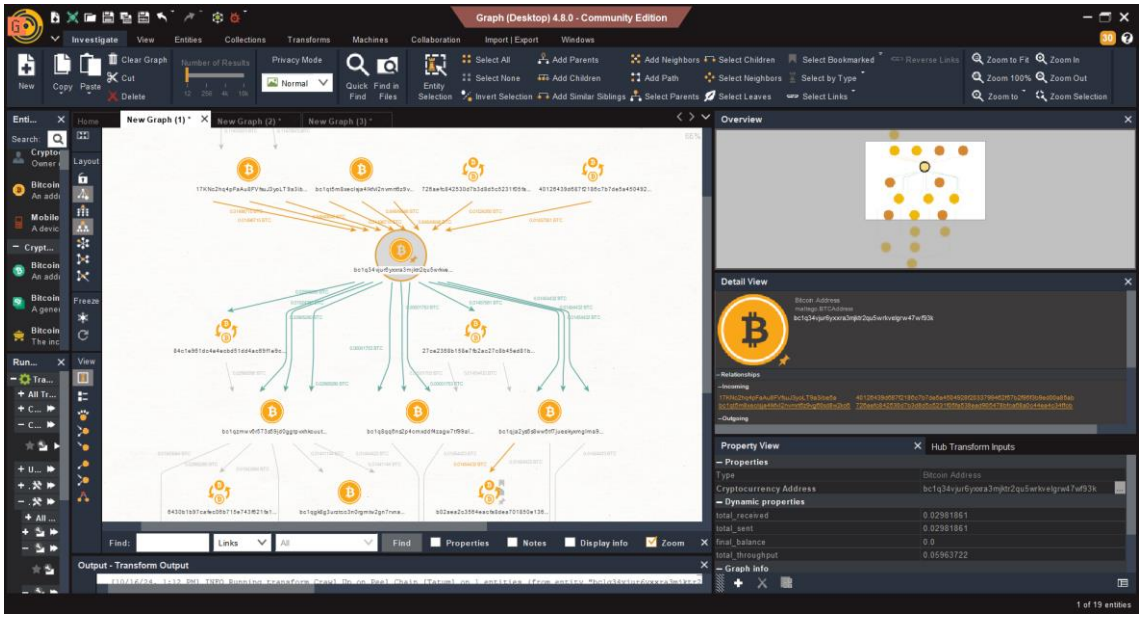


Рисунок 3.8 – Надходження коштів на біткоїн-адресу

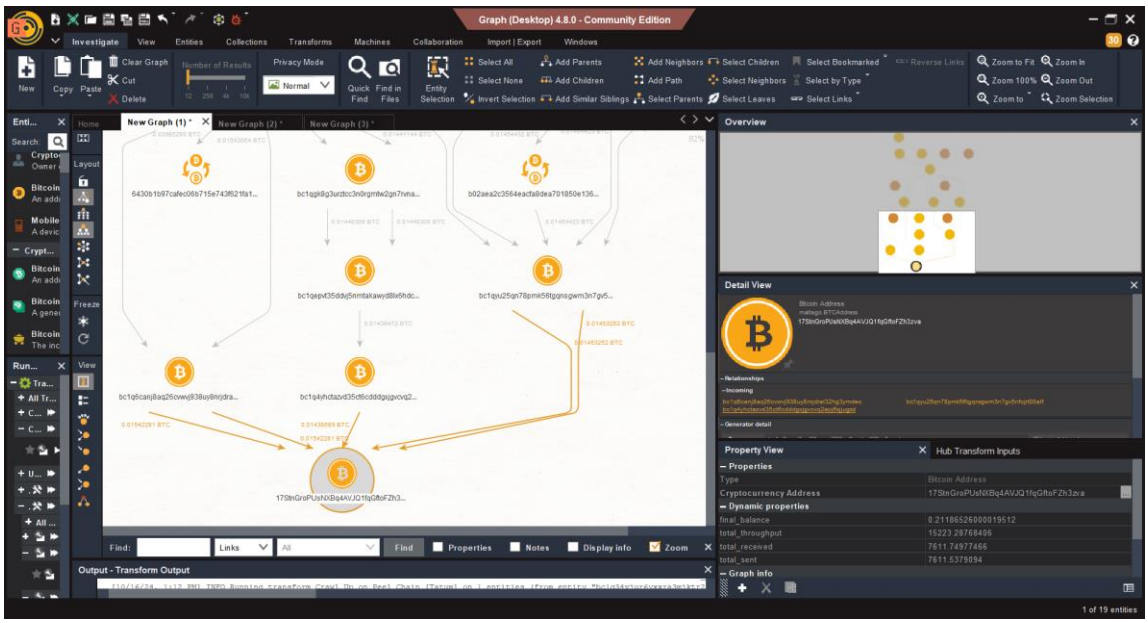


Рисунок 3.9 – Перерахування коштів на другу біткоїн-адресу

За допомогою веб-сайту Glasschain.org можна перевірити біткоїн-адресу на предмет шахрайства та визначити, чи були вже подані звіти щодо даної адреси (рис. 3.10).

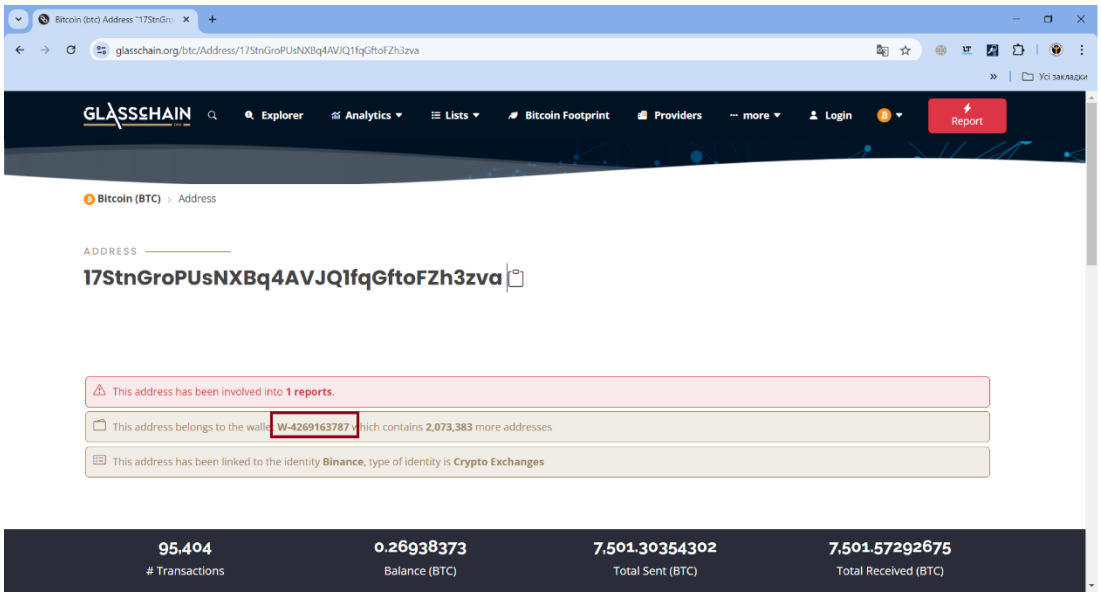


Рисунок 3.10 – Перевірка біткоін-адреси на шахрайство через Glasschain.org

Як видно, ця адреса належить до гаманця W-4269163787, який містить ще 2 074 416 адрес. Якщо перейти до цього гаманця, стане очевидним, що він був залучений у дев'яти звітах про шахрайство. Це свідчить про потенційно небезпечну діяльність, пов'язану з даним гаманцем, що викликає підозру у можливій участі в шахрайських схемах або інших незаконних операціях.

Крім того, можливе проведення пошуку гаманця за допомогою пошукових систем, таких як Google чи Bing. Часто трапляється, що адреса гаманця може бути вказана у реквізитах на різних форумах в Інтернеті, зокрема на тематичних майданчиках або платформах, пов'язаних із криптовалютами чи навіть "хакерських форумах". Пошукові системи здатні індексувати такі сторінки, надаючи доступ до інформації, яка може виявитися корисною для розслідування. Використання операторів розширених пошукових запитів (Google Dorks) дозволяє більш ефективно фільтрувати

інформацію, усуваючи непотрібні або непов'язані результати з пошукової видачі, що значно спрощує процес збору даних.

Існує також низка спеціалізованих веб-ресурсів для пошуку інформації про криптогаманці. Серед найбільш популярних та функціональних платформ можна відзначити такі сервіси, як:

- blockchain.com/explorer – загальний оглядач блокчейну з можливістю перегляду транзакцій у мережі Bitcoin;

- blockchair.com – мультиблокчейн експлорер, що підтримує декілька криптовалютних мереж;

- etherchain.org – платформа для моніторингу мережі Ethereum;

- etherscan.io – один із найпотужніших інструментів для аналізу транзакцій в мережі Ethereum, що дозволяє відстежувати адреси, баланси та історію транзакцій.

Завдяки різноманітності технологій OSINT і їх гнучкості в підходах до збору інформації, можливим є отримання комплексного уявлення про криптовалютну активність. Важливо те, що ці методи можна поєднувати з іншими дослідницькими підходами, такими як аналіз транзакцій, вивчення мережевих взаємозв'язків або використання інструментів для моніторингу блокчейнів. Така комбінація дозволяє отримати більш повну та об'єктивну інформацію про інцидент, що є критичним для ефективного розслідування у сфері криптовалют.

3.1.3 Використання методів OSINT для збору інформації, пов’язаної з URL-адресою

Отримання посилання на фішинговий веб-ресурс може бути охарактеризоване як кіберінцидент, що визначається самою URL-адресою. У даному випадку аналіз зосереджуватиметься на конкретному URL, без

врахування джерела його отримання. Однією з найбільш поширених категорій фішингових посилань в Україні є адреси, що стосуються "фінансової підтримки". У межах нашого дослідження ми будемо розглядати реальне фішингове посилання https://otrymaty-pidtrymku.pages.dev/selectB/?id=93jp1n5 (рис. 3.11), яке використовувалося для збору даних карткових рахунків та для зняття коштів з них.

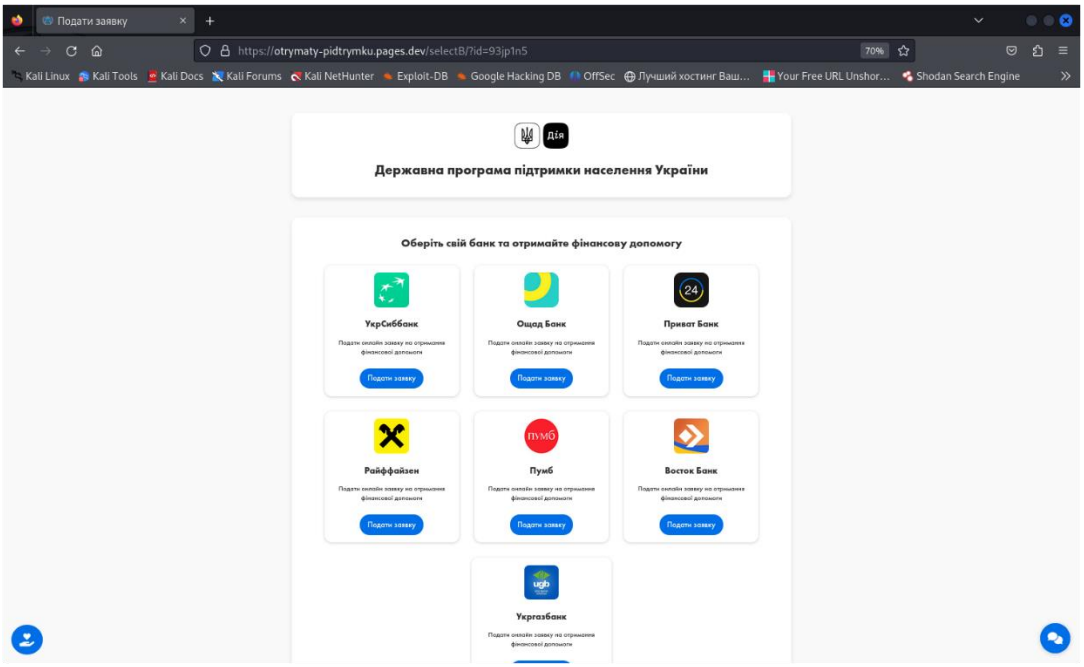


Рисунок 3.11 – Стартова сторінка фішингового веб-ресурсу

Першим кроком є виконання WHOIS-запиту для отримання базової інформації про домен, наприклад, дати його реєстрації та інформації про власника. Застосувавши інструмент "whois" через веб-ресурс https://thehost.ua/ua/domains/whois (рис. 3.12) отримали інформацію про домен:

- статус: активний;
- дата створення: 2020-09-02 02:33:29 UTC;
- дата оновлення: 2023-09-04 18:15:07 UTC;
- дата закінчення: 2026-09-02 02:33:29 UTC;

список неймсерверів (DNS): adi.ns.cloudflare.com, karl.ns.cloudflare.com;

та дані про реєстратора:

- реєстратор: CloudFlare, Inc.;

- контактний email для зв'язку з реєстратором: registrar-abuse@cloudflare.com;

- телефон для скарг на зловживання реєстраторів: +1.4153197517.

