

Міністерство освіти і науки України
Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки

ПОЯСНЮВАЛЬНА ЗАПИСКА

до випускної кваліфікаційної роботи бакалавра
на тему: «Методи, техніки та інструменти OSINT для
розслідування кіберінцидентів»

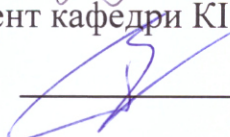
Виконав: студент 4-го курсу групи КБ-21-2
спеціальності 125 «Кібербезпека»

 Віктор НОВИЦЬКИЙ

Керівник: старший викладач кафедри КІ та КБ

 Олександра ПОКОТИЛО

Рецензент: доцент кафедри КІ та КБ, к.т.н.

 Олександр ПІРОГ

Житомир – 2025

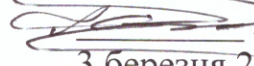
Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки
Спеціальність 125 «Кібербезпека»
Освітня програма «Кібербезпека»

ЗАТВЕРДЖУЮ

Завідувач

кафедри комп'ютерної

інженерії та кібербезпеки

 Андрій Єфіменко
3 березня 2025 р.

ЗАВДАННЯ

на випускн кваліфікаційну роботу бакалавра

Студент: Новіцький Віктор Сергійович

Тема роботи: «Методи, техніки та інструменти OSINT для розслідування кіберінцидентів»

затверджена Наказом університету від 3 березня 2025 р. № 80/с

Термін здачі студентом закінченої роботи 24 червня 2025 р.

Вихідні дані роботи (зазначається предмет і об'єкт дослідження):
Об'єктом дослідження є процес розслідування кіберінцидентів з використанням відкритих джерел інформації. Предметом дослідження є методи, техніки та інструменти OSINT, що застосовуються для збору, аналізу та інтерпретації інформації під час розслідування кіберінцидентів.

Обладнання та програмне забезпечення:

1. TraceLabs OSINT VM
2. Maltego CE
3. Recon-ng
4. Holehe
5. Nmap
6. Tor Browser
7. Windscribe

Консультанти з випускної кваліфікаційної роботи із зазначенням розділів, що їх стосуються

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Пірог О.В.	27.03.2025	27.03.2025
2	Пірог О.В.	15.04.2025	15.04.2025
3	Пірог О.В.	10.05.2025	10.05.2025

Студент  Віктор НОВІЦЬКИЙ

Керівник  Олександра ПОКОТИЛО

Календарний план

№ з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка завдання	03.03.2025	Виконано
2	Аналіз методів OSINT	04.03.2025 - 20.03.2025	Виконано
3	Опрацювання літературних джерел	21.03.2025 - 04.04.2025	Виконано
4	Пошук програмного забезпечення	05.04.2025 - 14.04.2025	Виконано
5	Налагодження робочого середовища	15.04.2025 - 22.04.2025	Виконано
6	Розслідування кіберінциденту розсилки фішингового листа	23.04.2025 - 01.05.2025	Виконано
7	Збір інформації про IP-адресу	02.05.2025 - 14.05.2025	Виконано
8	Аналіз зображення камери відеоспостереження	15.05.2025 - 28.05.2025	Виконано
9	Написання пояснювальної записки	29.05.2025 - 17.06.2025	Виконано
10	Отримання відгуку та рецензії		
11	Захист	24.06.2025	

Студент  Віктор НОВІЦЬКИЙ

Керівник  Олександра ПОКОТИЛО

АНОТАЦІЯ

Кваліфікаційна робота на тему «Методи, техніки та інструменти OSINT для розслідування кіберінцидентів» включає вступ, три розділи, висновки, список використаних джерел та додатки.

Текстова частина займає 65 сторінок друкованого тексту.

До пояснювальної записки входить список із 26 використаних джерел, що займають 3 сторінок. У роботі представлено 45 рисунків, загальний обсяг – 66 сторінок.

Завданням кваліфікаційної роботи є:

- дослідження концепції OSINT та його застосування у сфері кібербезпеки;
- аналіз технік та інструментів збору відкритих даних;
- вивчення правових аспектів використання OSINT;
- створення безпечного середовища для проведення OSINT-розслідувань;
- практичне застосування OSINT у дослідженні кіберінцидентів.

Перший розділ містить теоретичні відомості щодо природи OSINT, його класифікації, нормативно-правових аспектів використання відкритої інформації, а також ролі в системі кібербезпеки.

У другому розділі описано основні інструменти OSINT, такі як Holehe, Maltego, Recon-ng, Whois, Nmap, VirusTotal, VPNAPI.io, а також сервіси Google, які використовуються у процесі збору, аналізу та верифікації відкритих даних.

У третьому розділі змодельовано три практичні сценарії OSINT-розслідувань: фішингова атака через електронну пошту та шкідливий сайт, аналіз IP-адреси можливого зловмисника, а також визначення геолокації камери відеоспостереження на основі візуальних ознак і картографічних сервісів.

Ключові слова: OSINT, КІБЕРІНЦИДЕНТ, РОЗСЛІДУВАННЯ, ВІДКРИТІ ДЖЕРЕЛА, ДОСЛІДЖЕННЯ, ІНСТРУМЕНТИ, ЗБІР ІНФОРМАЦІЇ.

					KKIK.KP.B – 125 – 33 – ПЗ			
Змн.	Арк.	№ докум.	Підпис	Дата	Методи, техніки та інструменти OSINT для розслідування кіберінцидентів	Лім.	Арк.	Аркушів
Розроб.		Новіцький В.С.		18.06.25				
Керівник		Покотило О.А.		18.06.25			4	66
Реценз.		Пірог О.В.		18.06.25				
Н. контр.		Покотило О.А.		18.06.25				
Затверд.		Єфіменко А.А.		18.06.25		ФІКТ, Гр. КБ-21-2		

ANNOTATION

The qualification work on the topic "Methods, Techniques, and Tools of OSINT for Cyber Incident Investigation" includes an introduction, three chapters, conclusions, a list of references, and appendices.

The text portion consists of 65 pages of printed text.

The explanatory note includes a list of 26 sources, spanning 3 pages. The work contains 45 figures, with a total volume of 66 pages.

The tasks of the qualification work are:

- To explore the concept of OSINT and its application in the field of cybersecurity;
- To analyze techniques and tools for collecting open-source data;
- To study the legal aspects of using OSINT;
- To create a secure environment for conducting OSINT investigations;
- To demonstrate the practical application of OSINT in cyber incident investigations.

The first chapter contains theoretical information about the nature of OSINT, its classification, the legal framework for the use of open data, and its role in the cybersecurity system.

The second chapter describes the main OSINT tools such as Holehe, Maltego, Recon-ng, Whois, Nmap, VirusTotal, VPNAPI.io, as well as Google services used in the processes of data collection, analysis, and verification.

The third chapter presents three practical OSINT investigation scenarios: a phishing attack via email and a malicious website, analysis of a suspected attacker's IP address, and identification of the physical location of a surveillance camera based on visual clues and mapping services.

Keywords: OSINT, CYBER INCIDENT, INVESTIGATION, OPEN SOURCES, ANALYSIS, TOOLS, INFORMATION GATHERING.

		Новіцький В.С.			ККІКБ.КР.Б – 125 – 33 – ПЗ	Арк.
		Покотило О.А.				5
Змн.	Арк.	№ докум.	Підпис	Дата		

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ.....	7
ВСТУП.....	8
РОЗДІЛ 1 ТЕОРЕТИЧНІ АСПЕКТИ ВИКОРИСТАННЯ OSINT.....	9
1.1 Визначення та класифікація OSINT.....	9
1.1.1 Історія розвитку та основні поняття OSINT	9
1.1.2 CYBERINT	12
1.1.3 GEOINT	13
1.1.4 IMGINT.....	14
1.2 Нормативно-правові аспекти OSINT	16
1.3 Порівняння OSINT з іншими видами розвідки.....	18
РОЗДІЛ 2 ПРАКТИЧНІ ІНСТРУМЕНТИ ТА РЕСУРСИ ДЛЯ OSINT	22
2.1 Віртуалізація як засіб безпечного збору даних	22
2.1.1 Програмне забезпечення VirtualBox.....	22
2.1.2 Віртуальна машина Trace Labs.....	23
2.1.3 VPN як інструмент захисту віртуалізованого середовища	25
2.2 Інструменти та веб-сервіси для збору OSINT.....	27
2.3 Використання інтернет-ресурсів Google	35
РОЗДІЛ 3 ПРАКТИЧНЕ ЗАСТОСУВАННЯ OSINT.....	38
3.1 Підготовка віртуального середовища	38
3.2 Аналіз фішингового електронного листа	42
3.3 Отримання інформації про IP-адресу	49
3.4 Визначення локації за IP-камерою відеоспостереження	54
3.5 Узагальнення результатів OSINT-розслідувань	57
ВИСНОВКИ.....	61
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ	62
ДОДАТКИ.....	65

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

OSINT – Open Source Intelligence
GEOINT – Geospatial Intelligence
IMGINТ – Imagery Intelligence
CYBERINT – Cyber Intelligence
HUMINT – Human Intelligence
VPN – Virtual Private Network
IP – Internet Protocol
DNS – Domain Name System
SOC – Security Operations Center
CERT – Computer Emergency Response Team
FTP – File Transfer Protocol
SSH – Secure Shell
CTI – Cyber Threat Intelligence
VB – Virtual Box
VM – Virtual Machine
TL – Trace Labs
QGIS – Quantum GIS
GPS – Global Positioning System
TLVM – Trace Labs Virtual Machine
GDPR – General Data Protection Regulation
GIS – Geographic Information System
ASN – Autonomous System Number
NMAP – Network Mapper
API – Application Programming Interface
ICMP – Internet Control Message Protocol

		Новіцький В.С.			ККІКБ.КР.Б – 125 – 33 – ПЗ	Арк.
		Покотило О.А.				7
Змн.	Арк.	№ докум.	Підпис	Дата		

ВСТУП

Актуальність теми. З розвитком цифрових технологій та збільшенням кількості кіберзагроз особливої важливості набуває ефективне виявлення та розслідування кіберінцидентів. OSINT як метод збору та аналізу відкритої інформації стає ефективним інструментом для забезпечення кібербезпеки. Використання сучасних OSINT-технік і інструментів дозволяє швидко ідентифікувати джерела атак, проводити глибокий аналіз мережевих подій, а також визначати геолокацію і атрибути зловмисників. Водночас важливим є вивчення нормативно-правових аспектів застосування відкритих даних, що забезпечує легітимність та етичність розслідувань.

Метою кваліфікаційної роботи є дослідження методів, технік і інструментів OSINT для розслідування кіберінцидентів з практичною демонстрацією їх застосування на прикладі моделювання реальних сценаріїв.

Визначена мета обумовлює наступні завдання:

- дослідити концептуальні основи OSINT і його роль у кібербезпеці;
- проаналізувати основні техніки та інструменти збору відкритої інформації;
- ознайомитися з нормативно-правовою базою, що регламентує застосування OSINT;
- змодельовати практичні сценарії OSINT-розслідувань кіберінцидентів;
- провести аналіз отриманих результатів та сформулювати рекомендації щодо подальшого застосування.

Об’єктом дослідження є процес збору, аналізу та верифікації відкритих даних у контексті розслідування кіберінцидентів.

Предметом дослідження є методи, техніки та програмні засоби OSINT, а також нормативно-правові аспекти їх застосування у сфері кібербезпеки.

У процесі виконання кваліфікаційної роботи було розроблено комплекс практичних сценаріїв OSINT-розслідувань, що демонструють ефективність застосування відкритих джерел для аналізу фішингових атак, визначення IP-адреси зловмисника та геолокації камери відеоспостереження.

		Новіцький В.С.			ККІКБ.КР.Б – 125 – 33 – ПЗ	Арк.
		Покотило О.А.				8
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 1 ТЕОРЕТИЧНІ АСПЕКТИ ВИКОРИСТАННЯ OSINT

1.1 Визначення та класифікація OSINT

1.1.1 Історія розвитку та основні поняття OSINT

OSINT – це процес збору, аналізу та інтерпретації інформації з відкритих джерел, доступних для широкого кола осіб. Ці джерела можуть включати публічні записи, новини, наукові публікації, соціальні мережі, форуми, вебсайти та інші електронні ресурси. Відкрите джерело в контексті OSINT означає будь-яку інформацію, яку можна отримати без спеціального дозволу та без використання закритих або конфіденційних джерел. Цей метод дозволяє збирати та використовувати дані, що є доступними без порушення законодавства, а також без використання спеціальних технічних засобів[1].

Поява OSINT як окремої галузі аналітики пов'язана з розвитком інформаційних технологій та інтернету в кінці 20-го століття[3]. У 1990-х роках, коли доступ до мережі Інтернет став більш широким і популярним, збір інформації з відкритих джерел став доступним для більшої кількості людей і організацій. Поява таких інструментів, як пошукові системи, соціальні мережі та вебсайти з публічними даними, сприяла швидкому розвитку OSINT. Від початкового використання для розвідки та військових цілей, OSINT сьогодні охоплює різні сфери, включаючи правоохоронну діяльність, бізнес-аналіз, журналістику, а також моніторинг соціальних медіа(рис. 1.1).

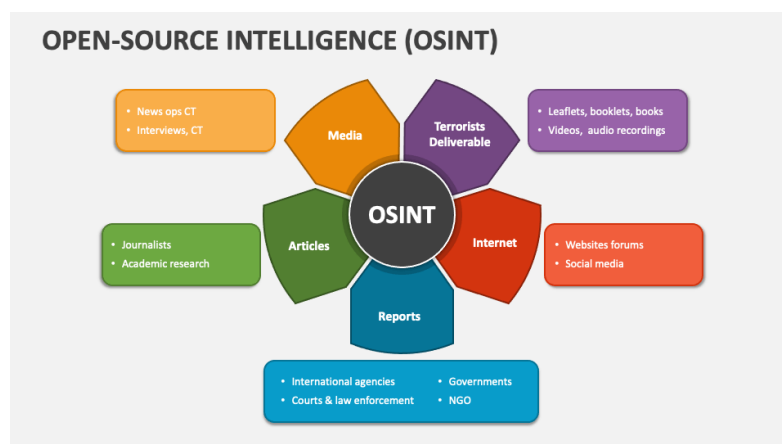


Рис. 1.1 - Сфери застосування OSINT

		Новіцький В.С.			ККІКБ.КР.Б – 125 – 33 – ПЗ	Арк.
		Покотило О.А.				9
Змн.	Арк.	№ докум.	Підпис	Дата		

Завдяки швидкому розвитку інтернет-технологій та глобалізації доступ до відкритої інформації значно збільшився[1]. Це створює нові можливості для ефективного використання OSINT у різних сферах, таких як національна безпека, розслідування, бізнес-аналіз та багато інших.

У сучасному світі потреба у використанні OSINT зростає, оскільки кількість доступної для загального користування інформації збільшується з кожним роком. Завдяки цьому організації та державні структури отримують нові можливості для прийняття обґрунтованих рішень, що базуються на актуальних даних. Збір інформації з відкритих джерел дає змогу більш ефективно реагувати на поточні події, відстежувати нові загрози та визначати можливі ризики для безпеки[16].

Однією з основних потреб у використанні OSINT є забезпечення національної безпеки, де доступ до відкритих даних дозволяє виявляти терористичні загрози, діяльність потенційних ворогів або інших груп, що можуть створити небезпеку для держави. Окрім того, OSINT використовується в розслідуваннях правопорушень, де відкриті джерела допомагають виявляти злочинців, збирати докази та відслідковувати незаконну діяльність[5].

Для бізнесу OSINT є важливим інструментом для аналізу ринку, конкурентів та споживчих уподобань. Компанії використовують дані з відкритих джерел для моніторингу змін на ринку та коригування своєї стратегії відповідно до зовнішніх умов.

Використання OSINT також є важливим для журналістів та медіа, оскільки дозволяє перевіряти факти, збирати інформацію для розслідувань та виявляти фальшиві новини або дезінформацію[2].

OSINT застосовується в багатьох сферах, де є потреба в аналізі великих обсягів відкритої інформації для ухвалення рішень. Однією з основних сфер є національна безпека та розвідка. Відкриті джерела дозволяють відстежувати діяльність терористичних груп, політичну ситуацію в різних країнах, а також загрози на зовнішніх кордонах держави. Інформація з відкритих джерел допомагає оперативно виявляти та нейтралізувати потенційні загрози для безпеки країни.

		Новіцький В.С.			ККІКБ.КР.Б – 125 – 33 – ПЗ	Арк.
		Покотило О.А.				10
Змн.	Арк.	№ докум.	Підпис	Дата		

У правоохоронній діяльності OSINT також має важливе значення, оскільки правоохоронні органи використовують відкриті джерела для розслідування злочинів, пошуку осіб та збору доказів[5]. Це допомагає виявляти схеми шахрайства, боротьбі з кіберзлочинністю та іншими правопорушеннями.

У бізнес-аналізі OSINT є ефективним інструментом для збору інформації про ринок, конкурентів і потенційних партнерів. Це дозволяє компаніям прогнозувати зміни в економічній ситуації, визначати споживчі тренди та адаптувати свої стратегії під нові умови.

В журналістиці OSINT допомагає журналістам перевіряти факти, збирати інформацію для розслідувань та аналізувати ситуацію в реальному часі. Відкриті джерела надають можливість проводити незалежну перевірку подій, що дозволяє створювати більш об'єктивні та точні матеріали.

Екологічний моніторинг – ще одна важлива сфера застосування OSINT. Збір даних з відкритих джерел дозволяє відстежувати екологічні катастрофи, зміну клімату та інші важливі екологічні фактори, що можуть мати серйозний вплив на навколишнє середовище.

Для ефективного збору та аналізу інформації з відкритих джерел використовуються різноманітні інструменти. Ось деякі з них:

1. Геолокаційні сервіси[17] – платформи, такі як *Google Maps* або *OpenStreetMap*, дозволяють відслідковувати місцезнаходження об'єктів або осіб, що є важливим для аналізу ситуацій на місці подій чи для моніторингу переміщень.