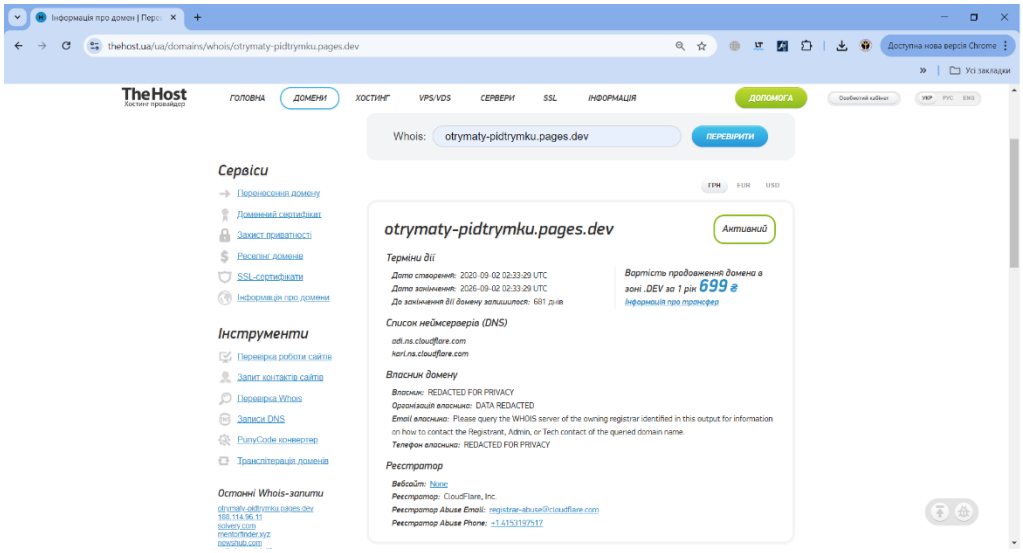


Рисунок 3.12 – WHOIS-запит

Оскільки домен використовує платформу Cloudflare Pages, інформація про реєстрацію не буде доступною через стандартний WHOIS-запит, оскільки Cloudflare забезпечує конфіденційність. Це є типовою практикою для багатьох фішингових ресурсів, оскільки вони намагаються уникнути виявлення та відповідальності. У таких випадках рекомендується звертатися до реєстратора для отримання додаткової інформації або вжиття заходів щодо зупинки шахрайської діяльності.

Для подальшого дослідження фішингового веб-ресурсу https://otrymaty-pidtrymku.pages.dev/selectB/?id=93jp1n5, корисним інструментом є urlscan.io. Цей сервіс дозволяє отримати детальну інформацію про структуру сайту, взаємодії з іншими доменами, ресурси, які сайт завантажує, а також виявити потенційні шкідливі елементи. (рис.3.13). Веб-сайт otrymaty-pidtrymku.pages.dev здійснив зв’язок із 6 різними IP-адресами в 4 країнах через

6 доменів, виконавши 20 HTTP-транзакцій. Основна IP-адреса сайту — 188.114.96.3, зареєстрована в Амстердамі (Нідерланди), та належить інфраструктурі Cloudflare (CLOUDFLARENET), що базується в США. Сертифікат безпеки TLS для цього домену було видано 17 жовтня 2024 року з терміном дії 3 місяці.

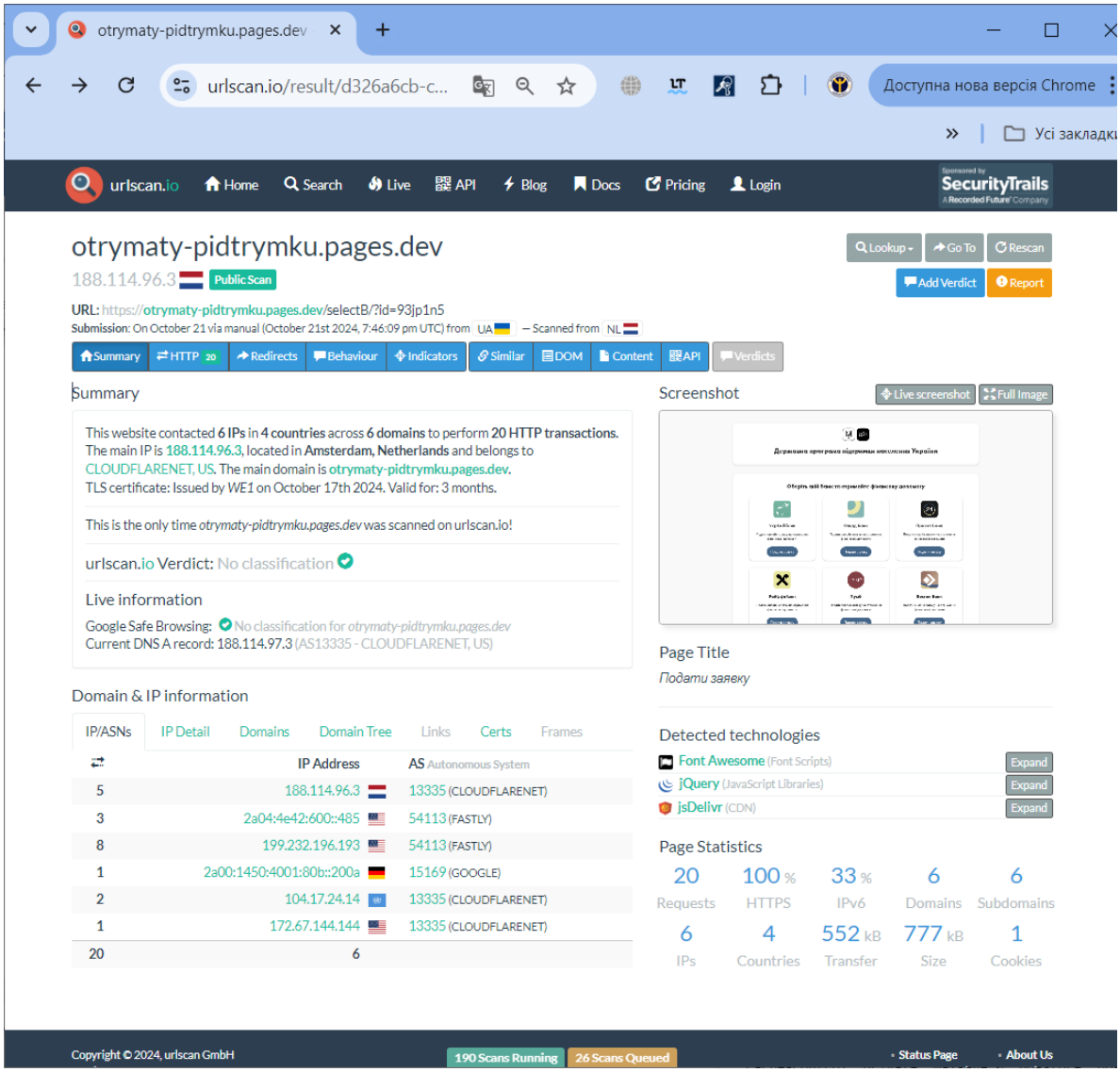


Рисунок 3.13 – Використання urlscan.io

Ресурс демонструє підозрілу активність, оскільки пов’язаний із кількома IP-адресами в різних країнах і взаємодіє з кількома доменами для виконання транзакцій. Це підтверджує його ймовірне використання для збору конфіденційних даних.

Для більш глибокого дослідження проводимо аналіз HTML-коду сторінки https://otrymaty-pidtrymku.pages.dev/selectB/?id=93jp1n5 на наявність форм для збору даних користувачів (рис. 3.14).

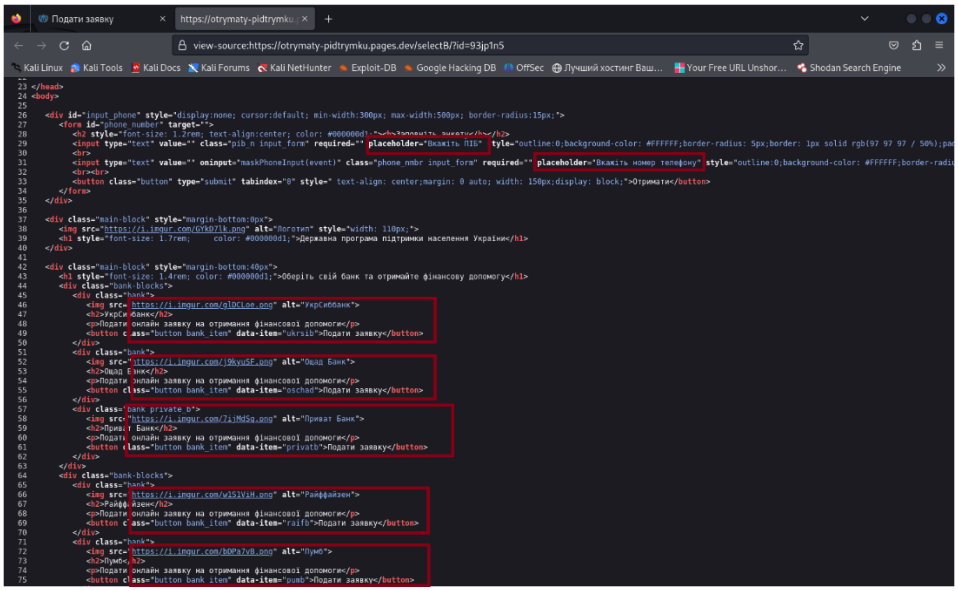


Рисунок 3.14 – HTML-код фішингової сторінки

Веб-сторінка складається з:

- назва сторінки: "Подати заявку";

- мета-теги сторінки вказують на пропозицію подачі заявки для отримання фінансової допомоги від міжнародних організацій з текстом про швидке схвалення заявки протягом 20 хвилин;

- на сторінці є зображення логотипів банків (УкрСиббанк, Ощадбанк, ПриватБанк та ін.), з яких користувач може обирати для подачі заявки на допомогу;

- присутні іконки банків з кнопками для подачі заявок через конкретні банки, а також зображення, що нагадують логотипи для створення довіри;

- основний блок для подачі заявок складається з кнопок "Подати заявку" для різних банків;

- присутні блоки з відгуками, у яких зображені імена користувачів та позитивні відгуки щодо допомоги (рис. 3.15).

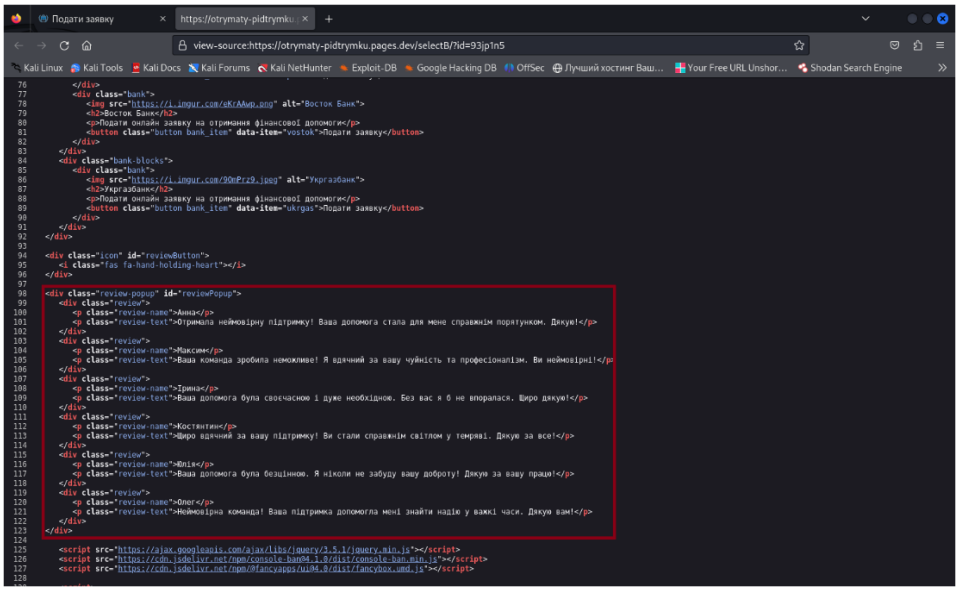


Рисунок 3.15 – Блоки з відгуками

Після натискання на кнопку "Подати заявку" (для прикладу обрали банк Приватбанк) з’являється форма для подачі заявки, яка вимагає введення персональних даних: ПІБ і номер телефону. Після введення цих даних відкривається сторінка "Приєднання картки" https://otrymaty-pidtrymku.pages.dev/privatb/?id=93jp1n5 (рис. 3.16) яка запитує дані банківської картки: номер картки, термін дії, CVV-код, і навіть баланс карти, що є ознаками фішингу.

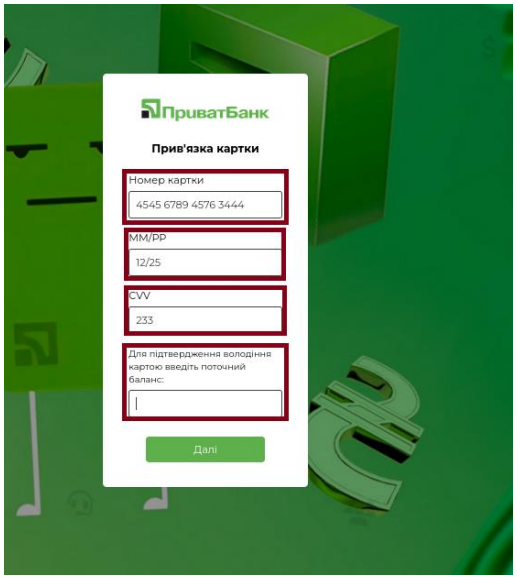


Рисунок 3.16 – Сторінка "Приєднання картки"

Проаналізувавши HTML-код сторінки https://otrymaty-pidtrymku.pages.dev/privatb/?id=93jp1n5 (рис.3.17) було виявлено що сторінка запитує не тільки дані банківської картки: номер картки, термін дії, CVV-код, баланс карти, а ще, для підтвердження, пропонується ввести смс-код, який зазвичай використовується для підтвердження фінансових транзакцій Використовуються відомості про помилки, такі як "неправильний баланс карти" чи "невірний смс-код", щоб повторно змусити користувача вводити свої дані. Також на сторінці використовується відео, яке нібито демонструє підтвердження операцій, що створює враження автентичності. Код скрипту для обробки даних має зашифровані та обфусцировані елементи JavaScript, що зазвичай використовують для приховування дійсного призначення коду від користувачів та захисту від виявлення системами безпеки (рис. 3.18). Скрипти використовуються для отримання та збереження інформації через кукі, такі як ідентифікатор замовлення та інші дані, які можуть бути використані для подальшого обману користувачів.

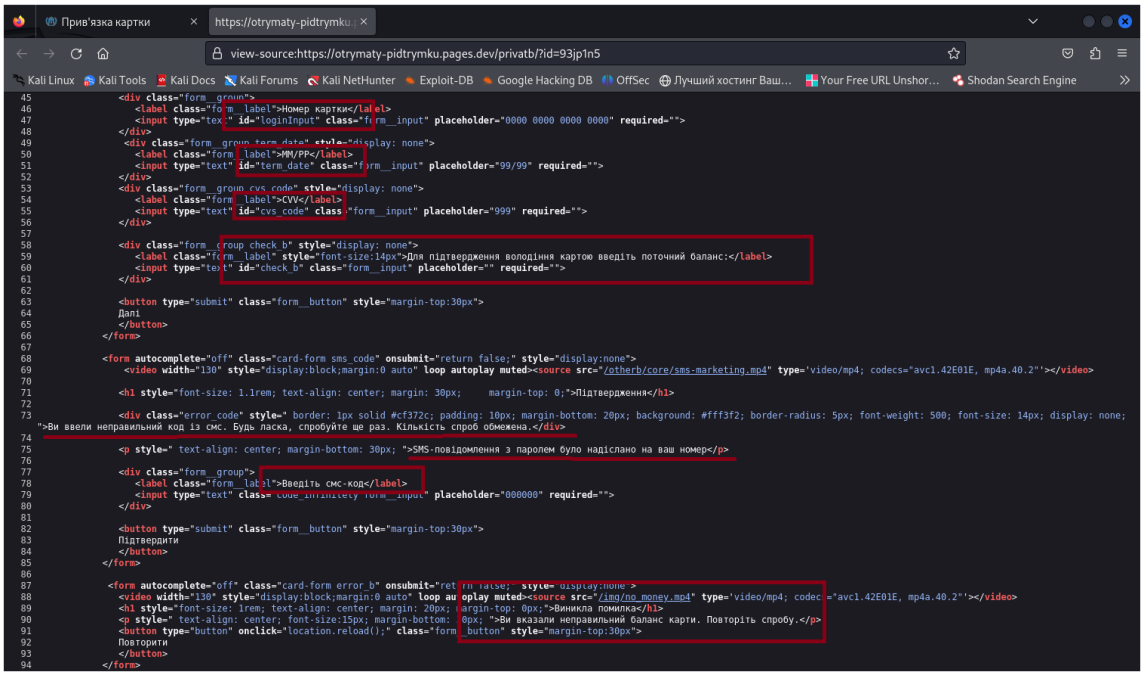


Рисунок 3.17 – HTML-код сторінки з запитами даних

Рисунок 3.18 – Один із скриптів фішингової сторінки

Наступним етапом є перевірка URL-адреси через VirusTotal, щоб визначити, чи була ця адреса відзначена як шкідлива або фішингова іншими користувачами або антивірусними системами (рис.3.19). Веб-сторінка має статус 200, що вказує на її активність і доступність. Вміст сторінки має формат text/html, який є типовим для веб-сторінок. Два постачальники безпеки вказали на потенційну загрозу:

- Seclookup класифікував цей ресурс як зловмисний;

- Trustwave позначив URL як фішинговий, що може свідчити про збір конфіденційної інформації користувачів (зокрема, банківських даних).

На момент аналізу спільнота не додала додаткових відгуків або інформації щодо даного URL-адресу, що може свідчити про обмежене розповсюдження цього фішингового ресурсу.

Використовуємо Google Dorks для пошуку інформації про даний домен та URL на форумах, у блогах чи в інших джерелах.

Використував такі запити як "otrymaty-pidtrymku.pages.dev", "otrymaty-pidtrymku.pages.dev/selectB", "site:pages.dev otrymaty-pidtrymku" виявили що ніяких згадок про сайт або скарг користувачів не було виявлено. Це може вказувати на те, що сайт ще не встиг набрати широкого розголосу або знаходиться на початковій стадії використання у шахрайських цілях.

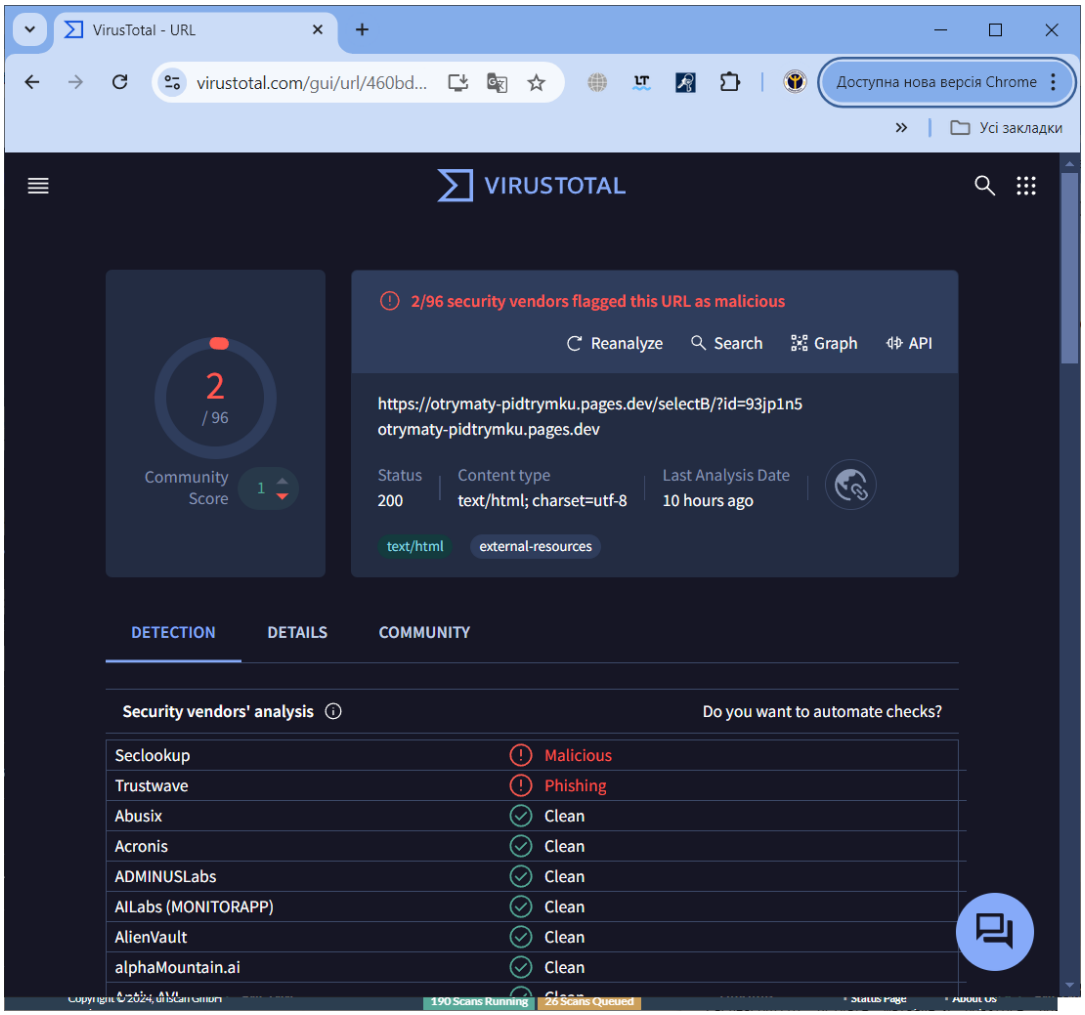


Рисунок 3.19 – Аналіз за допомогою VirusTotal

За допомогою Wayback Machine (archive.org) переглянемо історію змін веб-сайту. це допоможе з'ясувати, чи сайт раніше використовувався з іншою метою, або чи з'являлася на ньому потенційно шкідлива інформація. Wayback Machine не містить історії для цієї конкретної URL-адреси, що свідчить про її відносну новизну або те, що вона не була відзначена для архівування (рис.3.20).

У процесі аналізу фішингового веб-ресурсу https://otrymaty-pidtrymku.pages.dev/selectB/?id=93jp1n5 було виявлено, що цей сайт використовувався для збору конфіденційних даних користувачів, зокрема банківських реквізитів, з можливістю подальшого несанкціонованого доступу до фінансових ресурсів. Результати WHOIS-запиту, проведеного для аналізу домену, свідчать про його реєстрацію через сервіс Cloudflare, який забезпечує

конфіденційність інформації про власника домену. Аналіз за допомогою сервісу urlscan.io підтвердив зв'язок ресурсу з кількома IP-адресами та виявив його підозрілу активність, що пов'язана з потенційно шкідливими елементами.

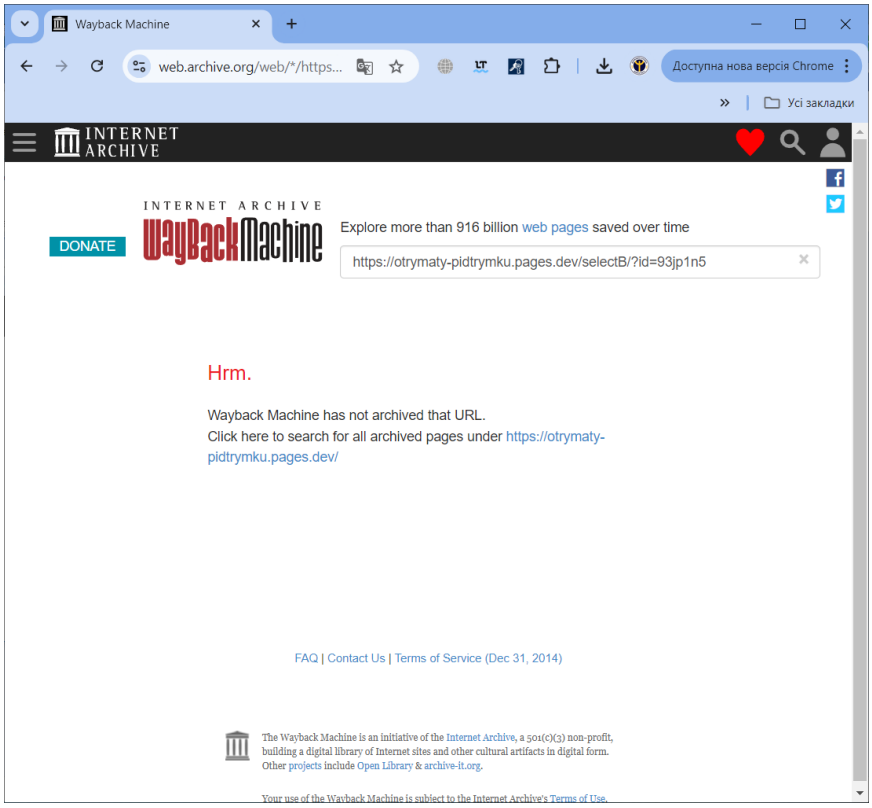


Рисунок 3.20 – Перегляд історії змін веб-сайту

Детальне дослідження HTML-коду веб-сторінки засвідчило наявність типових ознак фішингової діяльності: збір персональних та фінансових даних, використання підроблених логотипів банків та форм для введення банківських реквізитів. Результати аналізу через сервіс VirusTotal підтвердили, що ресурс було позначено як потенційно шкідливий кількома антивірусними системами, що свідчить про його фішинговий характер.

Відсутність згадок про сайт у результатах пошуку через Google Dorks, а також у архіві Wayback Machine, свідчить про його відносну новизну або обмежене розповсюдження. Це підкреслює необхідність вжиття заходів для блокування веб-ресурсу та запобігання подальшому використанню його для шахрайської діяльності.

3.2 Впровадження інструментів та методів безпеки для OSINT-розслідувань кіберінцидентів

У сучасних умовах зростання кіберзлочинності та зростаючої доступності інформації у відкритих джерелах OSINT (Open Source Intelligence) відіграє важливу роль у розслідуванні кіберінцидентів. OSINT дає змогу отримувати розвідувальну інформацію з таких джерел, як соціальні мережі, інтернет-форуми, новинні сайти та інші публічні ресурси. Це дозволяє встановлювати осіб або групи, які можуть бути причетні до кіберінцидентів, та оцінювати загрози й ризики. Водночас діяльність OSINT-аналітиків пов'язана з підвищеними ризиками, оскільки зловмисники можуть ідентифікувати розслідувача, відстежувати його активність або навіть створити загрози його безпеці.