2. Інструменти для зворотного пошуку зображень – сервіси *Google Lens* та інші дозволяють здійснювати пошук за фото, що допомагає ідентифікувати людей або виявляти джерела зображень, які використовуються в інтернеті.

3. Інструменти для аналізу мережевої інфраструктури – охоплюють засоби для дослідження IP-адрес, доменів, VPN-сервісів, відкритих портів, DNS-записів та інших аспектів мережевої активності. До них належать сервіси та утиліти, такі як Nmap, Recon-ng, Maltego, які дозволяють виявити активні пристрої, відстежити інфраструктуру атак, а також аналізувати цифрові сліди у відкритих джерелах.

		Новіцький В.С.			ККІКБ.КР.Б – 125 – 33 – ПЗ	Арк.
		Покотило О.А.				11
Змн.	Арк.	№ докум.	Підпис	Дата		

В OSINT існують різні методи збору інформації, які дозволяють аналізувати різноманітні типи даних з відкритих джерел. Одним з таких методів є GEOINT, який фокусується на геопросторових даних, таких як карти, супутникові знімки та інші просторові дані. GEOINT дозволяє здійснювати аналіз місцезнаходжень, переміщень і просторових взаємодій, що є корисним у розвідці, національній безпеці та навіть у бізнесі для прогнозування логістичних маршрутів або дослідження ринку[2].

Іншим важливим методом є IMGINT, що включає збір та аналіз зображень, таких як фотографії, супутникові знімки або відео. Цей метод допомагає у вивченні місцевості, об'єктів або інфраструктури, що може бути корисно в розслідуваннях, безпеці або вивченні змін на території.

CYBERINT зосереджується на зборі та аналізі технічної інформації, пов'язаної з кіберпростором, зокрема даних про шкідливу активність, вразливості, витоки, використання анонімних мереж, індикатори компрометації тощо. Цей напрям дозволяє ідентифікувати потенційні загрози, відстежувати діяльність хакерських груп, а також аналізувати цифрові сліди з метою запобігання або розслідування кіберінцидентів[6].

1.1.2 CYBERINT

CYBERINT – це процес збору, обробки та аналізу інформації з цифрового середовища з метою виявлення кіберзагроз, вразливостей, витоків даних, а також інших ознак злочинної активності в кіберпросторі. Основу CYBERINT складають технічні джерела: мережеві сканери, телеметрія з систем безпеки, результати OSINT-досліджень, а також дані з даркнету, форумів, ботнетів та репутаційних баз. Така інформація дозволяє виявити індикатори компрометації, пов'язані інфраструктури (IP, домени), а також методи та інструменти, які застосовуються атакувальниками[2].

До переваг CYBERINT належить здатність виявляти загрози до їх реалізації, що дає змогу запобігати інцидентам. Аналітика кіберзагроз дозволяє будувати

		Новіцький В.С.			ККІКБ.КР.Б – 125 – 33 – ПЗ	Арк.
		Покотило О.А.				12
Змн.	Арк.	№ докум.	Підпис	Дата		

профіль хакерських угруповань, визначати їхні цілі та техніки, а також відстежувати кампанії атак. Інформація, отримана за допомогою CYBERINT, є цінною для підрозділів кібербезпеки (SOC, CERT), слідчих органів, а також приватних компаній, які прагнуть захистити свою IT-інфраструктуру.

Серед основних труднощів використання CYBERINT – необхідність високого технічного рівня експертизи, обробка великих обсягів неструктурованих даних, а також проблеми з верифікацією отриманої інформації. Крім того, активне використання шифрування, VPN і анонімних мереж ускладнює ідентифікацію джерел атак і злочинців.

Для аналізу даних у CYBERINT широко застосовуються такі інструменти, як Maltego, який дозволяє візуалізувати зв'язки між IP-адресами, доменами та акаунтами[25]; Recon-ng – фреймворк для автоматизації OSINT-збірки[14]; Shodan і Censys – сканери Інтернету речей та сервісів; Nmap – для сканування портів та мережевих служб[18]; Holey – для перевірки акаунтів за email[26]. Допоміжні інструменти, як-от Have I Been Pwned, VirusTotal та IntelligenceX, дозволяють перевіряти витoki облікових даних, шкідливу активність та індексовані архіви[6].

1.1.3 GEOINT

GEOINT – це процес збору, аналізу та інтерпретації геопросторових даних для отримання розвідувальної інформації. Геопросторові дані охоплюють координати, карти, супутникові знімки, тривимірні моделі територій та інші ресурси, що описують просторові характеристики об'єктів. Такий підхід дозволяє аналізувати розташування, переміщення та взаємодію об'єктів у просторі, підтримуючи прийняття стратегічних та тактичних рішень завдяки візуалізації отриманої інформації[17].

Серед основних переваг GEOINT слід відзначити точність, яку забезпечують GPS-дані та супутникові знімки, з високою деталізацією й координатною прив'язкою. Візуалізація інформації у вигляді карт, моделей чи супутникових зображень значно полегшує аналіз складних даних, особливо у ситуаціях, що потребують швидкого реагування. Актуальність даних, які можуть оновлюватися в реальному

		Новіцький В.С.			ККІКБ.КР.Б – 125 – 33 – ПЗ	Арк.
		Покотило О.А.				13
Змн.	Арк.	№ докум.	Підпис	Дата		

часі, забезпечує оперативність у прийнятті рішень, наприклад, у кризових ситуаціях. GEOINT також має широкий спектр застосування: від військової розвідки до міського планування, моніторингу природних катастроф і навіть бізнес-аналітики.

Водночас є й недоліки. Ефективність GEOINT значною мірою залежить від доступу до сучасних супутникових систем і високих обчислювальних потужностей. Погодні умови, такі як хмарність, можуть ускладнювати отримання якісних знімків. Ще однією проблемою є висока вартість супутникових даних і програмного забезпечення. До того ж обмеження доступу до закритих джерел часто створює бар'єри для використання необхідної інформації.

Для роботи з геопросторовими даними доступні численні інструменти. Наприклад, Google Earth і Google Maps забезпечують доступ до супутникових знімків і карт, дозволяючи переглядати дані у високій роздільній здатності. QGIS (Quantum GIS) пропонує можливості для безкоштовного створення та аналізу географічних даних, тоді як ArcGIS є більш професійним інструментом, широко застосовуваним у науці, бізнесі й урядових установах. OpenStreetMap надає відкриті дані, створені користувачами, що є цінним ресурсом для громадських і дослідницьких проєктів. Sentinel Hub дозволяє працювати із супутниковими даними програми Copernicus, забезпечуючи доступ до великого обсягу актуальної інформації. Mapillary пропонує можливість збору та аналізу фотографій місцевості, що може бути корисним для вивчення конкретних локацій. Planet Labs є постачальником супутникових даних високої роздільної здатності, які використовуються для моніторингу змін на поверхні Землі[4].

1.1.4 IMGINT

IMGINT – це процес збору та аналізу візуальних даних, таких як фотографії, відео та супутникові знімки, для отримання розвідувальної інформації. Цей підхід дозволяє вивчати об'єкти, їхні характеристики та зміни у часі через візуальні спостереження. Завдяки IMGINT можна оцінювати стан інфраструктури, виявляти переміщення техніки або аналізувати наслідки природних чи техногенних катастроф[3].

		Новіцький В.С.			ККІКБ.КР.Б – 125 – 33 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		14

Перевагами IMGINT є:

Візуальна доступність: зображення дають можливість побачити об'єкти та території у їхньому реальному вигляді, що спрощує аналіз.

Моніторинг змін: IMGINT дозволяє відстежувати динаміку змін, наприклад, будівництво, пошкодження чи переміщення.

Широкий доступ: багато платформ надають відкритий доступ до зображень, зокрема супутникових, для аналітиків, дослідників і журналістів.

Глобальне охоплення: супутникові системи забезпечують можливість аналізу будь-якої точки планети.

Недоліками IMGINT є:

Обмеження якості зображень: погодні умови, низька роздільна здатність або тіні можуть ускладнювати аналіз.

Складність інтерпретації: аналіз зображень вимагає спеціальних знань та навичок.

Затримка у доступі до даних: деякі супутникові дані оновлюються із запізненням, що зменшує їхню актуальність.

Висока вартість якісних ресурсів: комерційні супутникові знімки часто коштують дорого, особливо для приватних користувачів.

IMGINT знаходить застосування у багатьох сферах:

Моніторинг конфліктних зон: аналіз супутникових знімків допомагає виявляти пересування військової техніки або зміну ландшафту через бойові дії.

Екологічні дослідження: IMGINT використовується для спостереження за змінами клімату, вирубкою лісів чи забрудненням територій.

Розслідування та журналістика: супутникові знімки часто використовуються для перевірки фактів або досліджень важкодоступних територій.

Управління кризами: оцінка наслідків природних катастроф, таких як повені чи землетруси, допомагає координувати рятувальні операції.

		Новіцький В.С.			ККІКБ.КР.Б – 125 – 33 – ПЗ	Арк.
		Покотило О.А.				15
Змн.	Арк.	№ докум.	Підпис	Дата		

1.2 Нормативно-правові аспекти OSINT

OSINT (Open Source Intelligence), тобто розвідка на основі відкритих джерел, стає все більш важливим інструментом у сфері національної безпеки, криміналістики та бізнес-аналітики. Оскільки OSINT включає збір і аналіз даних з публічно доступних джерел, таких як соціальні мережі, новинні сайти, форуми та інші ресурси, питання правового регулювання цієї діяльності є надзвичайно актуальними. Для забезпечення ефективного та законного використання інструментів OSINT необхідно враховувати специфіку національних і міжнародних норм і стандартів, що регулюють збір, обробку та захист інформації.

В Україні найбільше значення для правового регулювання діяльності з використання OSINT мають два основних документи: Закон України "Про захист персональних даних"[12] та Кримінальний процесуальний кодекс[21].

Закон України "Про захист персональних даних" регулює обробку персональних даних, визначаючи чіткі вимоги до збору, зберігання та використання особистої інформації. Він передбачає, що персональні дані можуть оброблятися тільки за умов: отримання явної згоди суб'єкта персональних даних, або якщо це необхідно для виконання юридичних зобов'язань.

Для діяльності OSINT важливим є той факт, що збирання персональних даних із публічних джерел (соціальні мережі, блоги, форуми) повинно бути законним, а також повинно відбуватися з дотриманням прав та свобод людини. Якщо зібрана інформація не стосується персональних даних або використовується без порушень конфіденційності, діяльність вважається дозволеною.

Кримінальний процесуальний кодекс України визначає правила збору доказів у кримінальних справах, включаючи інформацію з відкритих джерел. Згідно з статтями цього кодексу, слідчі органи можуть використовувати дані, зібрані з відкритих джерел (наприклад, інформацію з соціальних мереж або публічних баз даних), якщо це не порушує права на приватність і здійснюється з дотриманням законних процедур. Зокрема, дані, отримані з відкритих джерел, можуть бути використані як доказ у суді за умови, що їх збір не порушує законів про конфіденційність або авторське право.

		Новіцький В.С.			ККІКБ.КР.Б – 125 – 33 – ПЗ	Арк.
		Покотило О.А.				16
Змн.	Арк.	№ докум.	Підпис	Дата		

Це також дає можливість застосовувати OSINT у кримінальних розслідуваннях, особливо в контексті кіберзлочинів, шахрайства або терористичних загроз. Згідно з українським законодавством, використання даних з відкритих джерел не потребує спеціальних дозволів, якщо це не стосується обробки персональних даних без згоди їх власників.

У США важливим документом, що регулює використання відкритих даних, є Закон про свободу інформації (FOIA)[20]. Прийнятий у 1966 році, FOIA забезпечує право громадян на доступ до урядової інформації. Згідно з цим актом, федеральні органи влади зобов'язані надавати публічно доступну інформацію, за винятком тих випадків, коли доступ може зашкодити національній безпеці або порушити права приватних осіб.

Застосування FOIA в контексті OSINT дає змогу отримувати публічні звіти, документи, статистичні дані, а також інформацію, яка міститься в державних реєстрах і базах даних. Цей закон широко використовується в журналістиці та розслідувальних практиках для доступу до документів, що стосуються державної політики, фінансових звітів та інших важливих матеріалів.

Водночас, FOIA має ряд обмежень. Наприклад, інформація, що стосується національної безпеки або персональних даних, може бути закрита для доступу. Тому для отримання необхідної інформації спеціалісти з OSINT повинні уважно вивчати межі застосування цього закону.

Одним із важливих аспектів застосування OSINT є збір і аналіз даних з соціальних мереж, таких як Facebook, Instagram, Twitter, LinkedIn тощо. Персональні дані, що розміщуються користувачами в соціальних мережах, можуть бути використані для аналізу настроїв, виявлення зв'язків між особами та прогнозування різних соціальних або політичних процесів.

Однак у цьому контексті постає питання правомірності збору та використання цих даних, оскільки користувачі зазвичай не дають явну згоду на обробку своєї інформації для таких цілей. В Україні це питання регулюється Законом про захист персональних даних, а в Європейському Союзі — Загальним регламентом

		Новіцький В.С.			ККІКБ.КР.Б – 125 – 33 – ПЗ	Арк.
		Покотило О.А.				17
Змн.	Арк.	№ докум.	Підпис	Дата		

захисту даних (GDPR)[19], який став значущим міжнародним стандартом у питаннях приватності.

Однією з головних проблем у сфері правового регулювання OSINT є питання балансу між безпекою та правами людини. З одного боку, розвідка на основі відкритих джерел може допомогти у боротьбі з тероризмом, організованою злочинністю та іншими загрозами. З іншого боку, важливо забезпечити захист приватності користувачів і запобігти зловживанням, коли особисті дані збираються без їх відома.

Крім того, порушення авторських прав або використання комерційної інформації без дозволу може призвести до юридичних наслідків для тих, хто займається збором та аналізом даних через відкриті джерела. Це потребує постійного удосконалення законодавства та його адаптації до нових технологій та методів збору інформації.

1.3 Порівняння OSINT з іншими видами розвідки

У сфері розслідування кіберінцидентів особливу роль відіграє OSINT, яка дозволяє легально й ефективно збирати інформацію з загальнодоступних джерел для ідентифікації, моніторингу та аналізу цифрової активності. На відміну від закритих методів (наприклад, HUMINT або SIGINT), OSINT базується на публічних ресурсах, що дозволяє уникнути правових і технічних бар'єрів. Одним з найважливіших напрямків у межах OSINT є мережева розвідка, яка охоплює аналіз інфраструктури, IP-адрес, доменів, відкритих портів, використовуваних технологій, а також цифрових слідів зловмисників.

У рамках мережевої OSINT активно використовуються такі методи, як:

- Сканування портів – один із базових інструментів для виявлення відкритих сервісів на цільовому хості. Використовуючи інструменти на зразок nmap або masscan, дослідник може дізнатися, які порти прослуховуються, які сервіси працюють на пристрої (наприклад, веб-сервери, FTP, SSH, Telnet) та з

		Новіцький В.С.			ККІКБ.КР.Б – 125 – 33 – ПЗ	Арк.
		Покотило О.А.				18
Змн.	Арк.	№ докум.	Підпис	Дата		

якими версіями програмного забезпечення. Це дозволяє припускати, які вразливості можуть бути присутні (наприклад, застарілі версії Apache, відкритий доступ до Redis, тощо).

- WHOIS-запити – дозволяють отримати інформацію про власника домену, контактні дані, дати реєстрації, реєстратора, історію змін. Це може допомогти в ідентифікації фізичних або юридичних осіб, пов'язаних з доменом.

- DNS-розвідка – включає в себе визначення основних і піддоменів, зонування, записи типу A, MX, TXT тощо. Завдяки сервісам як DNSDumpster, SecurityTrails або recon-ng можна виявити приховані сервіси, пов'язані ресурси, корпоративні структури домену.

- Аналіз IP-адрес та інфраструктури – сервіси Maltego, Censys, ZoomEye дають змогу отримати технічні деталі про сервери, до яких відкритий доступ, включно з банерами сервісів, SSL-сертифікатами, геолокацією та портами. Це дозволяє не лише дізнатись про конфігурацію сервера, але й побачити, чи входить він до пулу VPN або TOR, чи був помічений у підозрілій активності.

- Активне сканування портів – дозволяє виявити відкриті порти та сервіси на віддалених хостах. Інструменти як Nmap, Masscan, Zmap допомагають ідентифікувати, які служби працюють і які потенційні вразливості можуть існувати.

- Пасивний аналіз DNS (Passive DNS) – дозволяє побачити історію доменних записів і дізнатися, які IP-адреси раніше були пов'язані з певним доменом, що корисно при виявленні ботнетів, фішингових ресурсів або переміщення зловмисної інфраструктури.

У рамках мережевої розвідки, окрім методів OSINT, активно застосовуються й інші підходи, що дозволяють здійснювати глибший технічний аналіз мережевої інфраструктури, виявляти потенційні загрози та збирати критично важливу інформацію. Одним із таких методів є SIGINT (Signals Intelligence), що передбачає перехоплення технічних сигналів у мережах, зокрема аналіз трафіку, моніторинг з'єд-

		Новіцький В.С.			ККІКБ.КР.Б – 125 – 33 – ПЗ	Арк.
		Покотило О.А.				19
Змн.	Арк.	№ докум.	Підпис	Дата		

нань, перехоплення пакетів і низькорівневих протоколів. Цей тип розвідки є технічно складним і зазвичай використовується з дотриманням правових норм, часто в контексті роботи центрів моніторингу безпеки (SOC)[13].

Також важливою частиною є технічна мережева розвідка, яка базується на активному скануванні мережі. До цього відноситься виявлення відкритих портів, банерів сервісів, аналіз топології маршруту за допомогою traceroute, а також визначення операційної системи чи конфігурацій хостів через активне fingerprint-сканування. Такі дії реалізуються за допомогою інструментів на кшталт Nmap, Masscan або Zmap, які дозволяють швидко оцінити структуру зовнішньої мережевої поверхні об'єкта. Ці методи забезпечують цінну інформацію для подальшого аналізу та планування заходів кіберзахисту.

Ще одним напрямом є тестування на проникнення, коли розвідка проводиться в умовах моделювання атаки для виявлення вразливостей. Це передбачає використання спеціалізованих фреймворків, як-от Metasploit, Nessus або OpenVAS, які дозволяють визначати відомі уразливості та симулювати експлуатацію з метою перевірки захищеності. У цьому контексті часто застосовується концепція red teaming – коли команда спеціалістів діє як умовний противник, намагаючись проникнути в систему або обійти засоби захисту. Такий підхід допомагає виявити слабкі місця в системі безпеки до того, як ними скористаються реальні зловми-сники.

Також у процесі мережевої розвідки використовують аналіз трафіку, який дозволяє досліджувати поведінку мережевих потоків без повного перехоплення вмісту пакетів. За допомогою NetFlow, IPFIX та інших систем можна виявляти аномалії в роботі мережі, слідкувати за підозрілою активністю або визначати витік інформації. Цей підхід допомагає оперативно реагувати на потенційні загрози та підвищувати рівень безпеки мережевої інфраструктури. Поряд із цим застосовується аналіз історичних даних, наприклад, Passive DNS або Passive SSL, які дозволяють визначати, які домени раніше були пов'язані з IP-адресою чи сертифікатом, що ча-

		Новіцький В.С.			ККІКБ.КР.Б – 125 – 33 – ПЗ	Арк.
		Покотило О.А.				20
Змн.	Арк.	№ докум.	Підпис	Дата		

сто допомагає у виявленні інфраструктури кіберзлочинців. Використання таких даних сприяє більш глибокому розумінню поведінки атакуювальних кампаній і підвищенню ефективності розслідувань.

Не менш важливим є напрям Cyber Threat Intelligence, що об'єднує різні типи даних, включаючи OSINT, NETINT та інші, для побудови загальної картини загроз. СТІ орієнтується не лише на технічні дані, а й на їх стратегічне осмислення, формуючи інформаційну підтримку для рішень на рівні безпекової політики. Завдяки цьому організації можуть проактивно планувати заходи захисту та зменшувати ризики кіберінцидентів[6].

Порівняння видів розвідки наведено у Додатку А.

Незважаючи на те, що OSINT має обмеження у доступі лише до відкритих джерел, він залишається ключовим і ефективним методом розвідки, особливо на етапах виявлення, збору попередньої інформації та побудови загальної картини об'єкта розслідування. Його легальність, доступність і невидимість роблять його незамінним в умовах, коли прямий доступ до систем або мережевих потоків неможливий.

Висновки до першого розділу

У першому розділі було розглянуто основи OSINT та його класифікацію, зокрема напрямки GEOINT, IMGINТ та CYBERINT. Також проаналізовано нормативно-правові аспекти використання відкритих джерел і проведено порівняння OSINT з іншими типами розвідки – SIGINT, HUMINT, TECHINT тощо. Особливу увагу приділено мережевій розвідці як ключовому напрямку у зборі технічної інформації. Визначено основні методи та інструменти збору даних, що забезпечують комплексний підхід до аналізу кіберінцидентів. У підсумку встановлено, що OSINT, попри обмеження у доступі лише до відкритих джерел, залишається ефективним і легальним способом отримання цінної інформації для кібербезпеки, здатним доповнювати інші види розвідки та забезпечувати оперативність у розслідуваннях.

		Новіцький В.С.			ККІКБ.КР.Б – 125 – 33 – ПЗ	Арк.
		Покотило О.А.				21
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 2 ПРАКТИЧНІ ІНСТРУМЕНТИ ТА РЕСУРСИ ДЛЯ OSINT

2.1 Віртуалізація як засіб безпечного збору даних

2.1.1 Програмне забезпечення VirtualBox

VirtualBox – це інструмент віртуалізації, створений компанією Oracle, який дозволяє запускати кілька операційних систем на одному фізичному комп'ютері в ізольованому середовищі. Ця ізоляція є ключовою для забезпечення безпеки під час проведення OSINT-розвідки, оскільки гостьова система працює незалежно від основної, що захищає персональні дані дослідника від розкриття.

Однією з головних переваг VirtualBox є можливість створення закритого середовища, яке дозволяє дослідникам проводити збір даних із мінімальним ризиком виявлення. Завдяки віртуалізації можна приховати реальну IP-адресу користувача, оскільки трафік із гостьової системи проходить через хостову машину. Це особливо корисно під час аналізу потенційно небезпечних вебсайтів або збирання інформації з платформ, які можуть відстежувати дії користувача. Наприклад, мережеві налаштування VirtualBox дозволяють ізолювати віртуальну машину від реальної мережі або використовувати спеціалізовані VPN-сервіси для забезпечення анонімності[7]. На рисунку 2.1 зображено основний інтерфейс програми VirtualBox.

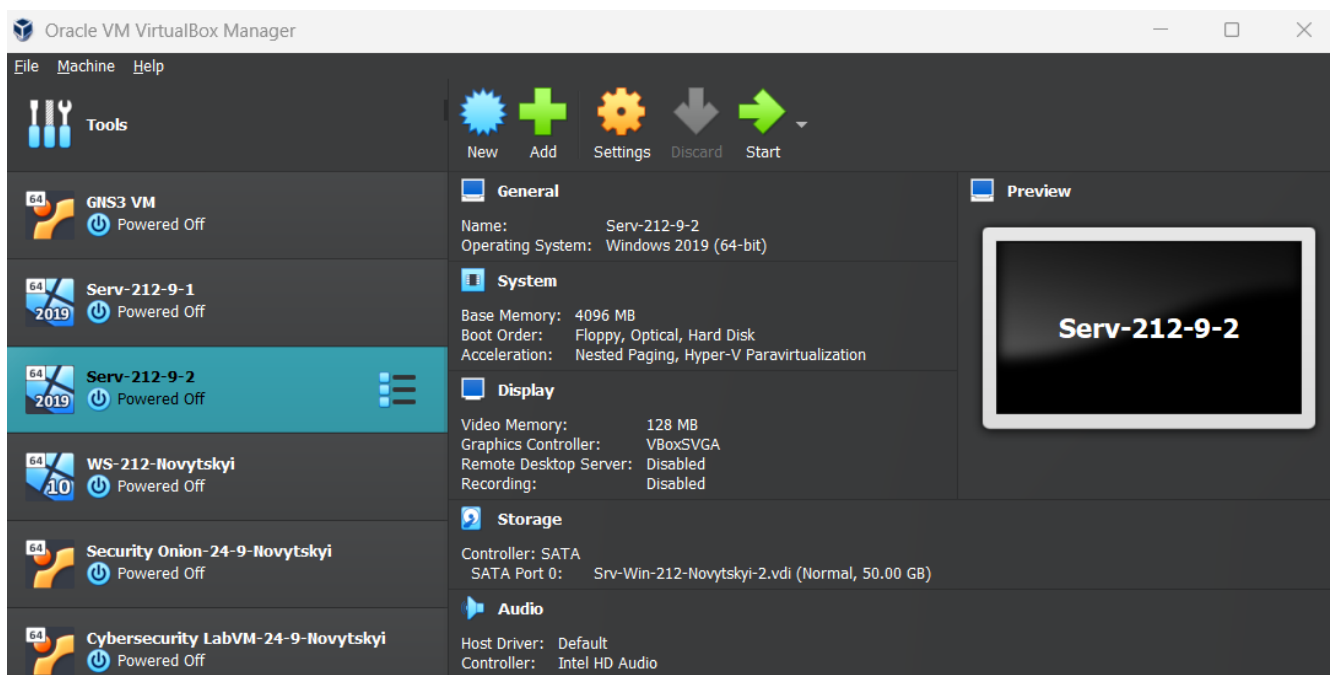


Рис. 2.1 – Інтерфейс програми VirtualBox

		Новіцький В.С.			ККІКБ.КР.Б – 125 – 33 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		22

VirtualBox дозволяє повністю ізолювати гостьову операційну систему, відключаючи її від основних мереж або ресурсів хостової машини. Наприклад, можна заборонити інтеграцію між системами, виключивши доступ до спільних папок, USB-пристроїв або принтерів. Це значно зменшує ризик несанкціонованого доступу до основних даних користувача.

Особливу увагу під час OSINT-розвідки приділяють використанню спеціалізованих операційних систем, таких як TLVM[23] або Whonix, які розроблені для забезпечення максимальної конфіденційності. Ці системи можуть працювати виключно у віртуальному середовищі, створеному VirtualBox, що дозволяє безпечно взаємодіяти з мережею Інтернет, приховуючи місцезнаходження та інші ідентифікатори. Налаштування таких систем часто включає використання багатопланового захисту, наприклад, маршрутизації через Tor, щоб унеможливити відстеження дій дослідника.

На додаток до можливостей захисту, VirtualBox підтримує "відновлення стану" віртуальної машини. Це дозволяє створювати "чисте" середовище перед кожним новим етапом дослідження, усуваючи ризик випадкового збереження небажаних змін або шкідливих файлів. Такі функції забезпечують високу гнучкість і безпеку під час роботи з OSINT-даними.

Таким чином, VirtualBox є потужним і універсальним інструментом для забезпечення анонімності та захисту під час проведення OSINT-досліджень. Його функції ізоляції, можливість налаштування мережі та підтримка спеціалізованих операційних систем роблять його незамінним для безпечного аналізу інформації.

2.1.2 Віртуальна машина Trace Labs

Trace Labs Virtual Machine (TLVM)[23] – це віртуальне середовище, створене для підтримки розвідувальних операцій, заснованих на відкритих джерелах (OSINT). Воно дозволяє дослідникам працювати з різноманітними інструментами, які попередньо встановлені й налаштовані для ефективного збору, аналізу та обробки даних. TLVM базується на Linux і забезпечує безпечну, ізольовану платформу

		Новіцький В.С.			ККІКБ.КР.Б – 125 – 33 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		23

для роботи, що є важливим для збереження конфіденційності користувача та захисту від можливих кіберзагроз.

Головною перевагою цієї віртуальної машини є її готовність до використання. Усі необхідні інструменти вже встановлені, що дозволяє досліднику уникнути складного процесу налаштування. TLVM включає програми для збору інформації з соціальних мереж, аналізу геолокаційних даних і метаданих. Наприклад, ExifTool[22] допомагає витягувати метадані з файлів, таких як зображення, дозволяючи дізнатися про місце, дату створення та технічні параметри знімка. Інший популярний інструмент, Sherlock, дозволяє шукати профілі користувачів у соціальних мережах за їхнім іменем користувача, надаючи цінну інформацію для аналізу.

На рисунку 2.2 наведено приклад інтерфейсу Trace Labs Virtual Machine, де показано ключові компоненти цієї платформи. Важливим аспектом роботи з TLVM є налаштування мережевих параметрів для забезпечення анонімності. Інтеграція з Tor та VPN забезпечує захист і прихованість даних розвідника, унеможливлюючи ідентифікацію його місцезнаходження.

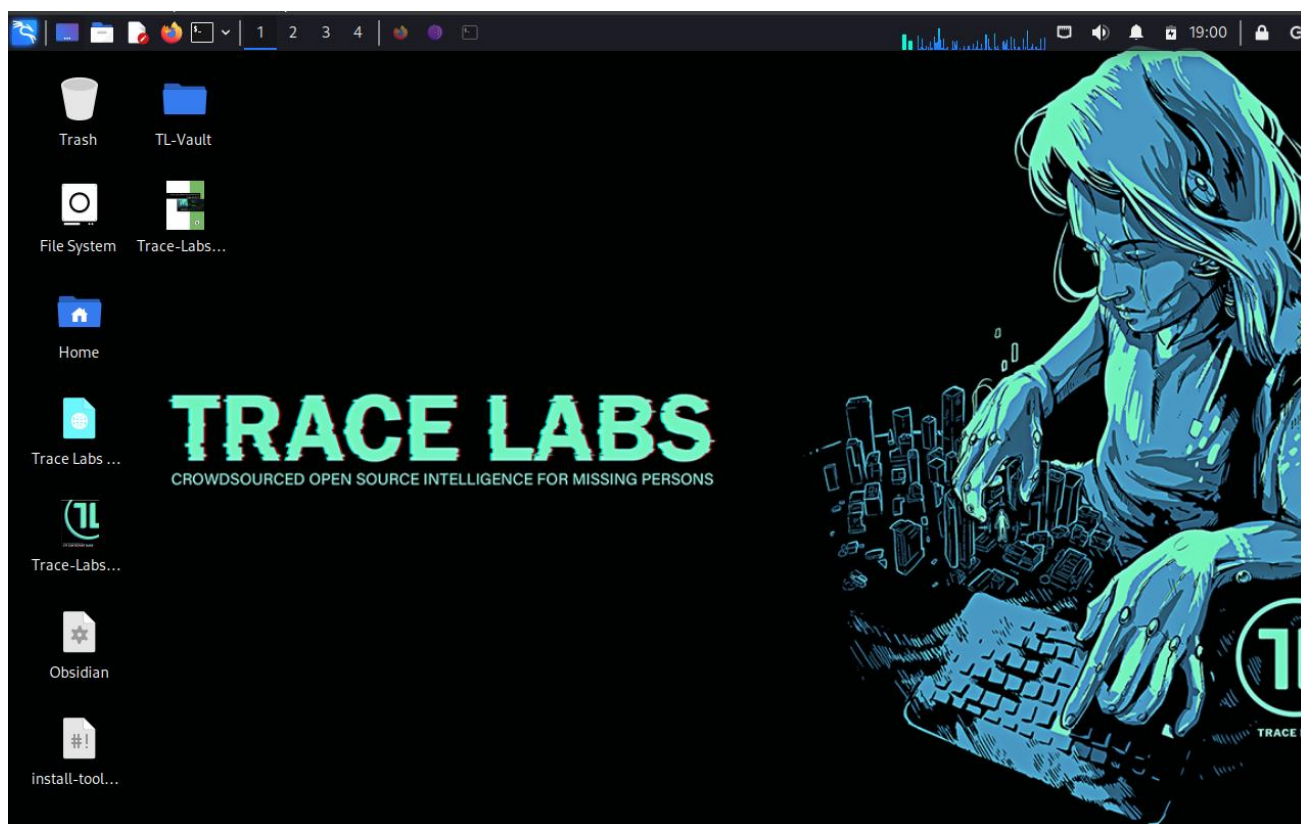


Рис. 2.2 – Віртуальна машина Trace Labs

		Новіцький В.С.			ККІКБ.КР.Б – 125 – 33 – ПЗ	Арк.
		Покотило О.А.				24
Змн.	Арк.	№ докум.	Підпис	Дата		

Trace Labs Virtual Machine є потужним інструментом для спеціалістів OSINT. Її переваги – ізольоване середовище, широкий набір попередньо налаштованих інструментів і підтримка анонімності – роблять її ідеальним вибором для виконання розвідувальних операцій. Завдяки таким функціям, як аналіз метаданих, пошук у соціальних мережах і забезпечення конфіденційності, TLVM стає універсальним рішенням для фахівців, які працюють у сфері розвідки на основі відкритих джерел.

2.1.3 VPN як інструмент захисту віртуалізованого середовища

VPN – це технологія, яка дозволяє створити захищене з'єднання через незахищену мережу, зокрема інтернет. VPN дає змогу анонімно передавати дані між комп'ютером користувача та віддаленим сервером, приховуючи справжню IP-адресу та шифруючи з'єднання, що робить процес збору та аналізу інформації більш безпечним і конфіденційним. Для дослідників OSINT використання VPN є важливим кроком у забезпеченні анонімності під час роботи з чутливими або обмеженими джерелами.

Одним із популярних інструментів VPN є *Windscribe*[11] – сервіс, який пропонує не лише можливості захисту інтернет-з'єднання, але й додаткові функції, які можуть бути корисними для аналізу даних у віртуалізованих середовищах. *Windscribe* дозволяє створювати захищене з'єднання, приховувати реальну IP-адресу та обирати з широкого спектра серверів у різних країнах. Це дозволяє не тільки обходити географічні обмеження, але й маскувати місцезнаходження користувача, що є важливим для розвідників і фахівців з OSINT, які збирають інформацію з відкритих джерел.

VPN також забезпечує захист віртуальних машин, таких як Trace Labs Virtual Machine, шляхом додаткового шарового захисту інтернет-з'єднань. Це дозволяє досліднику працювати без ризику розкриття його реального місцезнаходження під час роботи з потенційно небезпечними або підозрілими вебсайтами. Використання VPN дозволяє не лише забезпечити конфіденційність, а й уникнути спостереження або відстеження своїх дій в інтернеті.

		Новіцький В.С.			ККІКБ.КР.Б – 125 – 33 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		25

Завдяки VPN, користувач може підключитися до серверів по всьому світу, що відкриває можливості обходити блокування контенту або переглядати інформацію, яка недоступна у конкретному регіоні. Це особливо корисно при проведенні розвідки з відкритих джерел, коли важливо мати доступ до інформації, що зберігається на серверах в різних країнах, або виявити контент, заблокований через географічні обмеження.

Незважаючи на численні переваги, слід зазначити, що VPN не є гарантією повної безпеки. Наприклад, при неправильному налаштуванні або використанні ненадійних постачальників сервісів VPN, може виникнути ризик витоку інформації, оскільки деякі сервіси можуть зберігати лог-файли або мати вразливості, які дозволяють відслідковувати активність користувача.

Вибір надійного VPN-сервісу, як Windscribe, та правильне налаштування є ключовими для забезпечення необхідного рівня анонімності та безпеки при використанні віртуальних середовищ для збору OSINT. Інтерфейс VPN-сервісу Windscribe зображено на рисунку 2.3.