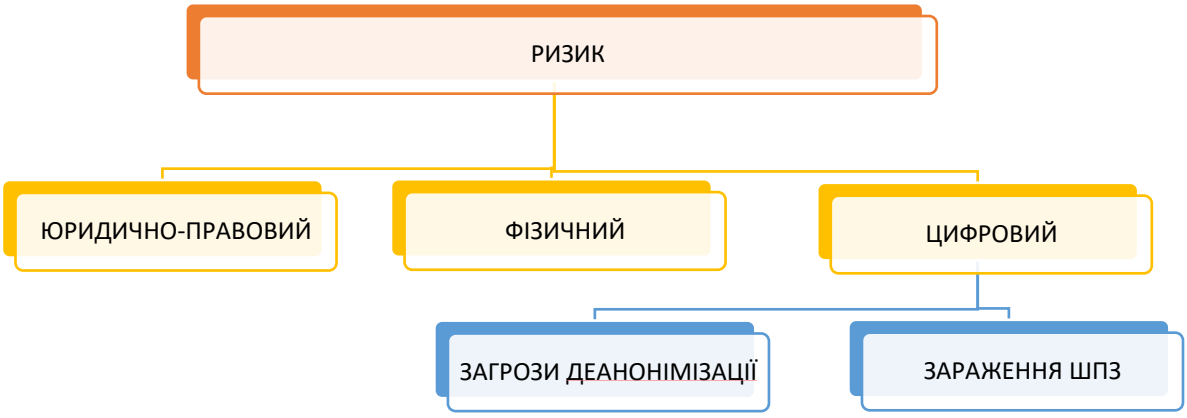


Рисунок 3.21 – Ризики час проведення розслідувань кіберінцидентів

Можна виокремити основні ризики, з якими стикаються OSINT-аналітики під час проведення розслідувань кіберінцидентів (рис. 3.21). Перший ризик — юридично-правовий. У процесі збору даних з відкритих джерел можуть застосовуватися різні інструменти й методи, деякі з яких можуть мати

сумнівний правовий статус або етичну обґрунтованість. Наприклад, певні інструменти можуть порушувати закони щодо конфіденційності та захисту даних, оскільки дають доступ до особистої або корпоративної інформації без згоди. Використання таких інструментів може призвести до юридичних наслідків, тому важливо ретельно перевіряти правомірність застосування інструментів та методів і враховувати етичні аспекти дослідження.

Другий ризик — фізичний. Розслідування кіберінцидентів може становити загрозу фізичній безпеці OSINT-аналітика, особливо якщо дослідження стосуються кіберзлочинних угруповань, впливових осіб або організацій з високим рівнем конфіденційності чи інтересів. Така діяльність може викликати негативну реакцію з боку суб’єктів розслідування, що прагнуть зупинити витік інформації, відстеження їхніх кібероперацій або ідентифікацію. У разі викриття особи аналітика це може призвести до погроз, тиску або навіть фізичного насильства з боку зловмисників. Тому критично важливим є забезпечення високого рівня анонімності та обережності, особливо під час роботи з чутливими даними або особистими даними зловмисників.

Третій ризик — цифровий, який включає загрози деанонімізації та зараження шкідливим програмним забезпеченням. Використання особистих засобів комунікації, таких як електронна пошта, мобільний телефон, справжня IP-адреса або банківські реквізити під час проведення OSINT-розслідування є небажаним, оскільки це значно полегшує ідентифікацію аналітика. Уразливість до цифрових загроз також включає ризик зараження шкідливим ПЗ, яке може потрапити на пристрій через ненадійні джерела, підозрілі посилання або неліцензійне програмне забезпечення. Таке ПЗ може надати зловмисникам віддалений доступ до пристрою аналітика, можливість відстежувати активність, або навіть зашифрувати файли на пристрої, що унеможливить їх відновлення. Для зменшення ризику цифрових загроз важливо використовувати засоби анонімізації, уникаючи підозрілих файлів і

посилань, а також застосовувати засоби захисту, зокрема антивірусне ПЗ та шифрування даних [55].

Додатковим ризиком є втрата конфіденційної інформації внаслідок неналежного поводження з даними. Зберігання незашифрованих файлів, неконтрольований доступ до облікових записів або випадкове розголошення конфіденційної інформації може призвести до витоку даних і підриву розслідування. Щоб запобігти цьому, важливо дотримуватися кібергігієни: використовувати багаторівневу автентифікацію, надійні паролі, окремі облікові записи для роботи та особистої діяльності, а також шифрувати всі важливі дані.

Особливої важливості набувають інструменти й методи захисту особистості та конфіденційності OSINT-фахівців. Використання таких засобів, як анонімізація активності в Інтернеті, захист облікових записів та підключень, застосування віртуальних приватних мереж (VPN) і спеціалізованих браузерів для анонімного перегляду, є критичним для безпеки аналітиків. Такі заходи сприяють приховуванню їхніх дій під час розслідувань, мінімізуючи ризик виявлення зловмисниками. Зокрема, використання операційних систем із підвищеним рівнем захищеності, проксі-серверів та інших технологічних засобів є доцільним для зменшення кіберризиків, які можуть виникнути під час OSINT-діяльності.

Додатково до технічних заходів, необхідними є спеціальні правила поведінки в мережі, що дозволяють знижувати ризик розкриття. Розслідувачі повинні дотримуватися кібергігієни, уникати переходу на сумнівні вебресурси та обмежувати взаємодію з підозрілими профілями, що може поставити під загрозу їхню анонімність і безпеку.

3.2.1 Інструменти забезпечення анонімності при розслідуванні кіберінцидентів

Інструменти для забезпечення анонімності є важливим компонентом захисту при розслідуванні кіберінцидентів за допомогою методів OSINT. Вони дозволяють приховати особисті дані, місцезнаходження та інші параметри, які можуть призвести до ідентифікації особи дослідника або розкриття його діяльності. До основних інструментів, що сприяють досягненню високого рівня анонімності можна віднести: VPN (Virtual Private Network), проксі-сервери, інструменти для шифрування даних і комунікацій, браузери для анонімного серфінгу, менеджери паролів та інструменти для приховування цифрових відбитків (рис. 3.22).

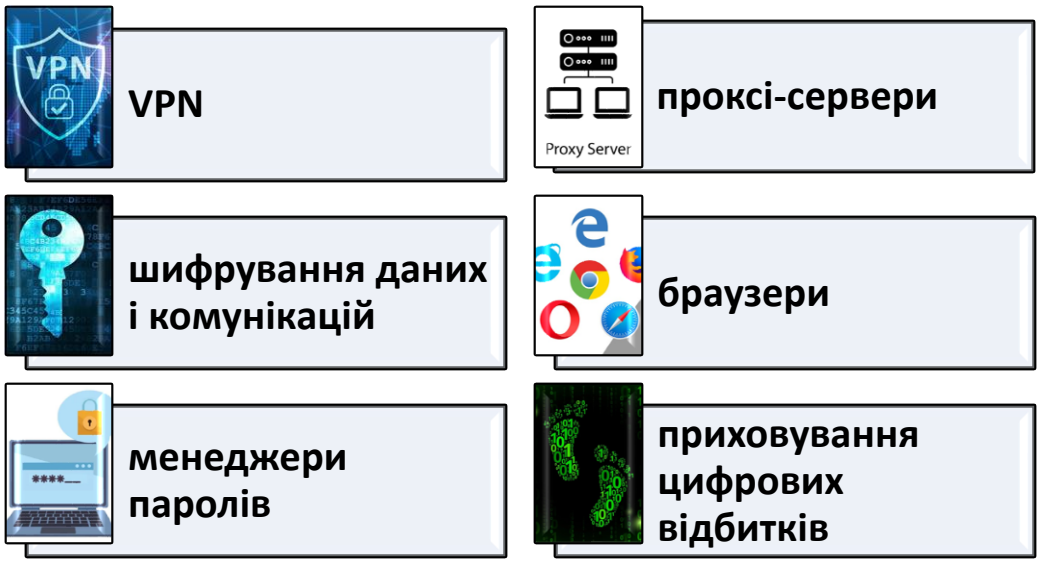


Рисунок 3.22 – Інструменти для забезпечення анонімності

VPN (Virtual Private Network) – це інструмент, який дозволяє розслідувачу захистити свій мережевий трафік, створюючи зашифрований тунель між пристроєм користувача та VPN-сервером. В результаті цього з'єднання

змінюється IP-адреса, що приховує реальне місцезнаходження розслідувача. VPN шифрує весь трафік, що робить його недоступним для сторонніх спостерігачів. Крім того, він дозволяє обійти регіональні блокування, забезпечуючи вільний доступ до інформації в мережі. При виборі VPN-сервісу важливо враховувати кілька ключових факторів. Перш за все, необхідно звертати увагу на політику No logs, що гарантує відсутність збереження записів про активність користувача. Важливим також є використання надійних алгоритмів шифрування, таких як AES-256, які забезпечують високий рівень захисту даних. Крім того, слід звернути увагу на підтримку сучасних та безпечних протоколів, таких як OpenVPN, IKEv2 чи WireGuard, що забезпечують стабільність і швидкість з’єднання. Останнім, але не менш важливим аспектом є наявність функції Kill Switch, яка автоматично відключає інтернет-з'єднання у випадку втрати VPN-з'єднання, запобігаючи тим самим витоку даних [56]. Крім того, варто звертати увагу на географічне розташування серверів VPN-постачальника, що може впливати на швидкість з’єднання та можливість обходу регіональних обмежень. Не менш важливою є також сумісність сервісу з різними операційними системами та пристроями, щоб забезпечити зручність використання на різних платформах.

Браузери для анонімного серфінгу є важливими інструментами для забезпечення конфіденційності та анонімності користувачів, зокрема у контексті проведення OSINT-розслідувань. Одним із найвідоміших браузерів, що забезпечує високий рівень анонімності, є Tor Browser, який використовує мережу Tor для маршрутизації інтернет-трафіку через низку зашифрованих вузлів. Це дозволяє приховати реальне місцезнаходження користувача та захищати його ідентичність, ускладнюючи визначення його IP-адреси. Tor Browser також автоматично блокує сторонні трекери та куки, що зменшує кількість залишкових слідів у мережі та запобігає відстеженню діяльності користувача.

Іншим інструментом, що забезпечує підвищену конфіденційність, є Brave Browser, який вбудовано містить функціонал блокування реклами та трекерів.

Крім того, Brave надає можливість активації режиму приватного перегляду через мережу Tor, що додає додатковий рівень анонімності. Цей режим дозволяє приховати реальний IP-адрес користувача навіть під час стандартного серфінгу в Інтернеті, що значно знижує ризик ідентифікації та збору персональних даних. Brave також дає змогу користувачам блокувати сторонні скрипти та інші елементи, які можуть бути використані для збору інформації про їхню активність в мережі.

Проксі-сервери, такі як Smartproxy, ProxySite, та Oxylabs, функціонують як посередники між користувачем та цільовим веб-ресурсом, забезпечуючи ефективне маскування IP-адреси дослідника й підвищуючи рівень анонімності під час здійснення онлайн-діяльності. Ці сервіси можуть бути налаштовані для обробки певних типів трафіку, наприклад, HTTP або SOCKS, що дозволяє адаптувати їх до специфічних потреб користувача [57]. Проксі-сервери забезпечують перший рівень захисту, блокуючи можливість відстеження або ідентифікації користувача. Використання проксі-серверів разом із іншими інструментами конфіденційності, такими як VPN чи Tor, може значно підвищити рівень анонімності. Наприклад, Bright Data та GeoSurf пропонують функцію обертання IP-адрес для кожного окремого запиту, що ускладнює можливість відстеження активності користувача. Завдяки цій функції IP-адреса змінюється на нову щоразу, коли відбувається запит до ресурсу, що унеможливлює встановлення зв’язків між послідовними запитами.

Інструменти для шифрування даних і комунікацій є важливими засобами забезпечення захисту інформації, що передається або зберігається під час проведення OSINT-розслідувань. Зокрема, PGP (Pretty Good Privacy) широко застосовується для шифрування електронної пошти та файлів, що дозволяє захищати конфіденційні дані від несанкціонованого доступу. Цей інструмент використовує метод асиметричного шифрування, який забезпечує високий рівень безпеки, особливо під час передачі інформації, що має чутливий характер.

Месенджери з наскрізним шифруванням, такі як Signal та WhatsApp, захищають комунікації шляхом шифрування повідомлень від відправника до одержувача, запобігаючи можливості їх перехоплення сторонніми особами. Наскрізне шифрування є ефективним засобом захисту комунікацій у режимі реального часу, що є критично важливим у контексті розслідувань.

Для локального захисту даних застосовуються програми для шифрування файлів і дисків. Серед вбудованих механізмів шифрування виділяють BitLocker для Windows, FileVault для macOS та LUKS для Linux. Ці інструменти надають базовий рівень захисту, однак, для повноцінного використання часто потребують активації, а також відповідного налаштування параметрів доступу та збереження ключів. VeraCrypt є потужною некомерційною безкоштовною програмою для шифрування файлів і дисків, яка підтримується на платформах Windows, macOS та Linux. Вона забезпечує високий рівень безпеки завдяки можливості створення зашифрованих контейнерів та прихованих розділів. Це дозволяє надійно зберігати конфіденційні дані, мінімізуючи ризик несанкціонованого доступу до них у випадку втрати або крадіжки пристрою. VeraCrypt також підтримує функції шифрування системного розділу, що захищає весь вміст комп'ютера від стороннього доступу під час завантаження системи.

Використання таких інструментів, як менеджери паролів є важливим елементом у системі захисту інформації під час OSINT-розслідувань, де конфіденційність доступу до облікових записів має вирішальне значення для запобігання потенційним кіберзагрозам. Менеджери паролів відіграють ключову роль у забезпеченні безпеки доступу до облікових записів, запобігаючи ризикам, пов'язаним із використанням однакових або недостатньо надійних паролів для різних платформ. Інструменти на зразок LastPass, Bitwarden та 1Password забезпечують зберігання паролів у зашифрованому форматі, що унеможливлює несанкціонований доступ до конфіденційних даних. Ці сервіси також генерують унікальні й складні паролі для кожного облікового запису, що значно знижує ймовірність їх

компрометації. Додатково, більшість сучасних менеджерів паролів підтримують двофакторну автентифікацію, яка слугує додатковим рівнем захисту та підвищує загальний рівень безпеки інформації.

Інструменти для приховування цифрових відбитків використовуються для запобігання ідентифікації користувача за унікальними характеристиками браузера або пристрою. Розширення на зразок Privacy Badger і uBlock Origin блокують різні трекери, знижуючи ймовірність відстеження та ідентифікації користувача за допомогою збору інформації про його дії в мережі. Інші спеціалізовані програми, як-от Canvas Defender або User-Agent Switcher, забезпечують маскування та модифікацію унікальних параметрів браузера (наприклад, налаштувань рендерингу чи ідентифікатора браузера). Ці інструменти дозволяють ускладнити створення та використання цифрового відбитка, що значно підвищує рівень конфіденційності й анонімності користувача під час проведення OSINT-розслідувань.