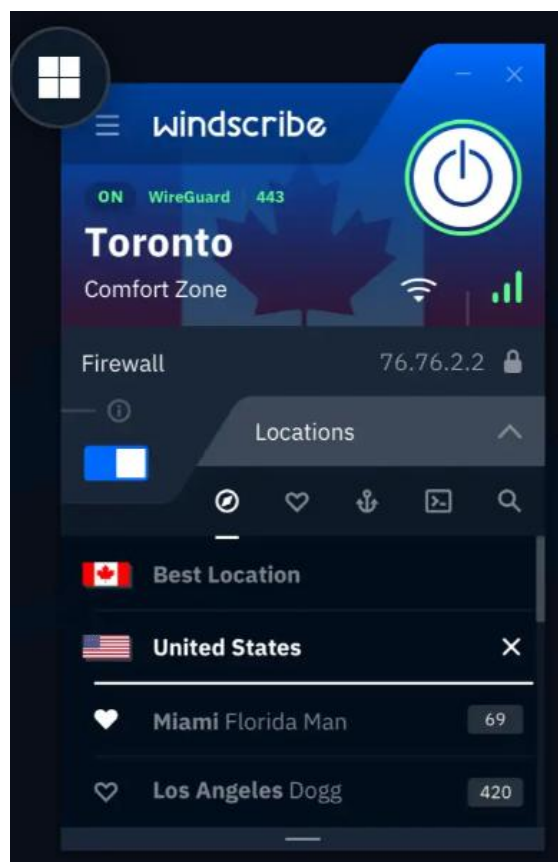


Рис. 2.3 – VPN-сервіс Windscribe

		Новіцький В.С.			ККІКБ.КР.Б – 125 – 33 – ПЗ	Арк.
		Покотило О.А.				26
Змн.	Арк.	№ докум.	Підпис	Дата		

2.2 Інструменти та веб-сервіси для збору OSINT

Для проведення OSINT-досліджень у сфері мережевої розвідки важливу роль відіграють інструменти, інтегровані в дистрибутив Kali Linux – операційне середовище, спеціалізоване на кібербезпеці, тестуванні на проникнення та інформаційній розвідці. Вони забезпечують широкий спектр функцій: від автоматизованого збору даних про домени, IP-адреси, мережеві порти та сервіси – до перевірки активності акаунтів, пошуку взаємозв'язків між цифровими об'єктами та взаємодії з API вебресурсів. Комбінація графічних інструментів, таких як Maltego чи Recon-ng, із консольними утилітами, на кшталт Nmap, whois, curl або HOLEHE, дозволяє досліднику гнучко поєднувати різні підходи та рівні деталізації аналізу залежно від поставлених цілей.

Maltego – це OSINT-інструмент із графічним інтерфейсом, призначений для виявлення взаємозв'язків між об'єктами у цифровому середовищі. Програма дозволяє будувати візуальні графи, які показують зв'язки між доменами, IP-адресами, акаунтами в соціальних мережах, електронними адресами, організаціями, документами тощо[25]. Інтерфейс програмного забезпечення Maltego зображено на рисунку 2.4.

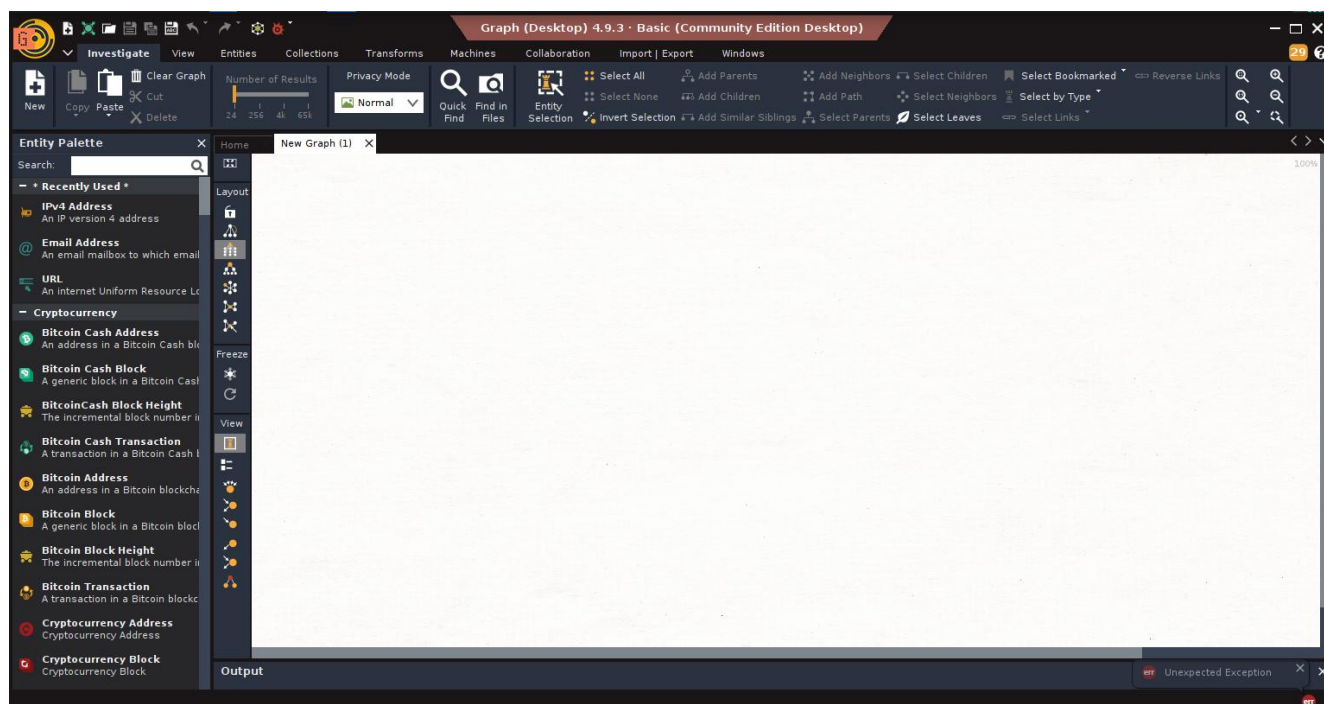


Рис. 2.4 – Інтерфейс програмного забезпечення Maltego

		Новіцький В.С.			ККІКБ.КР.Б – 125 – 33 – ПЗ	Арк.
		Покотило О.А.				27
Змн.	Арк.	№ докум.	Підпис	Дата		

Оснoву роботи Maltego складають трансформації(рис. 2.5) – автоматизовані запити до відкритих баз даних або API, які дозволяють дослідити об’єкт та пов’язані з ним дані. Наприклад, трансформація до IP-адреси може виявити домени, що раніше були до неї прив’язані, або інформацію з DNS-записів. Користувач може візуально відстежити зв’язки між суб’єктами, що значно полегшує аналіз навіть великих обсягів інформації.

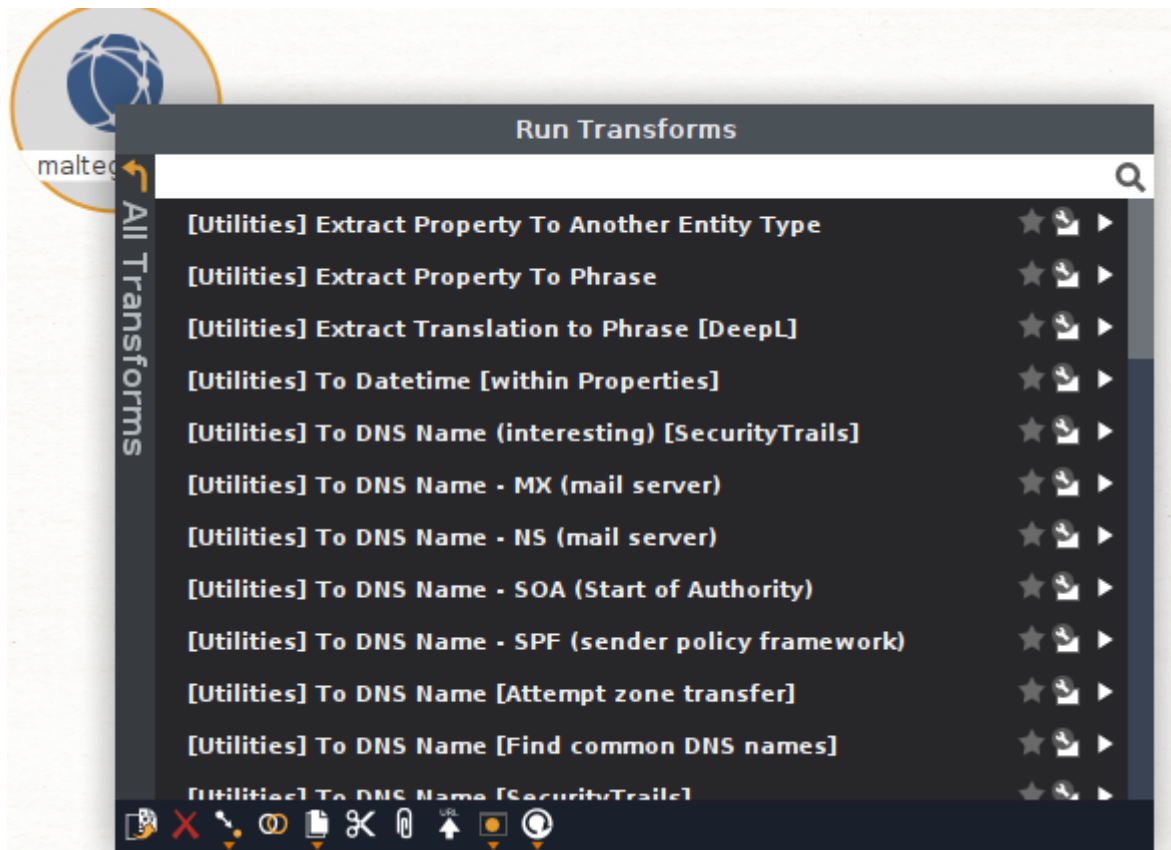


Рис. 2.5 – Перелік доступних трансформацій

Recon-ng – це модульний фреймворк для проведення OSINT-досліджень, що працює у текстовому інтерфейсі та нагадує структуру Metasploit. Його основне призначення – автоматизований збір інформації з відкритих джерел, таких як API публічних сервісів, бази даних, пошукові системи тощо. Recon-ng має вбудовану систему управління модулями, API-ключами та звітністю, що дозволяє проводити комплексне розслідування з мінімальним втручанням користувача[14]. Інтерфейс Recon-ng зображено на рисунку 2.6.

		Новіцький В.С.			ККІКБ.КР.Б – 125 – 33 – ПЗ	Арк.
		Покотило О.А.				28
Змн.	Арк.	№ докум.	Підпис	Дата		

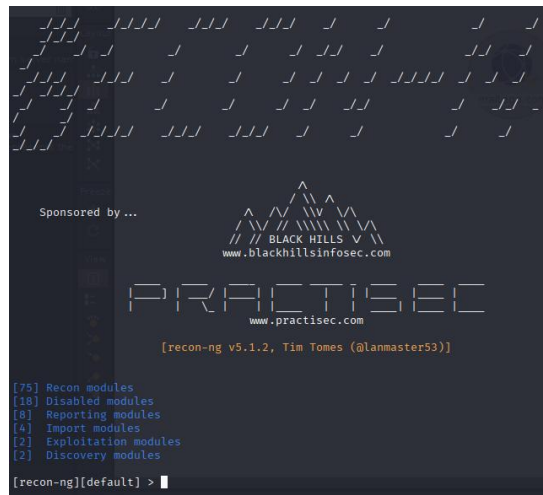


Рис. 2.6 – Інтерфейс програмного забезпечення Recon-ng

Recon-ng складається з великої кількості модулів(рис. 2.7), які поділяються за категоріями відповідно до типу даних або функцій[14]. Серед ключових модулів:

- recon/domains-hosts/ – здійснює пошук пов'язаних хостів за доменом;
- recon/hosts-hosts/ – дозволяє встановити зв'язки між відомими IP-адресами;
- recon/contacts/emailhunter/ – збір email-адрес, асоційованих із доменом;
- recon/companies-profiles/ – модулі для аналізу публічних даних про організації;
- reporting/html, csv, json – автоматизоване створення звітів у зручному форматі.

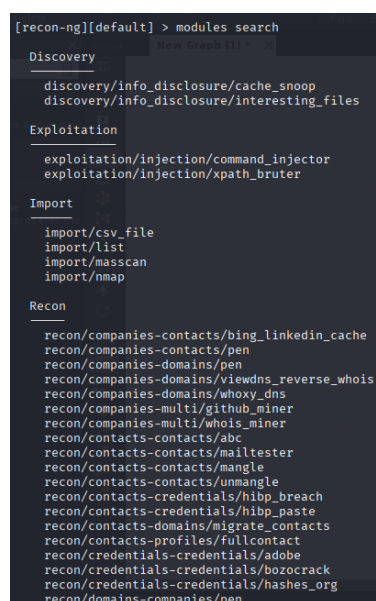


Рис. 2.7 – Список доступних модулів Recon-ng

		Новіцький В.С.			ККІКБ.КР.Б – 125 – 33 – ПЗ	Арк.
		Покотило О.А.				29
Змн.	Арк.	№ докум.	Підпис	Дата		

Holehe – це консольний OSINT-інструмент, що дозволяє перевірити наявність облікового запису за вказаною електронною адресою на десятках популярних вебсервісів. Він не надає повного доступу до акаунтів, але дозволяє з’ясувати, чи була ця адреса використана при реєстрації, що є корисним при ідентифікації активності особи або визначенні можливих точок компрометації. Holehe працює шляхом емулявання процесу автентифікації або перевірки реєстрації на різних сайтах[26].

Інструмент має простий синтаксис виклику в терміналі. У команді вказано досліджувану електронну адресу. Після виконання команди Holehe виведе список сайтів(рис. 2.8), на яких знайдено обліковий запис, або зазначить, що такий обліковий запис відсутній. Інструмент підтримує як перевірку однієї адреси, так і пакетну обробку списку адрес (через файл або скрипт), що робить його корисним у масових розслідуваннях.

```
*****
testmail@gmail.com
*****
[x] about.me
[x] adobe.com
[+] amazon.com
[x] amocrm.com
[+] any.do
[-] archive.org
[-] armurerie-auxerre.com
[x] atlassian.com
[-] axonaut.com
[x] babesshows.co.uk
[x] badeggsonline.com
[x] bios-mods.com
[x] biotechnologyforums.com
[x] bitmoji.com
[x] blablacar.com
[x] blackworldforum.com
[-] blip.fm
[x] forum.blitzortung.org
[x] bluegrassrivals.com
```

Рис. 2.8 – Перевірка адреси електронної пошти в Holehe

Nmap – це один із найвідоміших інструментів для мережевого сканування та виявлення активних хостів, відкритих портів, запущених сервісів, а також операційних систем на віддалених пристроях[18]. У контексті OSINT Nmap є потужним засобом для збору технічної інформації про об’єкти дослідження, оскільки дозволяє виявляти слабкі місця або неправильно сконфігуровані сервіси, які можуть бути використані для подальшого аналізу. Застосування Nmap не вимагає доступу

до внутрішньої інфраструктури, достатньо IP-адреси цілі(рис. 2.9). Інтерфейс командного рядка дозволяє гнучко керувати параметрами сканування, а результати зручно зберігати у форматах XML або txt для подальшої обробки.

```
(osint@tlosint)-[~]
$ nmap -sV -Pn -T4 192.168.1.1
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-16 23:03 UTC
Stats: 0:00:08 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 7.50% done; ETC: 23:05 (0:01:39 remaining)
Nmap scan report for 192.168.1.1
Host is up.
All 1000 scanned ports on 192.168.1.1 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 102.74 seconds
```

Рис. 2.9 – Сканування IP-адреси за допомогою Nmap

У ході роботи застосовуються різні параметри(рис. 2.10), що дозволяють налаштовувати глибину та швидкість сканування. Наприклад, ключ -sV відповідає за визначення версій сервісів, що працюють на відкритих портах, тоді як -Pn вимикає спроби попереднього виявлення активності хоста через ICMP (ping), що дозволяє обійти фільтрацію або блокування. Параметр -T4 задає агресивніший темп сканування, що пришвидшує процес, а -A активує розширений аналіз – включає виявлення ОС, traceroute та інші функції.

```
$ nmap -help
Nmap 7.95 ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sl: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PU/PY[portlist]: TCP SYN, TCP ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
SCAN TECHNIQUES:
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
  -sU: UDP Scan
  -sN/sF/sX: TCP Null, FIN, and Xmas scans
  --scanflags <flags>: Customize TCP scan flags
  -sI <zombie host[:probeport]>: Idle scan
  -sY/sZ: SCTP INIT/COOKIE-ECHO scans
  -sO: IP protocol scan
  -b <FTP relay host>: FTP bounce scan
PORT SPECIFICATION AND SCAN ORDER:
```

Рис. 2.10 – Список параметрів синтаксису Nmap

WHOIS – це один із базових інструментів для отримання інформації про доменні імена, IP-адреси та автономні системи. У контексті OSINT WHOIS використовується для ідентифікації реєстрантів доменів, дізнавання контактних даних, дати створення та закінчення терміну дії домену, реєстратора, DNS-серверів та інших атрибутів. Ці дані дають змогу встановити зв'язок між кіберінфраструктурою та конкретною особою або організацією, а також виявити інші домени, зареєстровані тим самим суб'єктом[24]. При цьому WHOIS-запити не потребують доступу до системи жертви – інформація надається з реєстрів у відкритому вигляді(рис. 2.11).

```

(ubuntu@ubuntu) ~$ whois ztu.edu.ua
% Request from 77.75.150.188
% This is the Ukrainian Whois query server #W.
% The Whois is subject to Terms of use
% See https://hostmaster.ua/services/
%
% IN THE PROCESS OF DELEGATION OF A DOMAIN NAME,
% THE REGISTRANT IS AN ENTITY WHO USES AND MANAGES A CERTAIN DOMAIN NAME,
% AND THE REGISTRAR IS A BUSINESS ENTITY THAT PROVIDES THE REGISTRANT
% WITH THE SERVICES NECESSARY FOR THE TECHNICAL MAINTENANCE OF THE REGISTRATION AN
D OPERATION OF THE DOMAIN NAME.
% FOR INFORMATION ABOUT THE REGISTRANT OF THE DOMAIN NAME, YOU SHOULD CONTACT THE
REGISTRAR.
%
% .UA whois
% Domain Record:
%
domain:          ztu.edu.ua
admin-c:         ZTU1-UANIC
tech-c:          YM36-UANIC
status:          OK-UNTIL 20260614113437
nserver:         ns2.trifle.net
nserver:         ns.ztu.edu.ua
nserver:         static.154.92.4.46.clients.your-server.de
remark:          Zhytomyr Polytechnic State University
remark:          103, Chernyakhovsky St.
remark:          Zhitomir, 10005
remark:          Ukraine
created:         0-UANIC 20060123000000
changed:         UARR168-UANIC 20250515085735
source:          UANIC

```

Рис. 2.11 – Отримання даних WHOIS для домену

WHOIS підтримує низку параметрів(рис. 2.12), які дозволяють гнучко налаштовувати запити. Наприклад, параметр `-h` дозволяє вказати конкретний WHOIS-сервер (наприклад, `whois.iana.org`), що корисно для точнішого отримання інформації про IP-адреси або домени верхнього рівня. Прапорець `--verbose` (у деяких реалізаціях) активує розширений вивід із додатковими технічними деталями. За допомогою `--host` або `--port` можна вручну задати порт і сервер для нестандартних конфігурацій. Також у деяких клієнтах передбачена опція `--raw`, що дозволяє отримати результат без форматування, придатний для подальшого автоматизованого аналізу.

		Новіцький В.С.			ККІКБ.КР.Б – 125 – 33 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		32

```

$ whois -help
Usage: whois [OPTION] ... OBJECT ...

-h HOST, --host HOST    connect to server HOST
-p PORT, --port PORT    connect to PORT
-I                      query whois.iana.org and follow its referral
-H                      hide legal disclaimers
--verbose              explain what is being done
--no-recursion         disable recursion from registry to registrar servers
--help                display this help and exit
--version              output version information and exit

These flags are supported by whois.ripe.net and some RIPE-like servers:
-l                    find the one level less specific match
-L                    find all levels less specific matches
-m                    find all one level more specific matches
-M                    find all levels of more specific matches
-c                    find the smallest match containing a mnt-irt attribute
-x                    exact match
-b                    return brief IP address ranges with abuse contact
-B                    turn off object filtering (show email addresses)
-G                    turn off grouping of associated objects
-d                    return DNS reverse delegation objects too
-i ATTR[,ATTR] ...    do an inverse look-up for specified ATTRIBUTES
-T TYPE[,TYPE] ...    only look for objects of TYPE
-K                    only primary keys are returned
-r                    turn off recursive look-ups for contact information
-R                    force to show local copy of the domain object even
                        if it contains referral
-a                    also search all the mirrored databases
-s SOURCE[,SOURCE] ... search the database mirrored from SOURCE
-g SOURCE:FIRST-LAST  find updates from SOURCE from serial FIRST to LAST
-t TYPE               request template for object of TYPE
-v TYPE               request verbose template for object of TYPE
-q [version|sources|types] query specified server info

```

Рис. 2.12 – Список параметрів синтаксису Whois

Для збору інформації в межах OSINT-дослідження активно застосовуються спеціалізовані веб-сервіси, доступні через браузер. Вони дозволяють безкоштовно отримувати значний обсяг технічних та аналітичних даних з відкритих джерел. Такі інструменти є важливими для ідентифікації IP-адрес, аналізу доменів, виявлення шкідливої активності або перевірки ознак маскування трафіку через VPN або TOR. Нижче наведено опис декількох онлайн-сервісів, які були використані у рамках цього дослідження для збору та аналізу відкритої мережевої інформації.

urlscan.io – це веб-сервіс для автоматичного аналізу URL-адрес. Він дозволяє здійснювати сканування вебсторінок для виявлення потенційно шкідливого вмісту, витягувати метадані, DNS-записи, ресурси, які завантажуються під час відвідування сайту. За допомогою цього інструмента можна перевірити, чи пов'язана адреса з фішингом, шкідливим ПЗ або підозрілими серверами. urlscan.io часто використовується у сфері кібербезпеки для дослідження фішингових кампаній, доменів,

отриманих із шкідливих листів, або просто для вивчення поведінки невідомого сайту без ризику зараження[24]. Веб-сайт urlscan.io показано на рисунку 2.13.

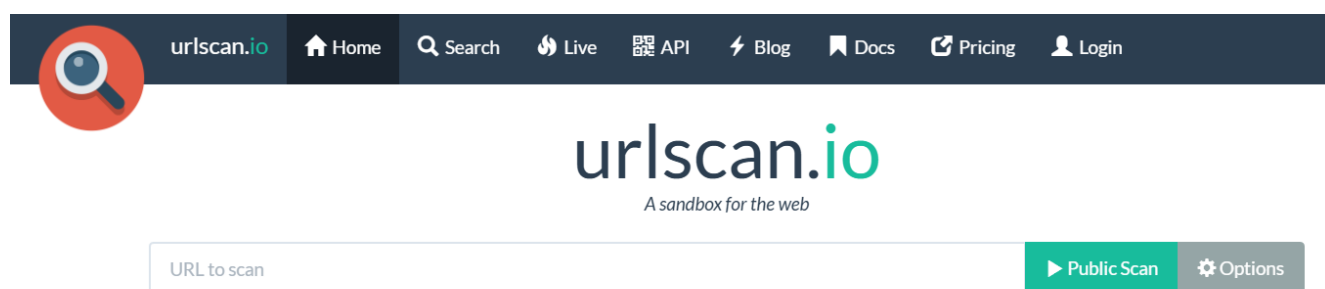


Рис. 2.13 – Веб-сервіс Ulrscan.io

VPNAPI.io – інструмент для перевірки, чи використовує певна IP-адреса VPN, проксі або TOR-мережу. Він дозволяє визначити, чи є підозрілою активність користувача або сервера з точки зору маскуванню справжнього розташування. API також надає інформацію про країну, регіон, місто, ANS, що може бути використано для побудови географічного профілю IP-адреси[24]. Це особливо корисно у розслідуваннях, пов'язаних з ботнетами, кіберзлочинністю або анонімною активністю. Веб-сайт VPNAPI.io показано на рисунку 2.14.

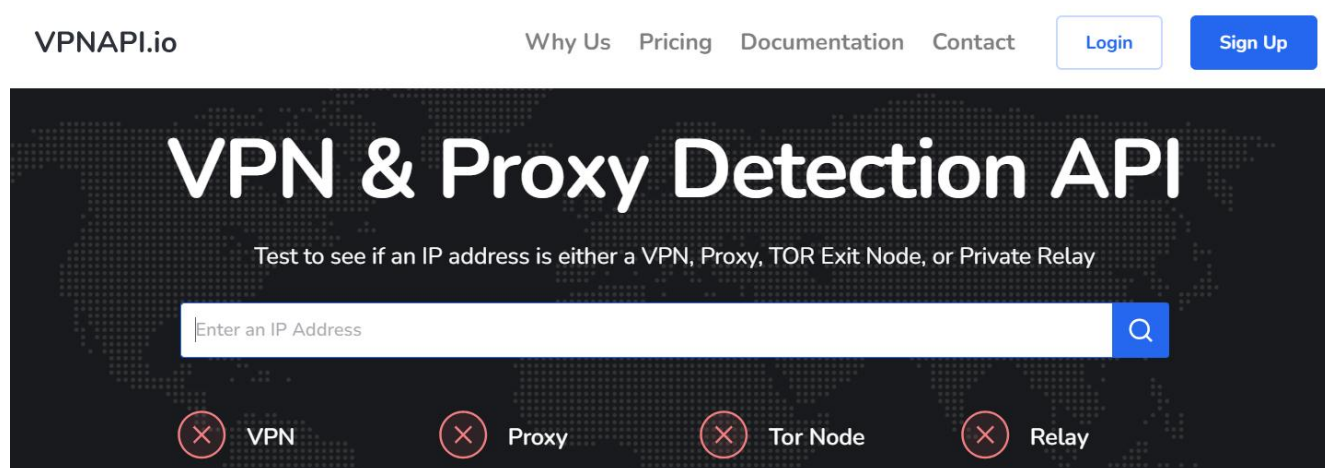


Рис. 2.14 – Веб-сервіс VPNAPI.io

IPQualityScore – веб-інструмент для оцінки якості IP-адрес, URL, доменів, поштових адрес тощо. Він дозволяє виявляти боти, VPN, TOR, проксі, зламані пристрої, фішингові сайти й шкідливі домени. IPQS надає ймовірнісну оцінку ризику, пов'язану з конкретним об'єктом, що допомагає швидко зрозуміти, наскільки підозрілою є IP-адреса чи вебсайт. Сервіс має як API-доступ, так і веб-інтерфейс, що

		Новіцький В.С.			ККІКБ.КР.Б – 125 – 33 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		34

робить його зручним як для автоматизованих сканувань, так і для ручного аналізу в OSINT-розслідуваннях[24]. Веб-сайт IPQualityScore показано на рисунку 2.15.

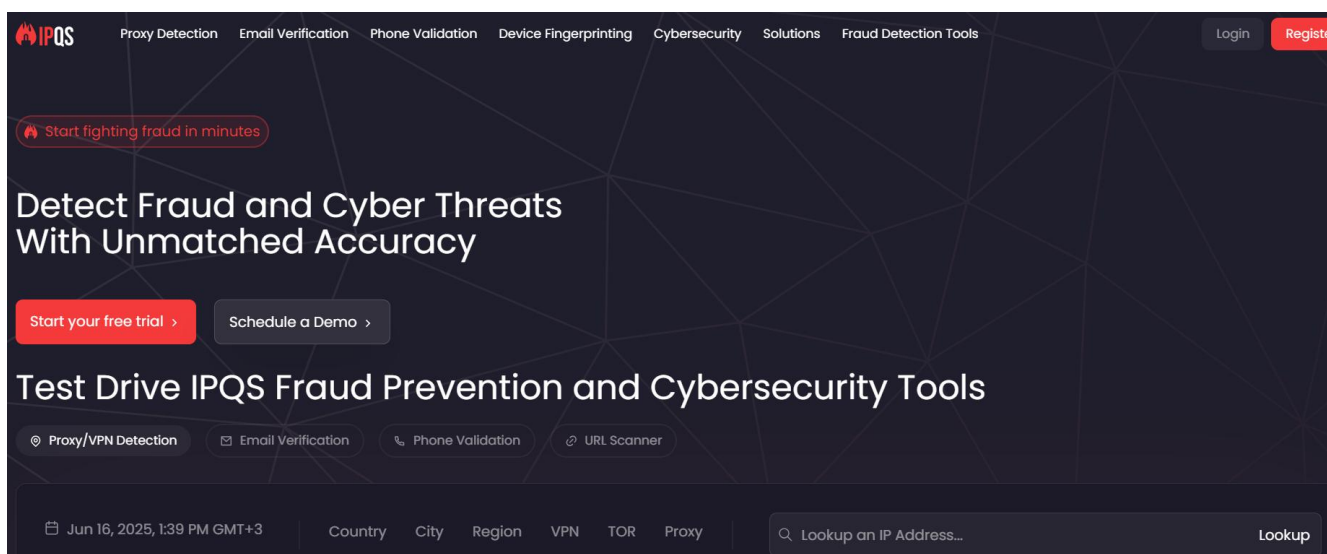


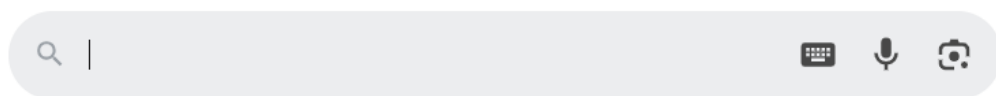
Рис. 2.15 – Веб-сервіс IPQualityScore

2.3 Використання інтернет-ресурсів Google

Google – це ефективний інструмент, який використовується в багатьох сферах, зокрема в OSINT для збору відкритої інформації з різноманітних джерел. Оскільки Google надає доступ до величезної кількості інтернет-ресурсів, його інструменти дають можливість здійснювати пошук за різними критеріями та отримувати релевантні дані для дослідження.

Google Search – це найбільш популярний інструмент для збору інформації. Завдяки розширеним функціям пошуку, таким як операції з фільтрацією результатів за допомогою операторів ("site:", "intitle:", "inurl:", "filetype:")[15], дослідники можуть значно звузити коло пошуку і знайти необхідну інформацію. Наприклад, використовуючи оператор "site:", можна обмежити пошук лише на певних вебсайтах чи доменах, що дозволяє знаходити специфічні дані або публікації, які зберігаються лише на визначених ресурсах. Це є важливим аспектом для збору точних даних, коли потрібно витягнути відомості з конкретних джерел або спеціалізованих сайтів. У Google Search можна також використовувати комбінацію фільтрів для уточнення запиту, що дозволяє швидко отримувати найбільш релевантну інформацію. Інтерфейс Google Search показано на рисунку 2.16.

		Новіцький В.С.			ККІКБ.КР.Б – 125 – 33 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		35



Пошук Google

Мені пощастить

Рис. 2.16 – Google Search

Іншим важливим інструментом є *Google Lens*, який дозволяє шукати інформацію за допомогою розпізнавання зображень. Цей інструмент активно використовують у OSINT для аналізу фотографій або зображень, де важливо ідентифікувати об'єкти, текст або навіть місця, що фігурують на фото. Наприклад, якщо на фотографії зображено певну будівлю, можна за допомогою Google Lens швидко знайти її розташування, історію або інші деталі. В OSINT це використовується для перевірки зображень, пошуку їхнього походження та аналізу контексту. Інтерфейс Google Lens для пошуку за зображенням показано на рисунку 2.17.

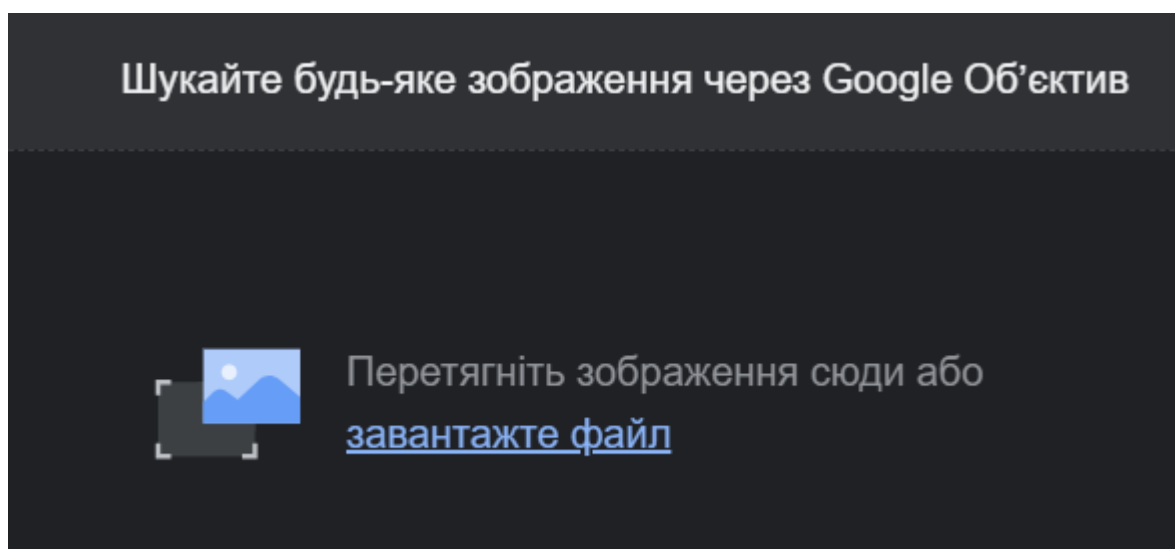


Рис. 2.17 – Google Lens

Використання *Google Maps* є ще одним важливим інструментом для географічного аналізу. Завдяки можливості переглядати карти, будівлі, вулиці, а також визначати географічні координати, Google Maps надає ефективні інструменти для

		Новіцький В.С.			ККІКБ.КР.Б – 125 – 33 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		36

роботи з даними місцевості. Це особливо корисно для розвідників та дослідників, які займаються аналізом території або намагаються вивчити доступні дані про конкретні географічні об'єкти. Google Maps дозволяє точно визначити місце розташування об'єктів, переглядати дороги, зони та інші елементи інфраструктури, що може бути корисно при проведенні розслідувань або для визначення потенційних точок доступу до певних локацій. Інтерфейс Google Maps показано на рисунку 2.18.

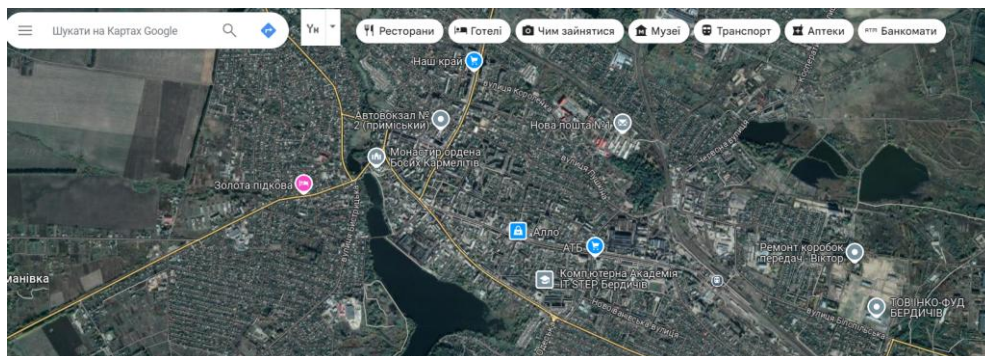


Рис. 2.18 – Google Maps

Ці інструменти Google дозволяють проводити детальну перевірку інформації, виконувати аналіз місцевості та збирати потрібні дані з відкритих джерел. Вони є невід'ємною частиною збору OSINT і суттєво підвищують ефективність процесу збору та обробки інформації.

Висновки до другого розділу

У другому розділі було обґрунтовано вибір інструментів та середовища для безпечного збору OSINT-даних. Для забезпечення анонімності та захисту дослідника було використано віртуальне середовище VirtualBox, спеціалізовану операційну систему TraceLabs OSINT VM, браузер Tor та VPN-сервіс Windscribe. Описано набір веб-інструментів urlscan.io, VPNAPI.io, IPQualityScore, програмні утиліти Maltego, Recon-ng, Holeyhe, Nmap, Whois, а також сервіси Google (Google Search, Google Maps, Google Lens), які дозволяють здійснювати технічний і контекстний аналіз, пошук осіб та мережевих об'єктів. Сукупність обраних інструментів охоплює основні потреби OSINT-дослідження, забезпечуючи ефективність, гнучкість і безпеку роботи.