3.2.2 Захист цифрової інфраструктури при розслідуванні кіберінцидентів

Захист цифрової інфраструктури є одним із ключових аспектів проведення OSINT-розслідувань кіберінцидентів. Належний рівень безпеки дозволяє зберігати конфіденційність, цілісність і доступність зібраної інформації, а також запобігати атакам, спрямованим на розслідувача. На рисунку 3.23 розглянуто основні заходи щодо захисту цифрової інфраструктури - ізоляція робочого середовища, моніторинг активності, забезпечення надійного доступу та організація безпечного зберігання даних.

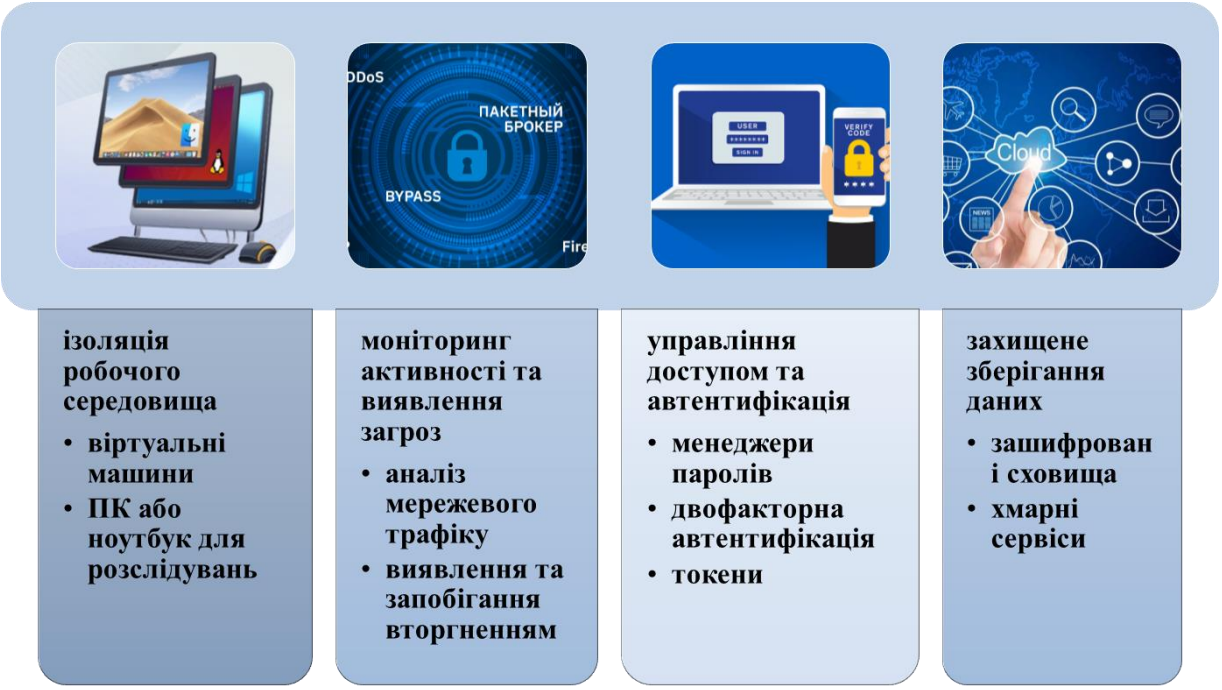


Рисунок 3.23 – Захист цифрової інфраструктури

Для забезпечення безпеки під час роботи з потенційно небезпечними файлами, програмами або вебресурсами доцільно використовувати ізольовані віртуальні середовища. Віртуальні машини (VM) дозволяють створювати середовища із високим рівнем ізоляції, які можуть бути налаштовані відповідно до потреб користувача, легко видалені або відновлені у разі виникнення загроз. Популярні програмні рішення для створення віртуальних машин, такі як VirtualBox і VMware Workstation які пропонують різні функціональні можливості та рівні безпеки.

VirtualBox – це безкоштовне рішення з відкритим кодом, яке підтримується корпорацією Oracle. Воно є доступним для широкого кола користувачів та забезпечує створення багатоплатформових віртуальних середовищ. VirtualBox пропонує такі функції, як підтримка шифрування жорстких дисків віртуальних машин, налаштування мережевих адаптерів для ізоляції трафіку та створення загальних папок для обміну файлами між хостом і віртуальним середовищем.

VMware Workstation є комерційним продуктом, який забезпечує високу продуктивність і гнучкість у налаштуванні віртуальних середовищ. Є і

безкоштовна версія VMware Workstation Player з обмеженими функціями. Цей інструмент підтримує створення кількох одночасно працюючих віртуальних машин із можливістю використання різних операційних систем, таких як Windows, Linux або macOS. Однією з ключових функцій є підтримка ізоляції мережевого доступу між віртуальними машинами та хост-системою, що значно зменшує ризик мережевих атак.

Моніторинг мережевої активності та системних подій є одним із важливих компонентів забезпечення кібербезпеки під час OSINT-розслідувань. Використання інструментів для аналізу мережевого трафіку, таких як Wireshark, дозволяє ідентифікувати аномальну активність, яка може свідчити про спроби атак або несанкціонований доступ до системи.

Wireshark є високоефективним інструментом для детального аналізу протоколів та мережевих пакетів у режимі реального часу, що надає можливість OSINT-аналітикам ідентифікувати мережеві вразливості, а також аналізувати підозрілий трафік, ідентифікувати можливі спроби компрометації та простежувати джерела атак [58].

Системи виявлення та запобігання вторгненням (IDS/IPS), такі як Snort і Suricata, дозволять здійснити оперативний аналіз загроз. Snort - це система з відкритим кодом, що може працювати на різних операційних системах, яка дозволяє аналізувати мережевий трафік у режимі реального часу. Завдяки правилам і сигнатурам вона ідентифікує загрози та забезпечує можливість використання різних методів аналізу, таких як сигнатурний, статистичний та гібридний. Snort може бути налаштована для блокування підозрілих з'єднань у режимі запобігання вторгненням (IPS), що підвищує ефективність захисту від кіберзагроз. Suricata - це багатофункціональна платформа для аналізу мережевого трафіку, яка об'єднує функції виявлення вторгнень, аналізу протоколів і обробки трафіку. Вона здатна працювати з великими обсягами даних у середовищах із високими вимогами до продуктивності, що робить її ефективним інструментом для моніторингу інфраструктури з великим навантаженням. Suricata підтримує комбінований підхід до аналізу, що

включає сигнатурний, статистичний і поведінковий методи, підвищуючи її гнучкість і надійність у виявленні загроз [59].

Під час OSINT-розслідувань кіберінцидентів важливо впроваджувати політики мінімального доступу (Principle of Least Privilege, PoLP), які обмежують права доступу до мінімально необхідного рівня, та регулярно перевіряти привілеї користувачів. Використання спеціалізованого програмного забезпечення, як-от CyberArk або BeyondTrust, дозволяє автоматизувати управління привілеями, обмежуючи доступ відповідно до принципу PoLP. Також доцільно налаштовувати сегментацію мережі та обмеження доступу до баз даних і сховищ за допомогою ролей у таких платформах, як AWS IAM або Microsoft Azure RBAC. Ці заходи знизять ризик несанкціонованого доступу, навіть якщо окремий обліковий запис буде скомпрометовано. Для додаткової перевірки особи рекомендується використовувати двофакторну (2FA) або багатофакторну автентифікацію (MFA), наприклад через Google Authenticator, Authy або апаратні токени, такі як YubiKey чи Feitian. Токени забезпечать додатковий рівень безпеки, оскільки генерують унікальні ключі або використовують апаратну криптографію для підтвердження особи. Менеджери паролів, дозволяють створювати та зберігати унікальні складні паролі для облікового запису. Регулярна зміна паролів і заборона їх повторного використання є важливими елементами безпеки. Забезпечення захисту фізичного доступу до робочих пристроїв через паролі, картки доступу або біометричні засоби є критичним для запобігання несанкціонованому втручанню. Крім того, використання віртуальних приватних мереж (VPN) і списків дозволених IP-адрес для обмеження доступу до систем ззовні підвищує рівень безпеки.

Зберігання даних є критично важливим елементом OSINT-розслідувань, оскільки отримана інформація часто має конфіденційний характер і потребує надійного захисту. Для резервного копіювання даних доцільно використовувати як хмарні сервіси (наприклад, Google Диск, Dropbox, OneDrive, iCloud), так і зовнішні носії (USB, HDD, SSD). Хмарні платформи

пропонують зручність доступу і певний обсяг безкоштовного сховища, однак вимагають налаштування надійних паролів та двофакторної автентифікації для зниження ризику несанкціонованого доступу. Зовнішні накопичувачі забезпечують автономність зберігання, але їх також рекомендується захищати за допомогою шифрування та паролів, що мінімізує ризик компрометації у випадку фізичної втрати пристрою.

3.2.3 Безпечні методи комунікації та захист акаунтів при проведенні OSINT-розслідувань

Важливою складовою ефективного OSINT-розслідування є безпечна комунікація та захист акаунтів. Для цього слід застосовувати сучасні методи анонімізації та шифрування, фіктивні акаунти та інші техніки маскування, що дозволяють знизити ризики ідентифікації та зберегти конфіденційність. За допомогою спеціальних генераторів для створення автентичних, випадкових даних можна створити псевдонімні профілі без реальних даних. Підготувати окремі номери телефонів, електронну пошту та банківську карту для OSINT-розслідування. При створенні облікових записів для OSINT-розслідувань доцільно використовувати унікальні паролі для кожного акаунта, а також прив’язувати облікові записи до різних електронних адрес, що унеможливлює їх взаємозв’язок. Для підвищення рівня безпеки необхідно впроваджувати двофакторну автентифікацію (2FA) або використовувати апаратні ключі, які забезпечують додатковий рівень захисту. У разі довгострокового використання облікових записів рекомендується періодично оновлювати паролі, щоб мінімізувати ризики компрометації. Регулярний моніторинг активних сесій і пристроїв, які мають доступ до акаунта, дозволяє своєчасно виявляти підозрілу активність і вживати необхідних заходів для захисту. Варто зазначити що зловмисники, які знаходяться з вами в одній країні можуть

перехоплювати ваші sms-повідомлення, телефонні розмови, а також відстежувати вашу локацію через стільникову мережу мобільного оператора. Тому для комунікації варто використовувати зашифровані канали з'єднання такі як повідомлення або дзвінки у месенджерах. Універсально найбезпечнішого месенджера не існує, оскільки кожен канал зв’язку має свої переваги та недоліки. Основні критерії вибору месенджерів включають шифрування, анонімність та захист пристроїв.

Месенджери використовують два основних типи шифрування:

- шифрування від пристрою до сервера: дані передаються у зашифрованому вигляді, але зберігаються на сервері у відкритому форматі. Таке шифрування застосовують, наприклад, Google, Facebook (для групових чатів), Telegram (за винятком секретних чатів). Оскільки власники серверів мають доступ до цих даних, вони можуть надати їх урядовим органам на запит. Попри це, такі випадки висвітлюються у щорічних звітах про прозорість.

- наскрізне шифрування: дані зберігаються у відкритому вигляді лише на пристроях користувачів, а на сервері – у зашифрованому форматі. Головною відмінністю є те, що доступ до переписок можливий лише з оригінального пристрою. Цей тип шифрування забезпечує вищий рівень конфіденційності та захищає інформацію навіть у разі зламу облікового запису. Прикладами таких месенджерів є Signal та WhatsApp. Для передачі чутливої інформації рекомендується використовувати саме платформи з наскрізним шифруванням за замовчуванням.

Анонімність дозволяє мінімізувати цифровий слід і ускладнити відстеження дій фахівця при проведенні OSINT-розслідувань. Для забезпечення анонімності рекомендується використовувати окремі облікові записи, створені спеціально для розслідувань, а також застосовувати VPN, який приховує IP-адресу, забезпечуючи додатковий рівень конфіденційності.

Захист пристроїв є критичним елементом безпеки комунікацій, оскільки фізичний доступ зловмисника до пристрою може скомпрометувати конфіденційність даних, навіть за наявності шифрування. Щоб мінімізувати

такі ризики, важливо використовувати сильні паролі або біометричний захист, регулярно оновлювати операційну систему та програмне забезпечення, а також встановлювати виключно ліцензійне ПЗ.

3.3 Висновки до розділу 3

Технології OSINT демонструють значний потенціал у сучасних умовах інформаційного суспільства, забезпечуючи перевагу в сферах конкуренції, особистої, корпоративної та національної безпеки.

Розслідування кіберінцидентів є складним і тривалим процесом, що вимагає систематичного підходу до аналізу подій, визначення типу інциденту, його тривалості та встановлення дій, що мали місце. Методи OSINT є одним із ключових інструментів, які дозволяють здійснювати ефективний моніторинг відкритих джерел інформації, аналіз індикаторів компрометації (IOC), геолокацію, а також дослідження мережевої активності через доменні імена та IP-адреси. Наприклад, аналіз електронної пошти дозволяє ідентифікувати джерело загроз шляхом дослідження IP-адрес і серверів розсилки. Аналіз криптогаманців у межах блокчейн-технологій допомагає виявляти підозрілі транзакції і взаємозв'язки між ними. Аналіз URL-адрес сприяє виявленню фішингових ресурсів та їхньої інфраструктури. Поєднання OSINT із іншими підходами (глибокий аналіз шкідливих програм, вивчення мережевих зв’язків) може значно посилити ефективність розслідувань і забезпечити надійний захист інформації та активів у цифровому середовищі.

Для забезпечення ефективного і безпечного проведення таких розслідувань необхідно впроваджувати інструменти безпеки, зокрема використовувати VPN, проксі-сервери, анонімні браузери (Tor), шифрування даних, а також забезпечити високий рівень анонімності. Це дозволяє приховати особисті дані та місцезнаходження аналітиків, мінімізуючи ризики

їх ідентифікації. Крім того, важливо застосовувати віртуальні машини для безпечної роботи з потенційно небезпечними ресурсами, моніторити мережеву активність для виявлення аномалій і атак, а також захищати цифрову інфраструктуру для збереження конфіденційності і цілісності даних. Тому впровадження таких методів є необхідним для безпечного та результативного проведення OSINT-розслідувань в умовах сучасних кіберзагроз.

ВИСНОВКИ

У магістерській роботі здійснено дослідження методів OSINT та їх впровадження для безпечного OSINT-розслідування кіберінцидентів. Основним завданням дослідження було висвітлити роль методів OSINT при розслідуванні кіберінцидентів.

Під час виконання магістерській роботи було проаналізовано сучасний стан використання методів OSINT, зокрема розглянуто й опрацьовано популярні інструменти, такі як Shodan, Maltego, Recon-ng та інші, що застосовуються для збору та аналізу інформації під час розслідувань кіберінцидентів. Практичні приклади ілюструють способи використання цих методів для ідентифікації джерел загроз, виявлення вразливостей у цифровій інфраструктурі та запобігання кібератакам.

Окрему увагу приділено використанню методів OSINT на правових аспектах. Проведено детальний аналіз нормативно-правових актів, які регламентують застосування відкритих джерел інформації, а також розглянуто проблеми, що виникають у процесі обробки конфіденційної інформації та персональних даних. Для підвищення ефективності та безпеки OSINT-розслідувань запропоновано впровадження спеціалізованих інструментів і методів захисту для аналітиків, зокрема створення захищеного середовища для роботи, використання анонімізації та захист даних. Це дозволяє мінімізувати ризики компрометації даних, забезпечити конфіденційність процесу розслідування та підвищити якість результатів.

Загалом, результати дослідження підтверджують важливість методів OSINT у сучасних умовах цифровізації та зростання кількості кіберінцидентів, а також підкреслюють необхідність їх інтеграції при розслідуванні кіберінцидентів, що може суттєво підвищити рівень інформаційної безпеки та забезпечити якісне реагування на загрози.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Електронна енциклопедія Wikipedia. Розвідка на основі відкритих джерел [Електронний ресурс] - Режим доступу до ресурсу: https://uk.wikipedia.org/w/index.php?title= Розвідка на основі відкритих джерел&stable=0

2. Жмур Н. В., Землянікіна М. П., Історія становлення та сучасний стан технології пошуку інформації OSINT – Київ: Національний авіаційний університет - 2022. [Електронний ресурс] - Режим доступу до ресурсу: http://www.law.nau.edu.ua/images/Nauka/Naukovij_jurnal/2022/3-64/15.pdf

3. Esteban Borges, What Is Open Source Intelligence (OSINT)? - 2024. [Електронний ресурс] - Режим доступу до ресурсу: https://www.recordedfuture.com/blog/open-source-intelligence-definition

4. Електронна енциклопедія Wikipedia. Глибинна мережа [Електронний ресурс] - Режим доступу до ресурсу: https://uk.wikipedia.org/w/index.php?title= Глибинна мережа&stable=0

5. Joseph E. Roop, Foreign Broadcast Information Service. History. Part 1: 1941-1947 - 1969. [Електронний ресурс]. – Режим доступу до ресурсу: https://apps.dtic.mil/sti/pdfs/ADA510770.pdf

6. Жарков Я. М., Васильєв А. О., Наукові підходи щодо визначення суті розвідки з відкритих джерел – Київ: Вісник Київського національного університету імені Тараса Шевченка. Військово-спеціальні науки. - 2013. [Електронний ресурс] – Режим доступу до ресурсу: http://nbuv.gov.ua/UJRN/VKNU_vsn_2013_30_12\

7. Admiral William Studeman, Teaching the Giant to Dance: Contradictions and Opportunities in Open Source Within the Intelligence Community - 1993. [Електронний ресурс] – Режим доступу до ресурсу: http://www.oss.net/dynamaster/file_archive/090716/f571532e0af491b3aefe870 fe9f454f0/AIJ%2092%20011-018%20Studeman.pdf

8. Hamilton, B., The DNI’s Open Source Center: An Organizational Communication Perspective, International Journal of Intelligence and CounterIntelligence – 2007. [Електронний ресурс] – Режим доступу ресурсу: https://www.researchgate.net/publication/233220754_The_DNI's_Open_Source_Center_An_Organizational_Communication_Perspective

9. Кожушко О.О., Розвідка відкритих джерел інформації (osint) у розвідувальній практиці США – Київ: Інститут міжнародних відносин Національного авіаційного університету – 2013. [Електронний ресурс] - Режим доступу до ресурсу: https://jrnl.nau.edu.ua/index.php/IMV/article/view/3264/3217

10. Zosym Maxym, Розвідка з відкритих джерел (Open-source intelligence - OSINT) - 2023. [Електронний ресурс] - Режим доступу до ресурсу: https://www.maxzosim.com/rozvidka-z-vidkritikh-dzherel-osint/

11. Understanding the Different Types of Intelligence Collection Disciplines. – 2022. [Електронний ресурс] - Режим доступу до ресурсу: https://www.maltego.com/blog/understanding-the-different-types-of-intelligence-collection-disciplines/

12. Електронна енциклопедія Wikipedia. Агентурна розвідка [Електронний ресурс] - Режим доступу до ресурсу: https://uk.wikipedia.org/w/index.php?title=Агентурна розвідка &stable=0

13. H. Akın Ünver, Digital Open Source Intelligence and International Security: A Primer - 2018. [Електронний ресурс] - Режим доступу до ресурсу: https://www.jstor.org/stable/resrep21048

14. Про інформацію: Закон України від 02.10.92 р. № 2657-XII. [Електронний ресурс] - Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/2657-12#Text

15. Про медіа: Закон України від 31.03.23 р. № 2849-IX. [Електронний ресурс] - Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/2849-20#Text

16. Електронна енциклопедія Wikipedia. Закон України «Про медіа» [Електронний ресурс] - Режим доступу до ресурсу: https://uk.wikipedia.org/w/index.php?title=Закон України «Про медіа»&stable=0

17. Про охоронну діяльність: Закон України від 22.03.12 р. № 4616-VI. [Електронний ресурс] - Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/4616-17#Text

18. Про захист персональних даних: Закон України від 01.06.10 р. №2297-VI. [Електронний ресурс] - Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/2297-17#Text

19. Ланде Д.В., Правові питання конкурентної розвідки: Журнал "Інформація і право" №2(33) – 2020. [Електронний ресурс] - Режим доступу до ресурсу: https://ippi.org.ua/lande-dv-pravovi-pitannya-konkurentnoi-rozvidki-st-51-68

20. Про Національний координаційний центр кібербезпеки: Указ Президента України від 07.06.16р. №242/2016. [Електронний ресурс] - Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/96/2016#Text

21. Середа О.Г., Красюк Т.В., Персональні дані працівника та їх захист в умовах цифровізації - Електронне наукове видання «Аналітично-порівняльне правознавство» - 2023. [Електронний ресурс] - Режим доступу до ресурсу: https://doi.org/10.24144/2788-6018.2023.03.33

22. Електронна енциклопедія Wikipedia. Персональні дані. [Електронний ресурс] - Режим доступу до ресурсу: https://uk.wikipedia.org/w/index.php?title= Персональні дані&stable=0

23. Кожухар О. Liga zakon. Обробка персональних даних в Україні: правові аспекти. [Електронний ресурс] - Режим доступу до ресурсу: https://jurliga.ligazakon.net/analitycs/226318_obrobka-personalnikh-danikh-v-ukran-pravov-aspekti

24. Проєкт Закону про захист персональних даних: Закон України від 25.10.2022 р. №8153. [Електронний ресурс] - Режим доступу до ресурсу: https://itd.rada.gov.ua/billInfo/Bills/Card/40707

25. Електронна енциклопедія Wikipedia. Petya [Електронний ресурс] – Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/Petya

26. Електронна енциклопедія Wikipedia. DarkHotel. [Електронний ресурс] – Режим доступу до ресурсу: https://en.wikipedia.org/wiki/DarkHotel

27. Електронна енциклопедія Wikipedia. WannaCry [Електронний ресурс] – Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/WannaCry

28. Ms.detector.media: Українські інформаційні ресурси зазнали потужної DDoS-атаки - Київ: Держспецзв'язку – 2022. [Електронний ресурс] – Режим доступу до ресурсу: https://ms.detector.media/kiberbezpeka/post/28957/2022-02-15-ukrainski-informatsiyni-resursy-zaznaly-potuzhnoi-ddos-ataky-derzhspetszvyazku

29. Enisa, Threat Landscape - 2022. [Електронний ресурс] - Режим доступу до ресурсу: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022/@@download/fullReport

30. Joseph Poppy, What is the cyber kill chain and why is it important? - 2019. [Електронний ресурс] - Режим доступу до ресурсу: https://www.bulletproof.co.uk/blog/what-is-the-cyber-kill-chain

31. Penetration Testing with Open-Source Intelligence (OSINT): Tips, Tools, and Techniques. – 2022. [Електронний ресурс] - Режим доступу до ресурсу: https://www.eccouncil.org/cybersecurity-exchange/penetration-testing/penetration-testing-open-source-intelligence-osint/

32. Алекс МакФарланд, 10 найкращих інструментів Open Source Intelligence (OSINT) – 2024. [Електронний ресурс] - Режим доступу до ресурсу: https://www.unite.ai/uk/best-open-source-intelligence-osint-tools/

33. Електронна енциклопедія Wikipedia. Shodan (вебсайт). [Електронний ресурс] - Режим доступу до ресурсу: https://uk.wikipedia.org/w/index.php?title= Shodan (вебсайт)&stable=0

34. Cyber Witcher. №4. Хакінг у практичному застосуванні та соціальна інженерія (Бізнес-розвідка з відкритих джерел)- 2023. [Електронний ресурс] -

Режим доступу до ресурсу: https://hackyourmom.com/kibervijna/biznes-rozvidka-z-vidkrytyh-dzherel-chastyna-4/

35. GeeksforGeeks. TIDoS-Framework – Offensive Web Application Penetration Testing Framework – 2021. [Електронний ресурс] - Режим доступу до ресурсу: https://www.geeksforgeeks.org/tidos-framework-offensive-web-application-penetration-testing-framework/

36. GitHub. TIDoS-фреймворк. [Електронний ресурс] - Режим доступу до ресурсу: https://github.com/0xInfection/TIDoS-Framework?tab=readme-ov-file

37. Електронна енциклопедія Wikipedia. Maltego. [Електронний ресурс] - Режим доступу до ресурсу: https://ru.wikipedia.org/wiki/Maltego

38. Cyber Witcher. Maltego Частина 1. Принципи роботи та можливості, 4 релізи. - 2023. [Електронний ресурс] - Режим доступу до ресурсу: https://hackyourmom.com/kibervijna/zbir-informacziyi-pro-suprotyvnyka/osint-akademiya/4-relizy-maltego-prynczypy-roboty-ta-mozhlyvosti/

39. Esteban Borges. theHarvester: a Classic Open Source Intelligence Tool – 2021. [Електронний ресурс] - Режим доступу до ресурсу: https://securitytrails.com/blog/theharvester-tool

40. eSecurity Institute. OSINT Framework. – 2021. [Електронний ресурс] - Режим доступу до ресурсу: https://www.esecurityinstitute.com/osint-framework/

41. Softlist. Cobwebs – платформа інтернет-розслідувань. [Електронний ресурс] - Режим доступу до ресурсу: https://softlist.com.ua/ua/catalog/cobwebs-platforma-internet-rassledovaniy

42. Електронна енциклопедія Wikipedia. Google hacking. [Електронний ресурс] - Режим доступу до ресурсу: https://en.wikipedia.org/wiki/Google_hacking

43. Esteban Borges. Top 15 OSINT Tools for Expert Intelligence Gathering. - 2024. [Електронний ресурс] - Режим доступу до ресурсу: https://www.recordedfuture.com/threat-intelligence-101/tools-and-technologies/osint-tools

44. Esteban Borges. Google Dorks: Top Tips and Tricks for Advanced Search Intelligence. – 2024. [Електронний ресурс] - Режим доступу до ресурсу: https://www.recordedfuture.com/threat-intelligence-101/threat-analysis-techniques/google-dorks

45. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.17 р. № 2163-VIII. [Електронний ресурс] - Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/2163-19#Text

46. Перелік категорій кіберінцидентів. [Електронний ресурс] - Режим доступу до ресурсу: https://cert.gov.ua/recommendation/16904

47. Б. М. Головкін, О. І. Денькович, В. В. Луцик, Д. М. Цехан. Кіберзлочинність та електронні докази: навчальний посібник – Львів: ЛНУ ім. Івана Франка – 2022. [Електронний ресурс] - Режим доступу до ресурсу: https://law.lnu.edu.ua/wp-content/uploads/2023/08/Cybercrime-and-Digital-Evidence.pdf

48. Статистичний звіт за результатами роботи Системи виявлення вразливостей і реагування на кіберінциденти та кібератаки в 2023 році. Державний центр кіберзахисту – 2024. [Електронний ресурс] - Режим доступу до ресурсу: https://scpc.gov.ua/uk/articles/334

49. Конвенція про кіберзлочинність. Статус Конвенції див. (994_789). Ратифікація від 07.09.2005. [Електронний ресурс] - Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/994_575#Text

50. Деякі питання забезпечення функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки: Постанова Кабінету Міністрів України від 23.12.2020 № 1295. [Електронний ресурс] - Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/1295-2020-%D0%BF#Text