		Новіцький В.С.			ККІКБ.КР.Б – 125 – 33 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		37

РОЗДІЛ 3 ПРАКТИЧНЕ ЗАСТОСУВАННЯ OSINT

3.1 Підготовка віртуального середовища

Для створення віртуального середовища було використано програму VirtualBox. Інсталяційний пакет було завантажено з офіційного сайту[7]. Інсталяція VB зображено на рисунку 3.1.

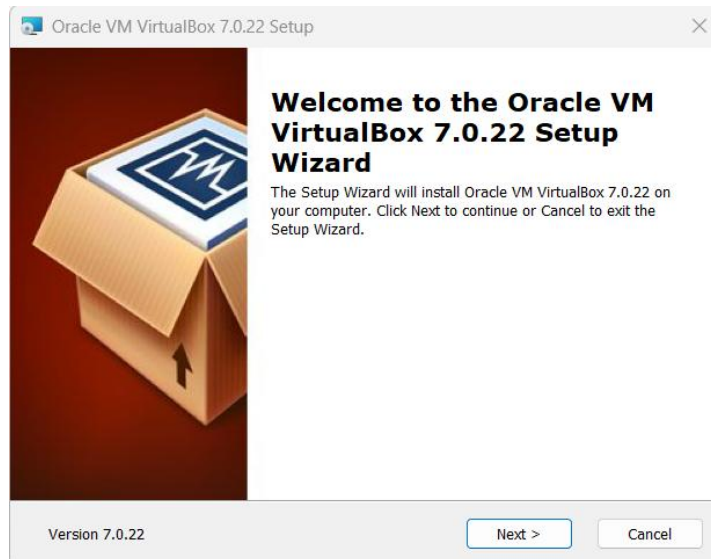


Рис. 3.1 – Встановлення VirtualBox

Було додано віртуальну машину Trace Labs, спеціалізовану на зборі та аналізі відкритих джерел інформації(рис. 3.2). Інсталяційний образ було завантажено з офіційного сайту.

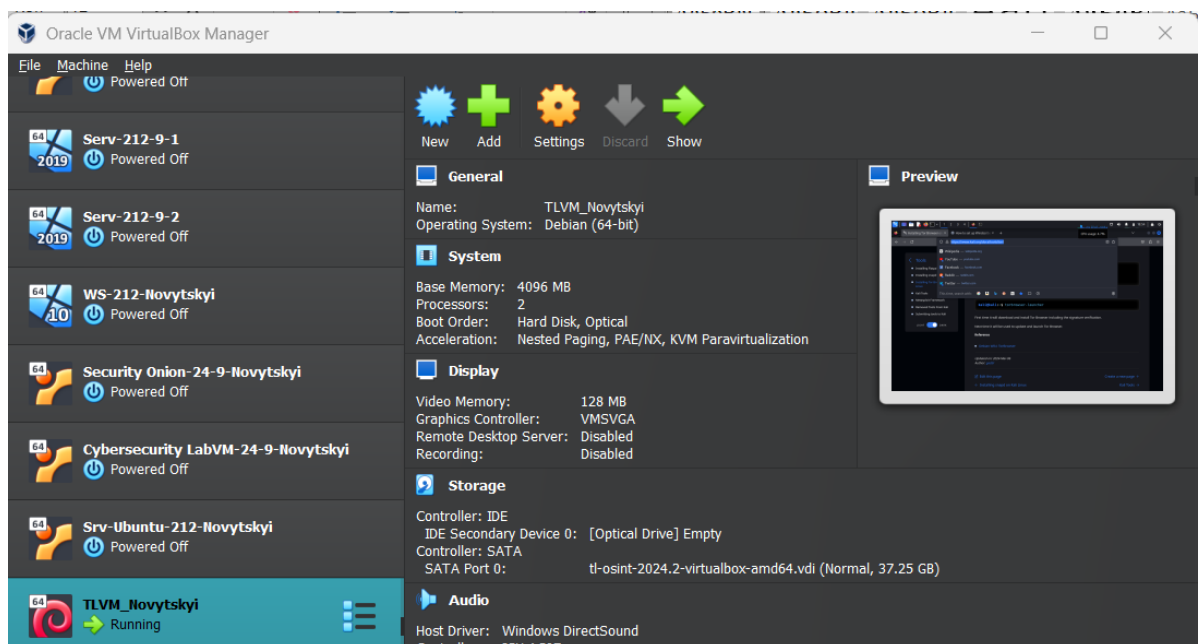


Рис. 3.2 – Імпортована віртуальна машина Trace Labs

		Новіцький В.С.			ККІКБ.КР.Б – 125 – 33 – ПЗ	Арк.
		Покотило О.А.				38
Змн.	Арк.	№ докум.	Підпис	Дата		

Для забезпечення анонімності під час роботи в Інтернеті було встановлено браузер Tor[8]. Для встановлення було використано термінал віртуальної машини і менеджер пакетів apt. Виконання встановлення лаунчера Tor показано на рисунку 3.3.

```

TLVM_Novytskyi [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
osint@tlosint: ~
File Actions Edit View Help
$ sudo apt install -y tor torbrowser-launcher
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
The following packages were automatically installed and are no longer require
d:
  fonts-noto-color-emoji libpython3.11-minimal libpython3.11-stdlib
  
```

Рис. 3.3 – Встановлення torbrowser-launcher

Для запуску інсталяції було використано команду `kali@kali:~$ torbrowser-launcher`.

Додатково було завантажено та налаштовано VPN-сервіс WindScribe. Він шифрує інтернет-з'єднання та дозволяє приховати справжнє місце розташування користувача, забезпечуючи додатковий рівень захисту під час використання віртуального середовища. Для використання даного VPN потрібно зареєструватися, тому було створено акаунт Google, яку буде використано в подальшому для реєстрації на інших веб-сайтах.

У процесі реєстрації акаунта Google було вирішено використовувати не власні дані, щоб забезпечити додатковий рівень захисту та анонімності під час збору інформації. Це дозволяє мінімізувати ризики, пов'язані з можливим витоком особистої інформації або зловживанням акаунтом. Використовувати вигадані або тимчасові дані для реєстрації акаунта є важливою практикою для збереження конфіденційності та уникнення прив'язки до особистих ідентифікаційних даних.

Цей підхід забезпечує додатковий захист, оскільки навіть у разі компрометації акаунта, жодна чутлива особиста інформація не буде доступна зловмисникам. Процес реєстрації зображено на рисунках 3.4, 3.5.

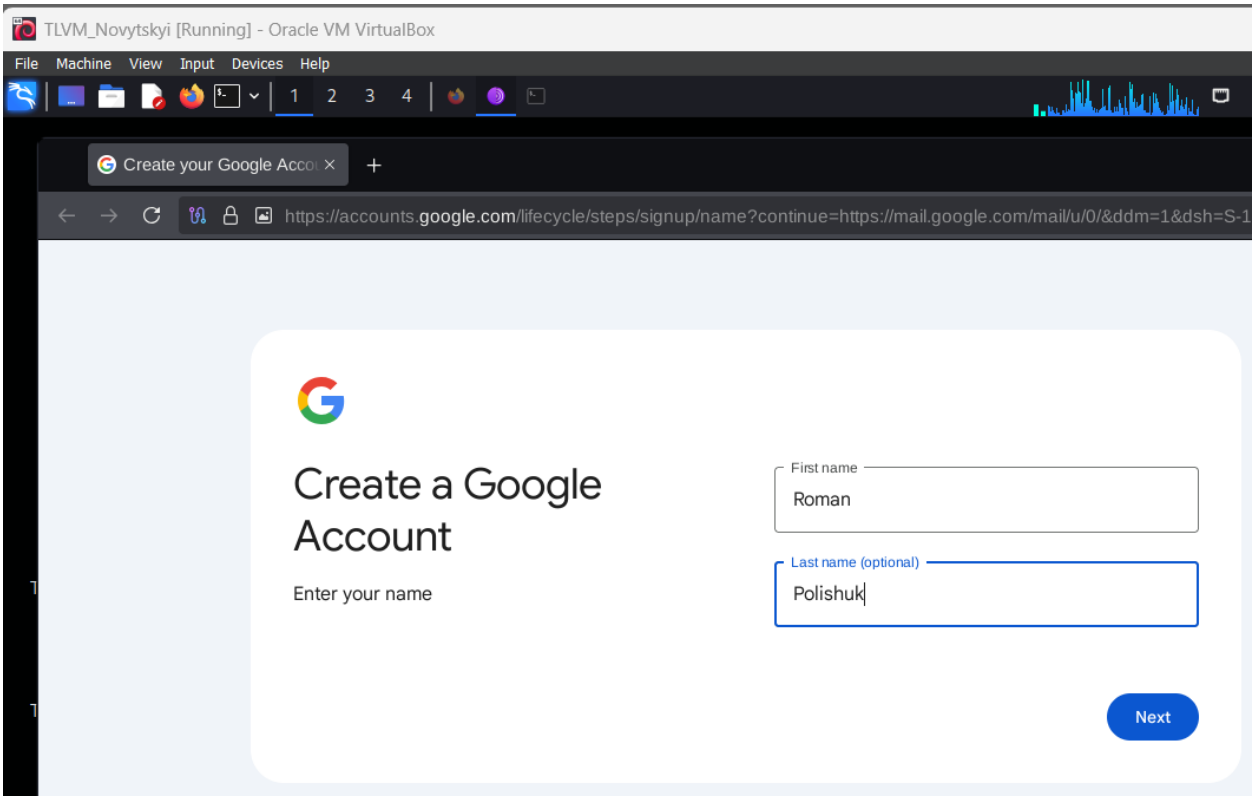


Рис. 3.4 – Введення облікових даних

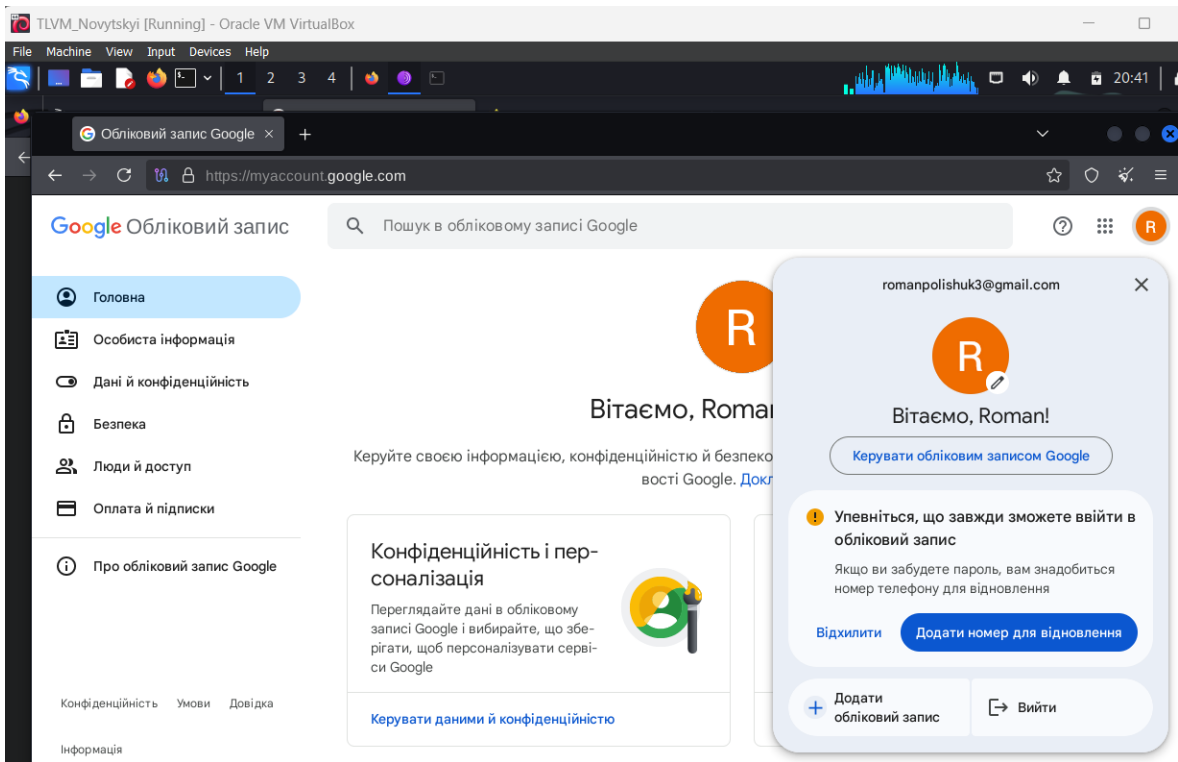


Рис. 3.5 – Результат реєстрації

		Новіцький В.С.			ККІКБ.КР.Б – 125 – 33 – ПЗ	Арк.
		Покотило О.А.				40
Змн.	Арк.	№ докум.	Підпис	Дата		

Для безпечного зберігання паролів і конфіденційної інформації на Kali Linux було встановлено менеджер паролів KeePass(рис. 3.6). Це дозволяє зберігати паролі в зашифрованому вигляді та уникати їх втрати або крадіжки[10](рис. 3.7).

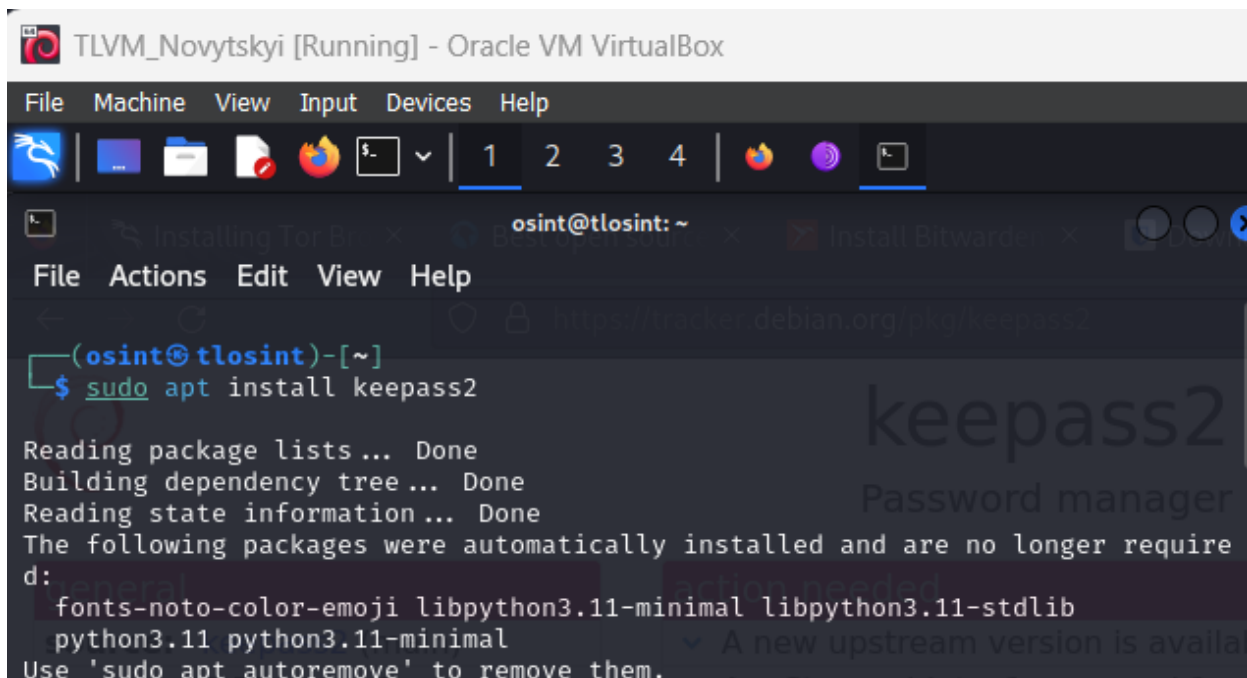


Рис. 3.6 – Встановлення KeePass

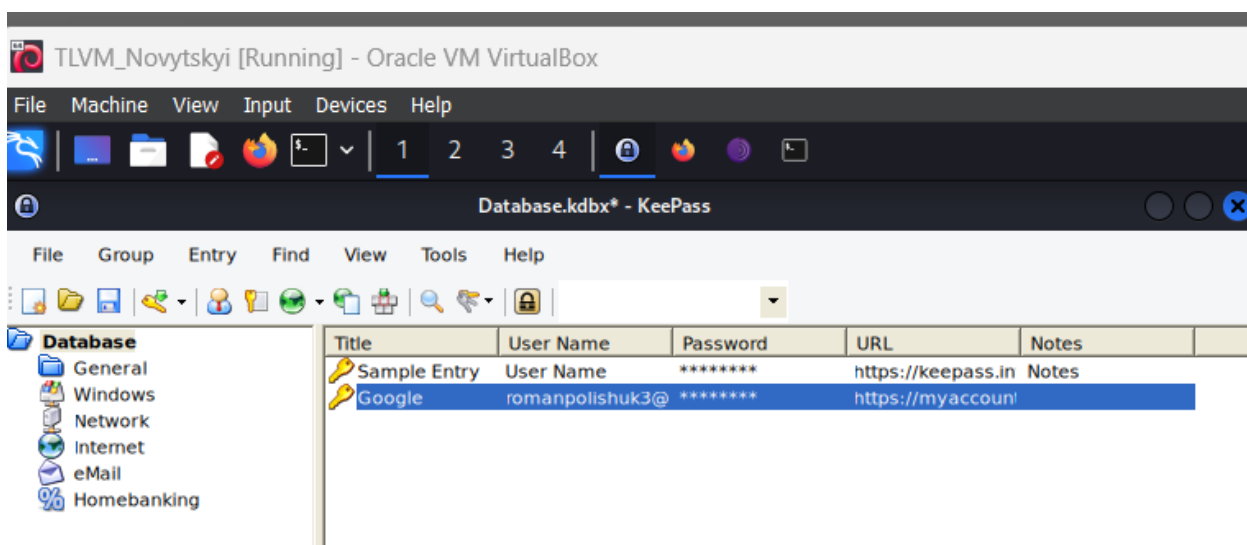


Рис. 3.7 – Структура KeePass

KeePass – це безкоштовний, відкритий менеджер паролів, який забезпечує зберігання та організацію паролів у зашифрованих базах даних. Для захисту паролів KeePass використовує потужні алгоритми шифрування, такі як AES-256 або ChaCha20, що гарантує високий рівень безпеки. Користувачі можуть зберігати па-

ролі, а також інші чутливі дані, такі як нотатки, банківські картки та особисті документи. KeePass не вимагає підключення до Інтернету для роботи, що дозволяє зберігати дані локально і уникати ризиків, пов'язаних з онлайн-обслуговуванням. Інтерфейс програми простий і зручний, а також підтримує додаткові плагіни для інтеграції з іншими додатками та системами. KeePass підтримує двофакторну автентифікацію і може синхронізуватися між пристроями через різні методи, зокрема за допомогою хмарних сервісів або локальних засобів зберігання.

Далі було використано акаунт Google для авторизації у WindScribe[9]. Роботу VPN-сервісу зображено на рисунку 3.8.

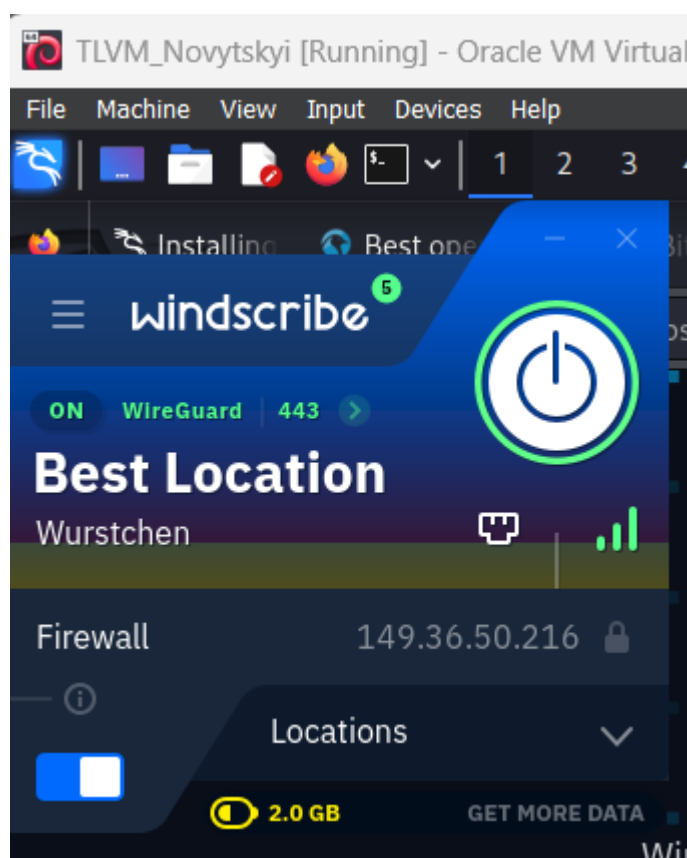


Рис. 3.8 – Робота WindScribe

3.2 Аналіз фішингового електронного листа

У межах практичного дослідження було змодельовано сценарій отримання фішингового електронного листа, що дозволяє проілюструвати реальну загрозу кібербезпеці, яка часто стає відправною точкою для подальших OSINT-розслідувань. Аналіз таких повідомлень допомагає виявити, заголовки, IP-адреси, домени, що ведуть до джерела атаки або використовуються в інфраструктурі зловмисника.

		Новіцький В.С.			ККІКБ.КР.Б – 125 – 33 – ПЗ	Арк.
		Покотило О.А.				42
Змн.	Арк.	№ докум.	Підпис	Дата		

Фішинговий лист – це вид соціальної інженерії, мета якого полягає в обмані користувача з метою отримання конфіденційної інформації: логінів, паролів, банківських реквізитів, або для запуску шкідливого коду. Такі листи зазвичай імітують офіційні повідомлення від авторитетних організацій (банків, держслужб, техпідтримки тощо) або знайомих осіб. Візуально вони можуть бути оформлені професійно, використовуючи логотипи, кольори та шаблони, характерні для справжніх компаній.

Фішингові повідомлення можуть містити:

- посилання на фальшиві вебсайти, які зовні ідентичні справжнім, але призначені для збору введених користувачем даних;
- вкладення з шкідливим ПЗ, яке активується при відкритті;
- елементи паніки або терміновості, щоб спонукати жертву до дій без належної перевірки (наприклад, «Ваш акаунт буде заблоковано», «Термінове оновлення безпеки» тощо).

На рисунку 3.9 представлено приклад фішингового листа, використаного у цьому сценарії. Він містить підозріле посилання, надійшов із сумнівної адреси і має елементи шаблонного оформлення, що є характерними ознаками шахрайського повідомлення.

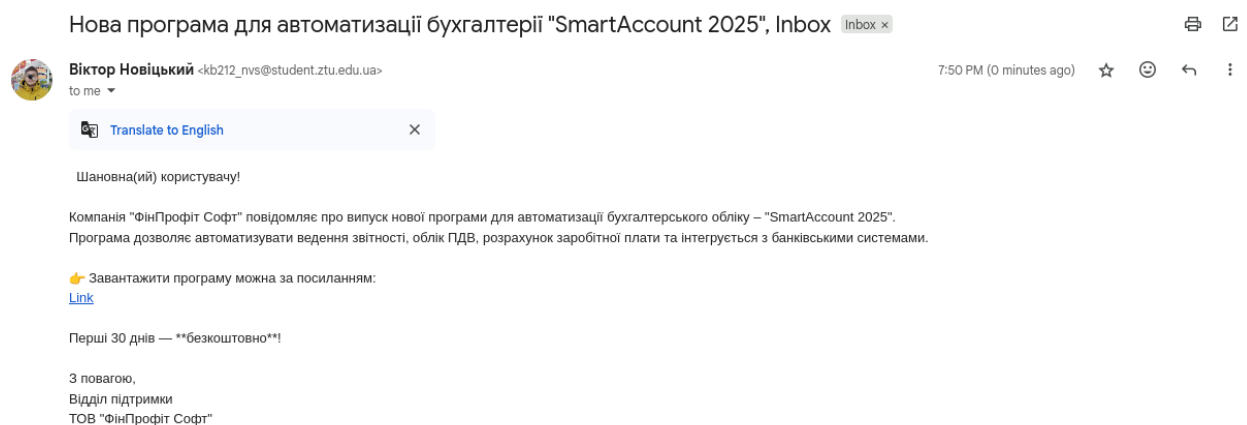


Рисунок 3.9 – Фішинговий лист

У межах дослідження файл, що був вкладенням у фішинговий лист, було завантажено на сервіс VirusTotal для перевірки на наявність шкідливого програмного забезпечення. Цей онлайн-інструмент дозволяє здійснити аналіз файлів або URL за допомогою десятків антивірусних рушіїв і систем виявлення загроз. Він широко

		Новіцький В.С.			ККІКБ.КР.Б – 125 – 33 – ПЗ	Арк.
		Покотило О.А.				43
Змн.	Арк.	№ докум.	Підпис	Дата		

використовується фахівцями з кібербезпеки для швидкого отримання звіту щодо потенційних ризиків. На рисунку 3.10 зображено результат перевірки вкладки, де видно, як більшість систем безпеки класифікували файл як загрозу.

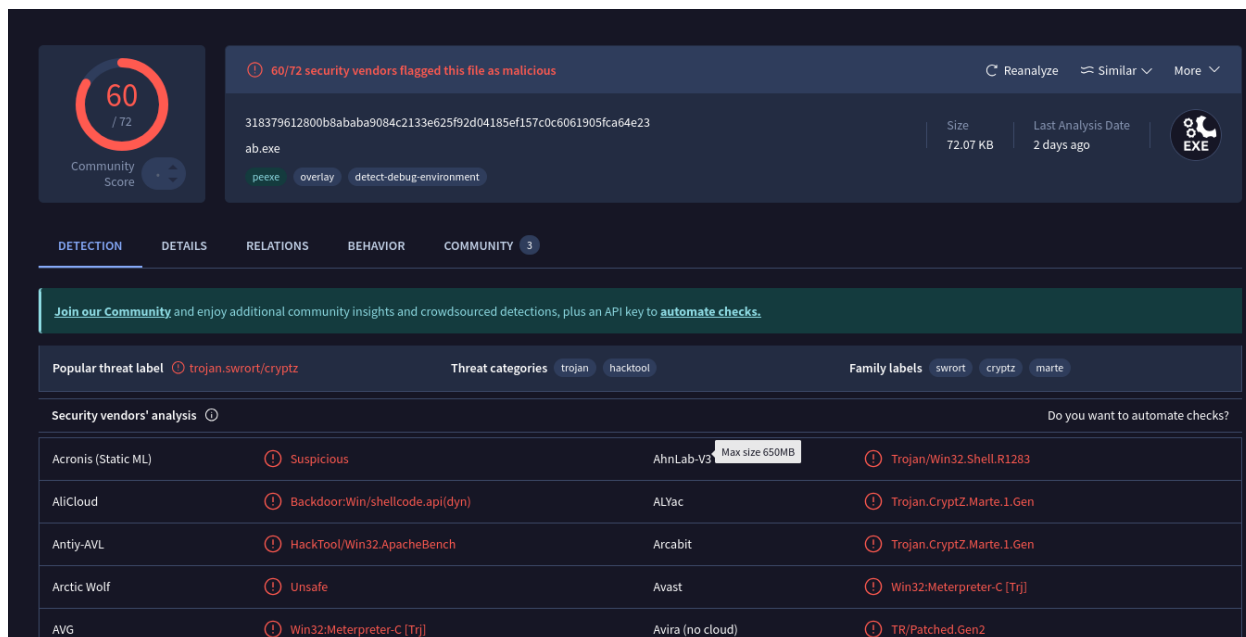


Рисунок 3.10 – Результати перевірки файлу у VirusTotal

Результати сканування показали, що 60 з 72 антивірусів визнали файл небезпечним. Це свідчить про високу ймовірність того, що вкладення містить шкідливий код. У таких випадках зазвичай ідеться про трояни, бекдори, шпигунські програми, кейлогери або інші типи шкідливого ПЗ, здатного викрадати дані або порушити функціонування системи.

Фішингові вкладення часто маскуються під документи, архіви або інші «нешкідливі» формати файлів, але після відкриття ініціюють виконання небезпечних процесів. Зловмисники можуть використовувати ці механізми для збору облікових даних, зараження системи, створення бекдорів чи завантаження інших вірусів.

Запуск програм або відкриття файлів з невідомих або ненадійних джерел несе значну загрозу для інформаційної безпеки. Без попереднього аналізу такі дії можуть призвести до повного компрометування системи, втрати конфіденційної інформації або встановлення контролю над комп'ютером третім особам. Тому використання сервісів на кшталт VirusTotal є важливим етапом у виявленні загроз на ранній стадії.

Після відкриття заголовка електронного листа було отримано детальну технічну інформацію про його надсилання. У полі Received виявлено адресу 209.85.220.41, яка відіграє ключову роль у ланцюжку доставки повідомлення.

На цьому етапі ще не достеменно відомо, кому належить ця IP-адреса, тому для подальшого аналізу була запланована перевірка за допомогою спеціалізованих OSINT-інструментів. Заголовок електронного листа з усією технічною інформацією наведено на рисунку 3.11.

Original Message

Message ID	<CAPKgnNhSYV4oxZda4DseXzs2Kzo7WcOcP=HLj4Bb2dOLU5qA@mail.gmail.com>
Created at:	Sat, Jun 14, 2025 at 7:50 PM (Delivered after 12 seconds)
From:	Віктор Носіцький <kb212_nvs@student.ztu.edu.ua>
To:	"romanpolishuk3@gmail.com" <romanpolishuk3@gmail.com>
Subject:	Нова програма для автоматизації бухгалтерії "SmartAccount 2025", Inbox
SPF:	NONE with IP 209.85.220.41 Learn more
DKIM:	"PASS" with domain ztu.edu.ua Learn more
DMARC:	"FAIL" Learn more

[Download Original](#) [Copy to clipboard](#)

Рис. 3.11 – Заголовок фішингового електронного листа

Для подальшого аналізу було використано інструмент WHOIS, який дозволяє отримати реєстраційну інформацію про IP-адресу. За допомогою цього сервісу вдалося визначити власника адреси, контактні дані та організацію, якій вона належить. Це важливий етап, який допомагає ідентифікувати, чи є IP-адреса пов'язана з відомими сервісами або потенційно підозрілими ресурсами.

Результати аналізу WHOIS показали, що IP-адреса 209.85.220.41 належить інфраструктурі серверів компанії Google (рис. 3.12), що підтверджує офіційне походження адреси та дає змогу зробити висновки щодо легітимності серверів, які брали участь у доставці листа. Це пояснюється тим, що в системі Gmail усі повідомлення спочатку надходять на сервери Google, тому в заголовках листів часто фігурує IP-адреса саме цих серверів.

		Новіцький В.С.			ККІКБ.КР.Б – 125 – 33 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		45

```
(osint@flosint) [~]
$ whois 209.85.220.41

#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
#
# Copyright 1997-2025, American Registry for Internet Numbers, Ltd.
#

From: Виктор Новицький <kb212_nvs@student.znu.edu.ua>
NetRange: 209.85.128.0 - 209.85.255.255
CIDR: 209.85.128.0/17
NetName: GOOGLE
NetHandle: NET-209-85-128-0-1
Parent: NET209 (NET-209-0-0-0-0)
NetType: Direct Allocation
OriginAS:
Organization: Google LLC (GOGL)
RegDate: 2006-01-13
Updated: 2012-02-24
Ref: https://rdap.arin.net/registry/ip/209.85.128.0
```

Рис. 3.12 – Використання інструменту whois

У фішинговому листі містилось посилання на сайт limewire.com, який є відомим ресурсом, пов’язаним із поширенням небезпечного програмного забезпечення. Для детального аналізу цього сайту був використаний сервіс urlscan.io, що дозволяє дослідити структуру веб-ресурсу, його геолокацію та перевірити наявність загроз.

За результатами аналізу, наведені на рисунку 3.13, було встановлено, що сервери limewire.com розташовані в Португалії. Крім того, Google Safe Browsing позначив цей сайт як Malicious, що свідчить про те, що на ресурсі можуть бути присутні шкідливі елементи, зокрема файли з вірусами чи троянами.

Таким чином, посилання з фішингового листа веде на потенційно небезпечний сайт, де знаходився шкідливий файл, що підтверджує ризик зараження при взаємодії з цим ресурсом (рис. 3.13).

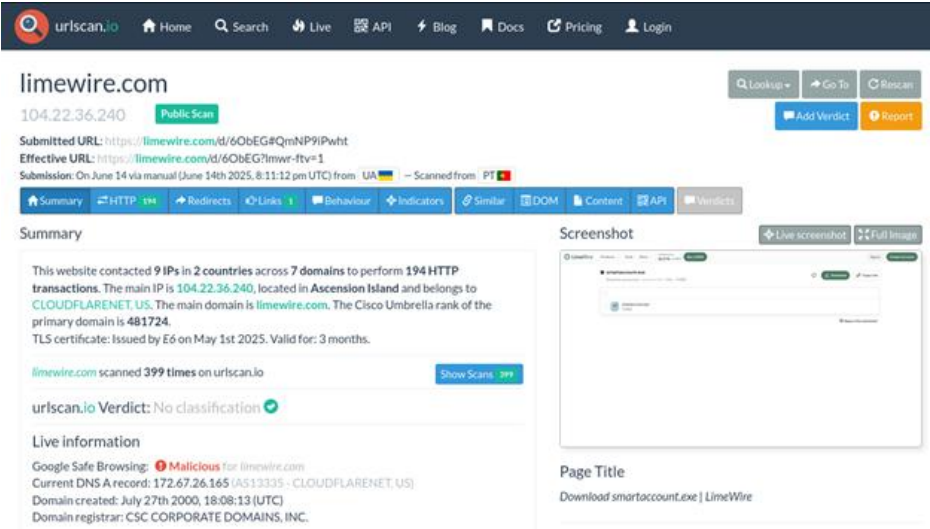


Рис. 3.13 – Результат перевірки з використанням urlscan.io

Для аналізу електронної пошти kb212_nvs@student.ztu.edu.ua був використаний інструмент Holehe, який спеціалізується на перевірці наявності заданої поштової адреси на різних популярних веб-сайтах і сервісах. Holehe дозволяє швидко з'ясувати, чи існує акаунт, пов'язаний із цією електронною адресою, на платформах соціальних мереж, форумах, поштових службах та інших ресурсах[26]. Результат аналізу показав, що дана пошта не зареєстрована і не використовується на жодному з перевірених сайтів (рис. 3.14).

```
*****
kb212_nvs@student.ztu.edu.ua
*****
[+] about.me
[+] akiba.com
[-] amazon.com
[+] anicdn.com
[-] any.do
[-] archive.org
[-] armurrie-auxerre.com
[+] atlassian.com
[-] axonaut.com
[+] babeshow.co.uk
[+] badeggsonline.com
[+] bang-midi.com
[+] biotechnologyforum.com
[+] bitmli.com
[+] blackcar.com
[+] blackworldforum.com
[-] blip.fm
[+] forum.blitzkrieg.org
[+] bluegrassrivals.com
[-] bodybuilding.com
[+] buyseacoffee.com
[+] discussion.cambridge-mt.com
[-] caringbridge.org
[+] chinaphonewares.com
[+] clashfarm.com
[+] codcademy.com
[+] forum.codeigniter.com
[+] codepen.io
[-] coroflot.com
[+] cpaelites.com
[+] cpahero.com
[+] cracked.to
[+] crexads.com
[+] deliveron.com
[+] deenforums.net
[-] devrant.com
[+] diigo.com
[+] discord.com
[-] docker.com
[+] doombox.fr
[+] ebay.com
[+] elite.cc
```

Рис. 3.14 – Використання Holehe для перевірки електронної адреси

Відсутність поштової адреси у відкритих базах може свідчити про кілька варіантів. По-перше, це може бути нова або маловживана адреса, яка ще не використовувалась для реєстрації акаунтів у відомих сервісах. По-друге, це може вказувати на те, що електронна пошта є тимчасовою або фіктивною, створеною спеціально для одноразового використання, наприклад, для розсилки фішингових листів або спаму.