51. Про затвердження Методичних рекомендацій щодо реагування суб’єктами забезпечення кібербезпеки на різні види подій у кіберпросторі: Наказ Адміністрації Держспецзв'язку від 03.07.2023 № 570. [Електронний ресурс] - Режим доступу до ресурсу: https://cip.gov.ua/ua/news/nakaz-

administraciyi-derzhspeczv-yazku-vid-03-07-2023-570-pro-zatverdzhennya-metodichnikh-rekomendacii-shodo-reaguvannya-sub-yektami-zabezpechennya-kiberbezpeki-na-rizni-vidi-podii-u-kiberprostori

52. Реагування на кіберінциденти/кібератаки. Державна служба спеціального зв'язку та захисту інформації України – 2024. . [Електронний ресурс] - Режим доступу до ресурсу: https://cip.gov.ua/ua/news/reaguvannya-na-kiberincidenti-kiberataki

53. Про затвердження Порядку передачі комплектів обладнання підсистеми збору телеметрії інформаційно-комунікаційних систем (активні сенсори) системи виявлення вразливостей і реагування на кіберінциденти та кібератаки до об’єктів кіберзахисту: Наказ Адміністрації Держспецзв’язку від 24.06.2022 № 284. [Електронний ресурс] - Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/z0758-22#Text

54. Деякі питання реагування суб’єктами забезпечення кібербезпеки на різні види подій у кіберпросторі: Постанова Кабінету Міністрів України від 04.04.2023 № 299. [Електронний ресурс] - Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/299-2023-%D0%BF#Text

55. Піківець Г.М., Корольков Р.Ю. Забезпечення анонімності аналітиків під час OSINT-розслідувань: НУ «Запорізька політехніка» - 2024. [Електронний ресурс] - Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/z0758-22#Text

56. Antanas Rimeikis. Який протокол VPN є найкращим у 2024?: Surfshark – 2024. [Електронний ресурс] - Режим доступу до ресурсу: https://surfshark.com/uk/blog/vpn-protocols

57. Antanas Rimeikis. Проксі-сервер: що це таке і чи потрібен він вам? ?: Surfshark – 2022. [Електронний ресурс] - Режим доступу до ресурсу: https://surfshark.com/uk/blog/proxy-server

58. Tsippi Dach. Top 9 Network Security Monitoring Tools for Identifying Potential Threats: AlgoSec – 2024. [Електронний ресурс] - Режим доступу до ресурсу: https://www.algosec.com/blog/network-security-monitoring-tools/

59. Коробейнікова Т., Цар О. Аналіз сучасних відкритих систем виявлення та запобігання вторгнень; Grail of Science, (27) - 2023. [Електронний ресурс] - Режим доступу до ресурсу: https://archive.journal-grail.science/index.php/2710-3056/article/view/1257

ДОДАТОК А

Апробація результатів

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ЗАПОРІЗЬКА ПОЛІТЕХНІКА»

ТИЖДЕНЬ НАУКИ-2024
Факультет інформаційної безпеки та електронних комунікацій

Збірник тез доповідей щорічної
науково-практичної конференції серед студентів, викладачів, науковців, молодих учених і аспірантів
15–19 квітня 2024 року

Електронне видання на DVD-ROM

Запоріжжя • НУ «Запорізька політехніка» • 2024

УДК 004.056
Піківець Г.М.[1], Корольков Р.Ю.[2]
[1] студ. гр. БКз-813м НУ «Запорізька політехніка»
[2] канд. техн. наук, доц. НУ «Запорізька політехніка»

ОГЛЯД МЕТОДІВ OSINT ТА ЇХ РОЛЬ У РОЗСЛІДУВАННІ КІБЕРІНЦИДЕНТІВ

Кіберзлочинність стрімко еволюціонує, перетворюючись на одну з найбільш актуальних проблем сучасності. Зловмисники постійно удосконалюють свої методи, завдаючи шкоду як приватним особам, так і великим компаніям. У цьому контексті, розслідування кіберінцидентів стає все більш важливим завданням, оскільки від його успіху залежить не лише компенсація завданих збитків, але й запобігання майбутнім атакам.

Звичайні методи розслідування не завжди є ефективними у віртуальному просторі, де зловмисники використовують складні інструменти та методи для приховування своїх дій. Розвідка з відкритих джерел стає все більш ефективним інструментом у боротьбі з кіберзлочинністю та кіберінцидентами [1]. В контексті протидії кіберзлочинності методи розвідки з відкритих джерел набувають все більшого значення, що дозволяє збирати інформацію про зловмисників, їхні методи та цілі, а також моніторити кіберзагрози.

Open Source Intelligence (OSINT) – це концепція, методологія та технологія для отримання та використання військової, політичної, економічної та іншої інформації з відкритих джерел без порушення чинного законодавства. OSINT використовується для прийняття рішень у сфері національної оборони та безпеки, у розслідуваннях кіберзлочинів, терористичних актів та інших подій, що включає збір інформації, реєстрацію, облік та аналіз, аналітичну та синтетичну обробку первинної інформації, зберігання та поширення інформації, інформаційну безпеку та подання результатів дослідження. Після того, як первинна інформація з відкритих джерел пройде аналіз та обробку, вона може стати корисною і ,якщо ця інформація не відноситься до категорії, що є державною таємницею, вона може бути розголошена [2].

Щоб максимізувати ефективність OSINT, вкрай важливо застосовувати різноманітні методи та використовувати відповідні інструменти. Ці техніки можна умовно розділити на пасивні та активні [3].

Пасивні OSINT-методи передбачають збір інформації без безпосереднього звернення до джерел, використовуючи інформацію, доступну для загального ознайомлення.

Деякі поширені методи включають:

1. Аналіз соціальних мереж: Facebook, Twitter, LinkedIn, Instagram та інші. Аналізуючи профілі користувачів, публікації та зв'язки, аналітики можуть отримати цінну інформацію про людей, організації та тенденції.

2. Запити в пошукових системах Google, Bing, DuckDuckGo та інших. Використовуючи оператори розширеного пошуку такі як Google Dork можливо уточнювати пошуки та отримувати цільову інформацію.

3. Дослідження веб-сайтів і доменів є важливою частиною методів OSINT і може надати цінну інформацію про підприємства, організації чи навіть окремих користувачів. Такі методи, як записи WHOIS, аналіз IP-адрес і веб-скрапінг, можуть розкрити важливу інформацію.

Активні методи OSINT передбачають безпосередню взаємодію з джерелами та активний збір даних, а також вимагають від користувача значних зусиль, в тому числі фінансових витрат.

До таких методів належать:

1. Сканування веб-сайтів та індексація каталогів що включає безпосередню взаємодію з веб-сайтами шляхом сканування їх структури, пошуку вразливостей та визначення характеристик, таких як доступні служби чи ресурси.

2. Звернення до джерел із запитами про інформацію ВКЛЮЧАЮЧИ направлення запитів до компаній, організацій або громадських установ для отримання конкретної інформації.

3. Активне спостереження і взаємодія в соціальних мережах. Цей підхід передбачає безпосереднє спостереження за активністю користувачів у соціальних мережах та взаємодію з ними для отримання додаткової інформації.

4. Тестування на проникнення та збір інформації про безпеку мережі передбачає активне тестування систем та мереж на предмет наявності потенційних вразливостей шляхом спроби проникнення в них.

5. Дослідження публічних архівів, таких як судові документи, реєстрація бізнесу та майнові записи, що надають цінну інформацію про окремих осіб, організації та їх діяльність.

6. Аналіз зображень і відео, що часто містять цінну інформацію, яка може сприяти збору розвідувальних даних. Такі методи, як реверсивний пошук зображень, аналіз метаданих і відеокриміналістика, допомагають отримати інформацію з візуального вмісту.

У розслідуванні кіберінцидентів OSINT відіграє важливу роль, допомагаючи: ідентифікувати зловмисників; визначити інструменти та методи які використовуються зловмисниками, та способи захисту від них; зібрати докази; моніторити кіберзагрози.

Хоча OSINT є потужним інструментом для розслідування кіберзлочинів та забезпечення кібербезпеки, його використання вимагає уважного

врахування етичних аспектів. Якість отриманих даних не завжди є достатньою, що потребує критичного аналізу та перевірки. Крім того, використання Open Source Intelligence може порушувати юридичні обмеження, особливо у випадках, коли стосується конфіденційної інформації або національної безпеки. Отже, при використанні OSINT необхідно дотримуватися етичних принципів та враховувати можливі ризики і обмеження, щоб забезпечити ефективність та законність проведених дій [4].

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Мамедова Л.Ш. Особливості використання спеціальних знань під час розслідування кіберзлочинів: міжнародний досвід. Юридичний науковий електронний журнал. 2021. № 12. С. 392–395. URL: https://doi.org/10.32782/2524-0374/2021-12/99 (дата звернення: 09.04.2024).

2. Електронна енциклопедія Wikipedia. Українськомовна версія URL: https://uk.wikipedia.org/w/index.php?title=Розвідка_на_основі_відкритих_джерел&stable=0 (дата звернення: 09.04.2024)

3. THE OSINT FRAMEWORK: UNVEILING THE ART OF INFORMATION GATHERING URL: https://www.pvt365.net/the-osint-framework-unveiling-the-art-of-information-gathering (дата звернення: 09.04.2024).

4. Open Source Intelligence (OSINT): A Powerful Tool for Information Gathering URL: https://www.linkedin.com/pulse/open-source-intelligence-osint-powerful-tool-information-t-w96pc (дата звернення: 09.04.2024)

Зав. кафедри Андрій КОРОТУН

Відповідальний на факультеті Станіслав ШАПТАЛА

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ЗАПОРІЗЬКА ПОЛІТЕХНІКА»
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ РАДІОЕЛЕКТРОНІКИ

ПАТ «УКРТЕЛЕКОМ» **КП «НВК «ІСКРА»**

НВП «ХАРТРОН-ЮКОМ» **ТОВ «ІНФОКОМ ЛТД»**

СУЧАСНІ ПРОБЛЕМИ І ДОСЯГНЕННЯ В ГАЛУЗІ РАДІОТЕХНІКИ, ТЕЛЕКОМУНІКАЦІЙ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

КОНФЕРЕНЦІЯ ПРИСВЯЧЕНА 125-РІЧЧЮ З ДНЯ ЗАСНУВАННЯ НАЦІОНАЛЬНОГО УНІВЕРСИТЕТУ «ЗАПОРІЗЬКА ПОЛІТЕХНІКА»

Тези доповідей

XII Міжнародної науково-практичної конференції
(10–12 грудня 2024 р., м. Запоріжжя)

Co-funded by the Erasmus+ Programme of the European Union

Запоріжжя – 2024

підкомітет, який виконує підтвердження транзакцій. Причому це підтвердження відбувається у кілька етапів, на кожному з яких вибирається свій підкомітет. Протокол гарантує з високою ймовірністю, близькою до одиниці, що підкомітет є чесним, якщо більше ⅔ учасників мережі є чесними, тобто кожен із підкомітетів також матиме ⅔ чесних учасника. Тут немає лідера, тому немає точки для атаки типу «відмова в обслуговуванні» (DoS-атаки). Цей протокол забезпечує високу пропускну спроможність облікової системи, швидке підтвердження транзакцій та захист від атаки «adaptive corruption».

Подальшого дослідження потребують такі протоколи: Ouroboros, BFT-Smart, Honeybadger BFT, SBFT, GPBFT, Red Belly, Tendermint, HotStuff, PaLa, Fast-HotStuff, Streamlet, Polygraph, DAG, Avalanche. Важливо зазначити, що розглянуті протоколи консенсу мають свої переваги та обмеження, а вибір протоколу залежить від конкретного випадку використання, цілей мережі та компромісів між такими факторами, як безпека, масштабованість, децентралізація та енергоефективність. Різні блокчейн-проекти можуть вибирати різні консенсусні протоколи на основі своїх конкретних вимог і пріоритетів.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System, 2008.
2. Miguel Castro and Barbara Liskov, Practical Byzantine Fault Tolerance//3rd Symposium on Operating Systems Design and Implementation (OSDI 99) New Orleans, LA, 1999.
3. Baird, L. The Swirlds Hashgraph Consensus Algorithm: Fair, Fast, Byzantine Fault Tolerance, 2016, http://www.swirlds.com/downloads/SWIRLDS-TR-2016-01.pdf
4. Build the future on Algorand [Електронний ресурс] - режим доступу: https://developer.algorand.org

УДК 004.056
Піківець Г.М.[1], Корольков Р.Ю.[2]
[1] студ. гр. БКз-813м НУ «Запорізька політехніка»
[2] доц. кафедри інформаційної безпеки та наноелектроніки, НУ «Запорізька політехніка»

ЗАБЕЗПЕЧЕННЯ АНОНІМНОСТІ АНАЛІТИКІВ ПІД ЧАС OSINT-РОЗСЛІДУВАНЬ

У сучасному світі, де відкриті джерела інформації (OSINT) стали важливим інструментом для розслідувань, питання анонімності аналітиків

набуває критичного значення [1]. Збір і аналіз даних з відкритих джерел охоплюють різноманітні платформи — від соціальних мереж до баз даних, доступних у відкритому доступі. Це створює додаткові ризики для аналітиків, які можуть стикатися з кіберзагрозами, ризиком розкриття особистих даних або тиском з боку тих, хто може бути об'єктом досліджень. Можна виділити наступні ризики. Перший — юридично-правовий. Слід розуміти, що не всі інструменти, які використовуються для розслідувань, є легальними: деякі програми можуть порушувати закони про конфіденційність або доступ до особистої інформації. Перед застосуванням будь-якого інструменту варто перевірити, чи відповідає його використання чинному законодавству. Другий ризик — фізичний. Розслідування, що стосуються впливових осіб, можуть бути небезпечними, оскільки такі особи можуть вдаватися до погроз або навіть застосовувати фізичне насильство [2]. З огляду на це, важливо діяти з максимальною обережністю та забезпечувати свою анонімність. Третій ризик — цифровий, який можна поділити на такі ризики як деанонімізація та зараження пристроїв шкідливим програмним забезпеченням. Використання персональної електронної пошти, телефонного номера, справжньої IP-адреси або банківської картки для розслідувань є недоцільним, оскільки це може значно спростити ідентифікацію аналітика з OSINT-розвідки. Програми з шкідливим програмним забезпеченням, або "віруси", можуть потрапити на пристрій, якщо завантажити файл з ненадійного джерела, перейти за підозрілим посиланням або встановити неліцензійне програмне забезпечення. У результаті стороння особа може отримати віддалений доступ до пристрою аналітика з OSINT-розвідки без йщго відома. Крім того, пристрій може бути уражений вірусом-шифрувальником, який зашифрує всі файли, що унеможливить їх відновлення. Тому важливо бути обережним із підозрілими файлами та посиланнями для мінімізації ризику зараження [3].

Для забезпечення анонімності під час OSINT-розслідувань важливо застосовувати комплекс стратегій, які допоможуть захистити особисту інформацію аналітика та мінімізувати ризики ідентифікації [4].

Перш за все, перед початком роботи треба підготувати окремі облікові записи під псевдонімами в соціальних мережах та на інших платформах [5], які використовуються для збору даних та телефонні номери та налаштувати робоче середовище на пристрої таким чином, щоб зберігати анонімність та захищати персональні дані.

Також, щоб мінімізувати ризик випадкового розкриття особистих даних, аналітики повинні працювати в ізольованому робочому середовищі. Це дозволяє відділити потенційно небезпечні завдання від основної операційної системи, зменшуючи ризик інфікування шкідливим програмним забезпеченням або випадкового витоку даних. Завдяки цьому підходу

аналітик може працювати з неперевіреними файлами, підозрілими сайтами та іншими небезпечними джерелами інформації, не піддаючи ризику основний комп'ютер.

Програмне забезпечення для віртуалізації надає широкі можливості налаштувань для створення окремих, ізольованих середовищ. VirtualBox, як програмний продукт з відкритим вихідним кодом, є одним із найпопулярніших варіантів, що дає змогу використовувати декілька операційних систем паралельно на одному пристрої. Його відкритий код забезпечує прозорість і дозволяє спільноті здійснювати аудит безпеки програми. VMware Workstation Pro, у свою чергу, є надійним та продуктивним рішенням, яке пропонує високий рівень підтримки та інтеграції, а також різноманітні функції для захисту конфіденційності й анонімності.

Крім того, при роботі в ізольованому середовищі аналітик має змогу створювати та відновлювати "знімки" (snapshots) системи, що забезпечує можливість швидкого повернення до попереднього стану в разі компрометації віртуальної машини або появи непередбачених проблем. Це значно підвищує ефективність роботи і знижує ризики втрати важливих даних або розкриття особистої інформації.

Другим кроком є використання певних браузерів, які можна використовувати для різних задач, та віртуальних приватних мереж (VPN). Браузер від компанії Google Chrome відомий своєю зручністю, швидкістю та стабільністю, регулярно отримує оновлення та має велику кількість розширень, крім того може створювати окремі профілі щоб розділити персональне використання та робоче візуально. Дуже добре реалізовано питання безпеки, кожна вкладка, плагін або розширення працюють у своєму власному ізольованому середовищі – це, так звана, технологія пісочниці. Головним недоліком Google Chrome є питання конфіденційності компанія збирає забагато даних про своїх користувачів через що важче забезпечити анонімність в роботі. Firefox від компанії mazilla у свою чергу приділяє більше уваги питанню конфіденційності та приватності на відміну від Chrome, за замовченням блокує рекламні трекери та має відкритий код, є технологія пісочниці однак вона не настільки добре реалізована як у Google Chrome. Браузер Tor є одним із найпопулярніших браузерів для анонімного доступу до інтернету. Він маршрутизує трафік через кілька серверів (вузлів), що дозволяє приховати IP-адресу та геолокацію користувача, дозволяє обходити цензуру, а також має вбудований захист від стеження. Його недоліком є зниження швидкості підключення через багаторівневий процес маршрутизації та варто пам'ятати що він орієнтований на анонімність а не на безпеку.

VPN є ефективним інструментом для захисту приватності та безпеки в інтернеті. Він приховує справжню IP-адресу користувача, що ускладнює визначення його геолокації, а також шифрує дані, забезпечуючи безпечне з'єднання навіть при використанні публічних Wi-Fi мереж. Крім того, VPN надає доступ до контенту, заблокованого у певних регіонах.

Варто зазначити, що VPN-розширення в браузері захищає тільки трафік, який проходить через цей браузер, тоді як окремий VPN-додаток забезпечує шифрування всього інтернет-трафіку на пристрої користувача. При виборі VPN-сервісу доцільно звертати увагу на такі важливі аспекти, як політика No logs (відсутність реєстрації активності користувача), використання надійного алгоритму шифрування (наприклад, AES-256), підтримка сучасних безпечних протоколів (таких як OpenVPN, IKEv2, WireGuard), а також наявність функції Kill Switch, яка забезпечує автоматичне відключення від інтернету у разі втрати VPN-з'єднання.

Для забезпечення безпеки під час OSINT-розслідувань важливо використовувати надійне шифрування для захисту даних, що зберігаються чи передаються. Існує три основні способи зберігання даних: на комп'ютері, у хмарних сервісах та на зовнішніх накопичувачах. Для зберігання на комп'ютері необхідно захистити пристрій як від віддалених загроз (ліцензійне ПЗ, антивіруси, регулярне оновлення системи), так і від фізичних (пароль на вхід, шифрування диска, збереження ключа шифрування). Вбудовані механізми шифрування, такі як BitLocker на Windows, FileVault на macOS та LUKS на Linux, часто потребують активації.

Для збереження даних резервні копії можна зберігати окремо — у хмарі чи на зовнішніх носіях (USB, HDD, SSD). Хмарні сервіси (Google Диск, Dropbox, OneDrive, iCloud) забезпечують певний безкоштовний обсяг сховища, але вимагають надійних паролів та двофакторної автентифікації. Для зовнішніх накопичувачів також рекомендоване шифрування з паролем.

Таким чином, в умовах сучасних ризиків, анонімність є запорукою безпеки аналітиків під час OSINT-розслідувань, дозволяючи працювати незалежно та ефективно. Забезпечення конфіденційності стає комплексним процесом, який включає застосування віртуалізованих середовищ, спеціалізованих браузерів та VPN-засобів, шифрування даних, а також дотримання етичних стандартів та обізнаність у галузі інформаційної безпеки [6]. Надійна організація процесів зберігання й захисту даних, зокрема резервне копіювання та шифрування зовнішніх носіїв, значно знижує ризик компрометації або витоку конфіденційної інформації, захищаючи аналітиків від кіберзагроз та мінімізуючи небезпеку ідентифікації. Реалізація цих заходів сприяє безпечній і ефективній роботі аналітиків, відповідаючи на виклики сучасного інформаційного простору та зміцнюючи захист особистих даних у процесі розслідувань.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. González-Manzano, L. A Primer on Open Source Intelligence (OSINT) Leveraging Existing Tools. Primer Congreso del Espacio y Ciberespacio EMAVI 2020 – Мадрид: Мадридський університет Карлоса III, 2020 – 8с. URL: https://e-archivo.uc3m.es/bitstreams/c382872a-f774-4880-8be8-02a4d6406c77/download (дата звернення: 01.11.2024)

2. Торбас О.О. OSINT при розслідуванні кримінальних правопорушень : підручник - Одеса : Видавництво «Юридика», 2024. - 180с. URL: https://dspace.onua.edu.ua/bitstreams/106c5467-2afb-4055-a0fb-3a500102db9c/download (дата звернення: 01.11.2024)

3. ESET. URL: Дослідження на основі відкритих джерел або OSINT: де використовується та в чому небезпека – 2021. URL: http://surl.li/mvddej (дата звернення: 04.11.2024)

4. OSINT Industries Team. Scrubbing Up On OSINT Cyber Hygiene (Best Practices) – 2024. URL: https://www.osint.industries/post/scrubbing-up-on-osint-cyber-hygiene-best-practices (дата звернення: 04.11.2024)

5. Narasimhan, P. K., Bhosale, C., Pervez, M. H., Naqvi, N. Z., Ecevit, M. I., Schwarz, K., & Creutzburg, R. Open-Source Intelligence (OSINT) Investigation in Facebook - IS&T International Symposium on Electronic Imaging 2023, Mobile Devices and Multimedia: Enabling Technologies, Algorithms, and Application, 2023. URL: https://library.imaging.org/admin/apis/public/api/ist/website/downloadArticle/ei/35/3/MOBMU-357 (дата звернення: 04.11.2024)

6. Гузій І. 21 правило цифрової безпеки: Європейський Простір – 2018. URL: https://euprostir.org.ua/practices/133410 (дата звернення: 04.11.2024)

УДК 003.26:004.056.53

Пономаренко Є. О.[1], Неласа Г. В.[2]
[1]асп. каф. ІБтаН НУ «Запорізька політехніка»
[2]доц. каф. ІБтаН НУ «Запорізька політехніка»

АНАЛІЗ МОЖЛИВОСТЕЙ ВИКОРИСТАННЯ ІЗОГЕНІЙ ГІПЕРЕЛІПТИЧНІ КРИВИХ ДРУГОГО РОДУ У КРИПТОГРАФІЧНИХ ПРОТОКОЛАХ

Гіпереліптичні криві другого роду[1] стали важливим компонентом сучасної криптографії, надаючи можливість ефективного захисту в умовах зростаючих загроз з боку квантових обчислень. Ізогенії гіпереліптичні кривих другого роду визначають відображення між гіпереліптичними кривими зі збереженням їхньої математичної структури, що має важливе значення в криптографічних системах. Порівняно з еліптичними кривими,

ДОДАТОК Б

Сертифікати про підвищення кваліфікації

Виданий 19.10.2024

СЕРТИФІКАТ

Цей сертифікат засвідчує, що

Ганна Піківець

успішно закінчив(ла) курс

«OSINT — розвідка з відкритих джерел та інформаційна безпека»

Курс розроблено командою проєкту Victory Drones Благодійного фонду Dignitas за підтримки партнерів проєкту

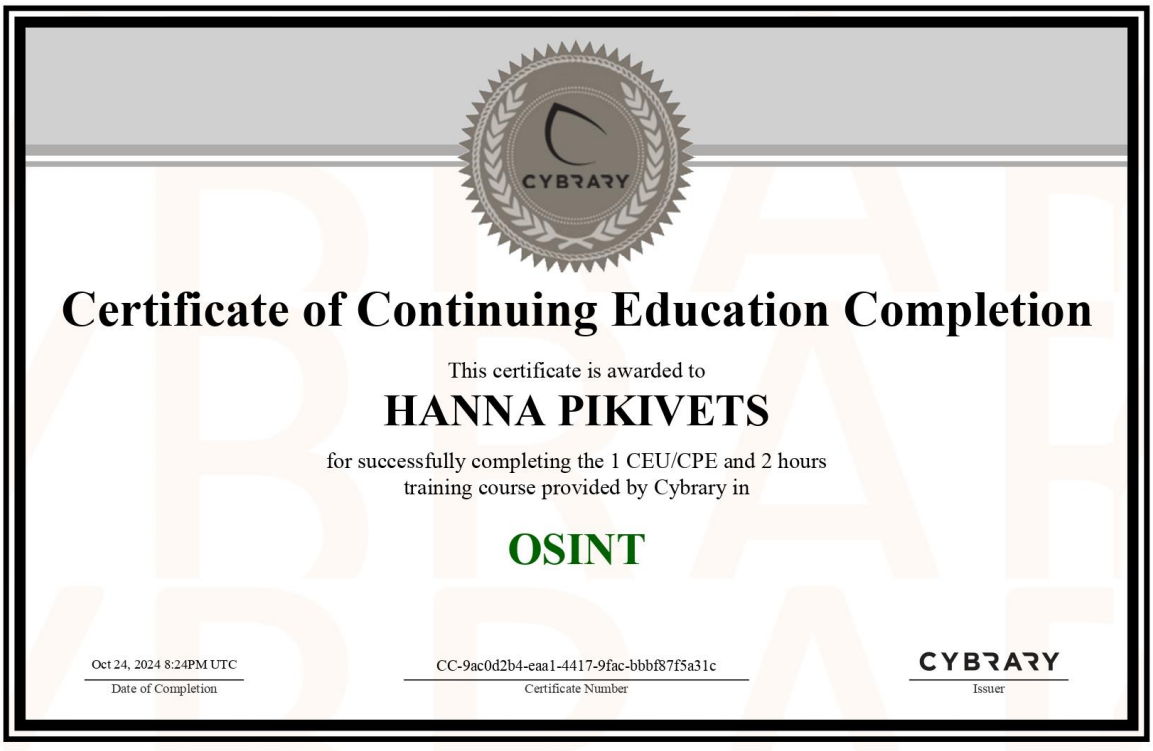
Марія Берлінська
Упорядниця та ініціаторка створення курсу

Автентичність сертифіката можна перевірити за посиланням:
https://certs.prometheus.org.ua/cert/6af1cce41e8d40fbad78c6569e8d53c8

DIGNITAS БЛАГОДІЙНИЙ ФОНД

VICTORY DRONES

PROMETHEUS



CYBRARY

Certificate of Continuing Education Completion

This certificate is awarded to

HANNA PIKIVETS

for successfully completing the 1 CEU/CPE and 2 hours training course provided by Cybrary in

OSINT

Oct 24, 2024 8:24PM UTC	CC-9ac0d2b4-eaa1-4417-9fac-bbbf87f5a31c	CYBRARY
Date of Completion	Certificate Number	Issuer

Official Cybrary Certificate - CC-9ac0d2b4-eaa1-4417-9fac-bbbf87f5a31c

Does not represent certification by any certifying body