Такий факт ускладнює верифікацію відправника, оскільки відсутність слідів в Інтернеті обмежує можливість перевірки історії та репутації адреси. Це підвищує ризик використання адреси в шахрайських схемах, адже нові або фейкові пошти

		Новіцький В.С.			ККІКБ.КР.Б – 125 – 33 – ПЗ	Арк.
		Покотило О.А.				47
Змн.	Арк.	№ докум.	Підпис	Дата		

часто застосовуються зловмисниками для маскування своєї справжньої ідентичності.

Для подальшого аналізу електронної пошти kb212_nvs@student.ztu.edu.ua був використаний інструмент Maltego, який дозволяє здійснювати глибокий пошук зв'язків між об'єктами в цифровому просторі[25]. Maltego використовує трансформації, що дозволяють автоматично витягувати інформацію про домени, IP-адреси та пов'язані об'єкти, надаючи візуальне представлення у вигляді графів(рис. 3.15).

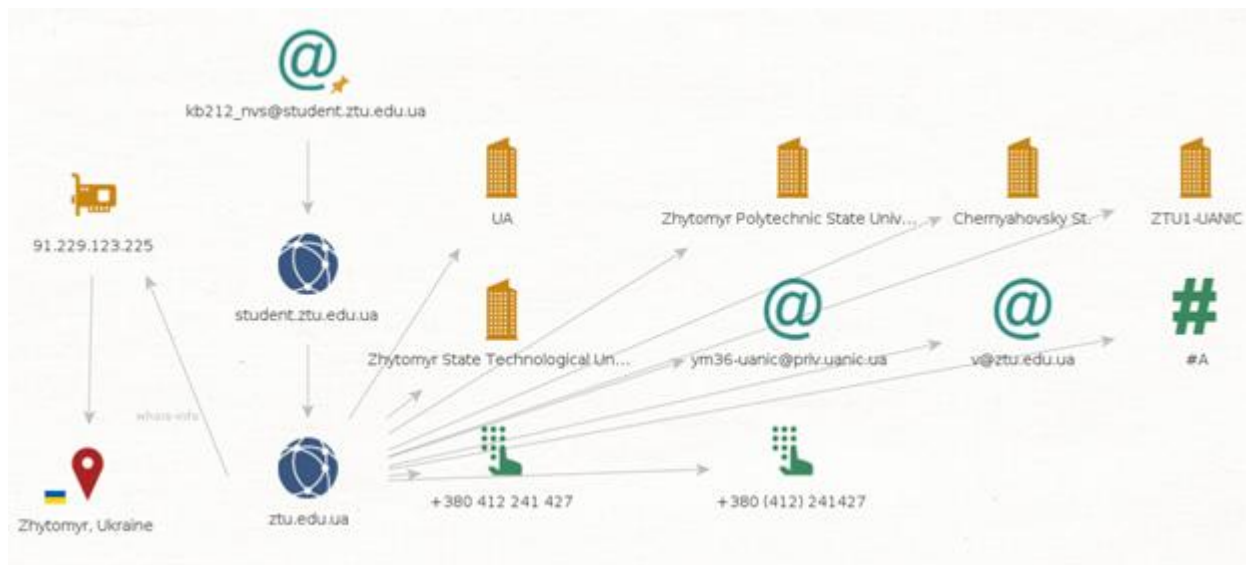


Рис. 3.15 – Граф аналізу пошти у Maltego

За допомогою Maltego було визначено, що домен, до якого належить пошта – `ztu.edu.ua`. Цей домен ідентифікує навчальний заклад, а саме ДУ “Житомирська політехніка”(Zhytomyr Polytechnic State University). Визначення домену є важливим кроком, оскільки дає змогу підтвердити офіційну приналежність пошти до певної організації.

Наступним етапом стала трансформація для отримання IP-адреси, що асоціюється з доменом `ztu.edu.ua`. Аналіз показав, що IP-адреса належить географічно Житомиру, Україна, що відповідає місцю розташування навчального закладу. Це підтверджує легітимність домену та його зв'язок із реальним об'єктом у мережі.

У ході практичного дослідження було проаналізовано фішинговий електронний лист, виявлено IP-адресу сервера доставки, перевірено вкладений файл за до-

помогою сервісу VirusTotal, а також досліджено підозріле посилання на сайт lime-wire.com через urlscan.io. Додатково перевірено електронну адресу відправника за допомогою HOLEHE та Maltego, що дозволило визначити її зв'язок із доменом ztu.edu.ua та підтвердити належність до Житомирської політехніки.

Отримані результати дозволили зібрати достатньо технічної інформації для початкової оцінки загроз та легітимності об'єктів. Надалі зібрані дані можуть бути передані фахівцям для глибшого аналізу без використання OSINT-методів, зокрема в рамках цифрової криміналістики або інцидент-респонсу.

3.3 Отримання інформації про IP-адресу

У рамках другого сценарію моделюється ситуація, коли в результаті атаки на локальну мережу вдається зафіксувати IP-адресу, яка, ймовірно, належить зловмиснику. Така адреса може бути виявлена в логах мережевого обладнання, систем моніторингу безпеки або серверах, які зазнали несанкціонованого доступу. Метою OSINT-аналізу є отримання додаткової інформації про цю IP-адресу: її географічне розташування, приналежність до певного провайдера, підозрілу активність, використання анонімізаторів тощо. Для дослідження була обрана IP-адреса 149.36.50.216.

Першим кроком у дослідженні IP-адреси 149.36.50.216 було використання фреймворку Recon-ng, який є зручним засобом автоматизованого збору відкритої розвідувальної інформації. У рамках аналізу було задіяно модуль recon/hosts-hosts/reverse_resolve, що дозволяє виконати зворотне DNS-розв'язання IP-адреси, тобто визначити доменне ім'я, яке прив'язане до конкретної IP.

У результаті запуску модуля було отримано доменне ім'я unn-149-36-50-216.datapacket.com, що відповідає досліджуваній IP-адресі (рис. 3.16). Особливу увагу було звернено на основний домен datapacket.com, оскільки він вказує на хостинг-провайдера або інфраструктуру, що може надавати серверні потужності стороннім клієнтам, у тому числі зловмисникам.

		Новіцький В.С.			ККІКБ.КР.Б – 125 – 33 – ПЗ	Арк.
		Покотило О.А.				49
Змн.	Арк.	№ докум.	Підпис	Дата		

Отримана інформація дозволяє перейти до подальшого аналізу домену datapacket.com, щоб з'ясувати, чи асоціюється цей ресурс із анонізаторами, VPN-сервісами, або був помічений у шкідливій активності.

```
[recon-ng][default][viewdns_reverse_whois] > modules load hosts-hosts/reverse_resolve
[recon-ng][default][reverse_resolve] > options set source 149.36.50.216
SOURCE => 149.36.50.216
[recon-ng][default][reverse_resolve] > run
[*] Country: None
[*] Host: unn-149-36-50-216.datapacket.com
[*] Ip_Address: 149.36.50.216
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
SUMMARY
[*] 1 total (0 new) hosts found.
[recon-ng][default][reverse_resolve] >
```

Рис. 3.16 – Зворотнє DNS-розв'язання IP-адреси

На наступному етапі розслідування було використано модуль recon/domains-hosts/hackertarget у середовищі Recon-ng. Цей модуль призначений для отримання IP-адрес, які пов'язані з певним доменом, шляхом взаємодії з API сервісу HackerTarget[14]. Метою було визначення масштабів інфраструктури, пов'язаної з доменом datapacket.com.

У результаті роботи модуля було виявлено 42 унікальні IP-адреси, які асоціюються з цим доменом (рис. 3.17). Така кількість адрес вказує на наявність великої серверної інфраструктури, що потенційно може бути частиною VPN-сервісу, проксі-мережі або хмарної платформи, яку орендують різні користувачі, зокрема й зловмисники.

Подібна структура характерна для компаній, що надають послуги з анонізації трафіку, оренди VPS чи хостингу з мінімальною ідентифікацією користувача. Це дозволяє зробити припущення, що IP-адреса, з якої було здійснено атаку, могла бути динамічно призначена одному з клієнтів сервісу datapacket.com, що ускладнює ідентифікацію кінцевого зловмисника.

		Новіцький В.С.			ККІКБ.КР.Б – 125 – 33 – ПЗ	Арк.
		Покотило О.А.				50
Змн.	Арк.	№ докум.	Підпис	Дата		

```

[recon-ng][default][viewdns_reverse_whois] > modules load hacker
[recon-ng][default][hackertarget] > options set source datapacket.com
SOURCE => datapacket.com
[recon-ng][default][hackertarget] > run

Lab: _____ TL Vault
DATAPACKET.COM

[*] Country: None
[*] Host: datapacket.com
[*] Ip_Address: 46.234.110.151
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
-----
[*] Country: None
[*] Host: internal.api.datapacket.com
[*] Ip_Address: 46.234.110.135
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
-----
[*] Country: None
[*] Host: autoinstall.datapacket.com
[*] Ip_Address: 185.102.218.219
[*] Latitude: None
[*] Longitude: None
[*] Notes: None

```

Рис. 3.17 – Використання hackertarget для аналізу домену

На наступному етапі дослідження IP-адреси було здійснено її перевірку за допомогою онлайн-сервісу VPNAPI.io. Цей веб-ресурс спеціалізується на виявленні ознак використання анонімізуючих технологій, таких як VPN, проксі-сервери чи TOR-вузли. Після введення IP-адреси у відповідне поле сервіс підтвердив, що вона дійсно належить VPN-провайдеру. Це ще раз вказує на високий рівень анонімності, який міг використовувати зловмисник (рис. 3.18).

Для поглибленої перевірки було також використано інструмент IPQualityScore, який дозволяє оцінити потенційну шкідливість IP-адрес, аналізуючи ознаки ботнет-активності, використання анонімизаторів, спам-репутацію та інші фактори. Результатом аналізу став максимальний Fraud Score 100, що свідчить про дуже високий рівень підозри щодо використання цієї адреси у зловмисній діяльності. Також сервіс підтвердив використання VPN та вказав геолокацію — Німеччина, м. Франкфурт (рис. 3.19).

API Output

```
{
  "ip": "149.36.50.216",
  "security": {
    "vpn": true,
    "proxy": false,
    "tor": false,
    "relay": false
  },
}
```

Рис. 3.18 – Перевірка за допомогою VPNAPI.io

IP Address 149.36.50.216	IP Address Reputation & Risk Details: <table border="0"> <tr><td>Country:</td><td>DE </td></tr> <tr><td>City:</td><td>Frankfurt am Main</td></tr> <tr><td>Region:</td><td>Hesse</td></tr> <tr><td>Hostname:</td><td>unn-149-36-50-216.datapacket.com</td></tr> <tr><td>ISP:</td><td>Cogent Communications</td></tr> <tr><td>Organization:</td><td>Windscribe VPN</td></tr> <tr><td>ASN:</td><td>212238</td></tr> <tr><td>Proxy Status:</td><td>true</td></tr> <tr><td>VPN Status:</td><td>true Active VPN</td></tr> <tr><td>TOR Status:</td><td>false</td></tr> <tr><td>Fraud Score:</td><td>100 75+ = suspicious 85+ = risky 90+ = high risk</td></tr> <tr><td>Abuse Velocity:</td><td>Premium required.</td></tr> <tr><td>Recent Abuse:</td><td>true</td></tr> <tr><td>Bot Activity:</td><td>true</td></tr> <tr><td>Frequent Abuser:</td><td>Upgrade your plan for better data and blocklists.</td></tr> <tr><td>High Risk Attacks:</td><td>Upgrade your plan for better data and blocklists.</td></tr> </table>	Country:	DE	City:	Frankfurt am Main	Region:	Hesse	Hostname:	unn-149-36-50-216.datapacket.com	ISP:	Cogent Communications	Organization:	Windscribe VPN	ASN:	212238	Proxy Status:	true	VPN Status:	true Active VPN	TOR Status:	false	Fraud Score:	100 75+ = suspicious 85+ = risky 90+ = high risk	Abuse Velocity:	Premium required.	Recent Abuse:	true	Bot Activity:	true	Frequent Abuser:	Upgrade your plan for better data and blocklists.	High Risk Attacks:	Upgrade your plan for better data and blocklists.
Country:	DE																																
City:	Frankfurt am Main																																
Region:	Hesse																																
Hostname:	unn-149-36-50-216.datapacket.com																																
ISP:	Cogent Communications																																
Organization:	Windscribe VPN																																
ASN:	212238																																
Proxy Status:	true																																
VPN Status:	true Active VPN																																
TOR Status:	false																																
Fraud Score:	100 75+ = suspicious 85+ = risky 90+ = high risk																																
Abuse Velocity:	Premium required.																																
Recent Abuse:	true																																
Bot Activity:	true																																
Frequent Abuser:	Upgrade your plan for better data and blocklists.																																
High Risk Attacks:	Upgrade your plan for better data and blocklists.																																
Strictness Level Medium (1 Week Reputation Lookback Period – Level 1) ☒ Allow Public Access Points (less strict) Allow IP addresses from corporate, university, and other public ranges while still detecting the worst offenders within these IP address blocks. ☒ Score this IP address as a mobile device (less strict) This feature adjusts the checks we perform to provide better accuracy for mobile IP addresses. ☒ Lighter Penalties for Mixed Quality IP Addresses (less strict) This feature lowers detection and elevated Fraud Scores for IP addresses shared by good and bad users. Lookup IP																																	

Рис. 3.19 – Перевірка за допомогою IPQualityScore

Комбінація результатів з VPNAPI.io та IPQualityScore дозволяє зробити обґрунтований висновок про використання зловмисником анонімізованого VPN-з'єднання, що ускладнює пряму ідентифікацію джерела атаки. Проте отримані географічні та технічні дані все ще можуть бути використані для подальшої кореляції з іншими подіями в мережі або звернення до провайдера послуг.

Для завершення технічного аналізу було проведено сканування IP-адреси за допомогою інструмента Nmap із ключем `-Pn`, який вимикає попередню перевірку доступності хоста через ICMP (ping). Це дозволяє виконати сканування навіть у випадках, коли пристрій фільтрує ICMP-запити або приховує свою активність в мережі[18]. Метою сканування було виявлення відкритих портів, що могли б свідчити про наявність активних сервісів (рис. 3.20).

```
(venv)-(osint@tlosint)-[~/recon-ng]
$ nmap -Pn 149.36.50.216
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-15 18:45 UTC
Stats: 0:03:25 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 99.99% done; ETC: 18:48 (0:00:00 remaining)
Nmap scan report for unn-149-36-50-216.datapacket.com (149.36.50.216)
Host is up.
All 1000 scanned ports on unn-149-36-50-216.datapacket.com (149.36.50.216) are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
Nmap done: 1 IP address (1 host up) scanned in 205.54 seconds
```

Рис. 3.20 – Сканування відкритих портів за допомогою Nmap

Результати сканування показали, що усі порти знаходяться в закритому стані, що означає відсутність відповідей на спроби з'єднання з будь-яким із типових сервісів. Такий результат може свідчити про кілька варіантів:

1. Використання VPN або проксі-сервера, який автоматично блокує зовнішні підключення;
2. Фаєрвол або фільтрація портів на рівні провайдера або системи користувача;
3. Навмисне маскування активності з боку злоумисника для ускладнення OSINT-аналізу.

Таким чином, відсутність відкритих портів не виключає підозрілу активність, але вказує на високий рівень захищеності чи приховування. Отримані дані слугують додатковим підтвердженням використання засобів анонімізації та можуть бути корисними при подальшому поглибленому розслідуванні поза межами OSINT-інструментів.

У результаті проведеного OSINT-дослідження вдалося встановити, що IP-адреса, з якої, ймовірно, було здійснено несанкціоновану активність у мережі, належить хостингу datapacket.com. Подальший аналіз за допомогою сервісів VPNAPI.io та IPQualityScore підтвердив, що адреса використовує VPN-сервіс, має максимальний рівень ризику (Fraud Score = 100), а її геолокація вказує на Франкфурт, Німеччина. Це може свідчити про спробу злоумисника приховати свою справжню IP-адресу.

Також за допомогою сканування Nmap було встановлено, що всі порти на вказаній IP-адресі закриті, що додатково підтверджує використання VPN або інших засобів фільтрації трафіку.

На основі зібраної інформації можна зробити припущення про навмисну спробу анонімізації з боку потенційного зловмисника. Для подальшого розслідування доцільно передати отримані дані до внутрішньої служби безпеки організації або правоохоронних органів, які можуть виконати глибший аналіз з використанням інструментів доступу до закритих систем, логів серверів, провайдерів, або аналізу поведінки в мережі, що виходить за межі OSINT-методів.

3.4 Визначення локації за IP-камерою відеоспостереження

У рамках третього сценарію змодельовано ситуацію кіберінциденту, під час якого було отримано відеозапис із камери відеоспостереження, місцезнаходження якої невідоме. Для подальшого розслідування поставлено завдання визначити географічне розташування камери на основі доступного зображення. На рисунку 3.21 наведено скріншот із відеопотоку камери.



Рис. 3.21 – Скріншот відеопотоку камери

		Новіцький В.С.			ККІКБ.КР.Б – 125 – 33 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		54

Спочатку було прийнято рішення проаналізувати червону вивіску з написом Wrigley Field, що видно на зображенні з камери (рис. 3.22), за допомогою сервісу Google Lens. Цей інструмент дозволяє здійснити пошук за зображенням, розпізнати об'єкти та отримати додаткову інформацію про них, що може допомогти у визначенні місця розташування камери. Результат аналізу показав, що це вивіска стадіону Wrigley Field, який знаходиться у місті Чикаго, США.

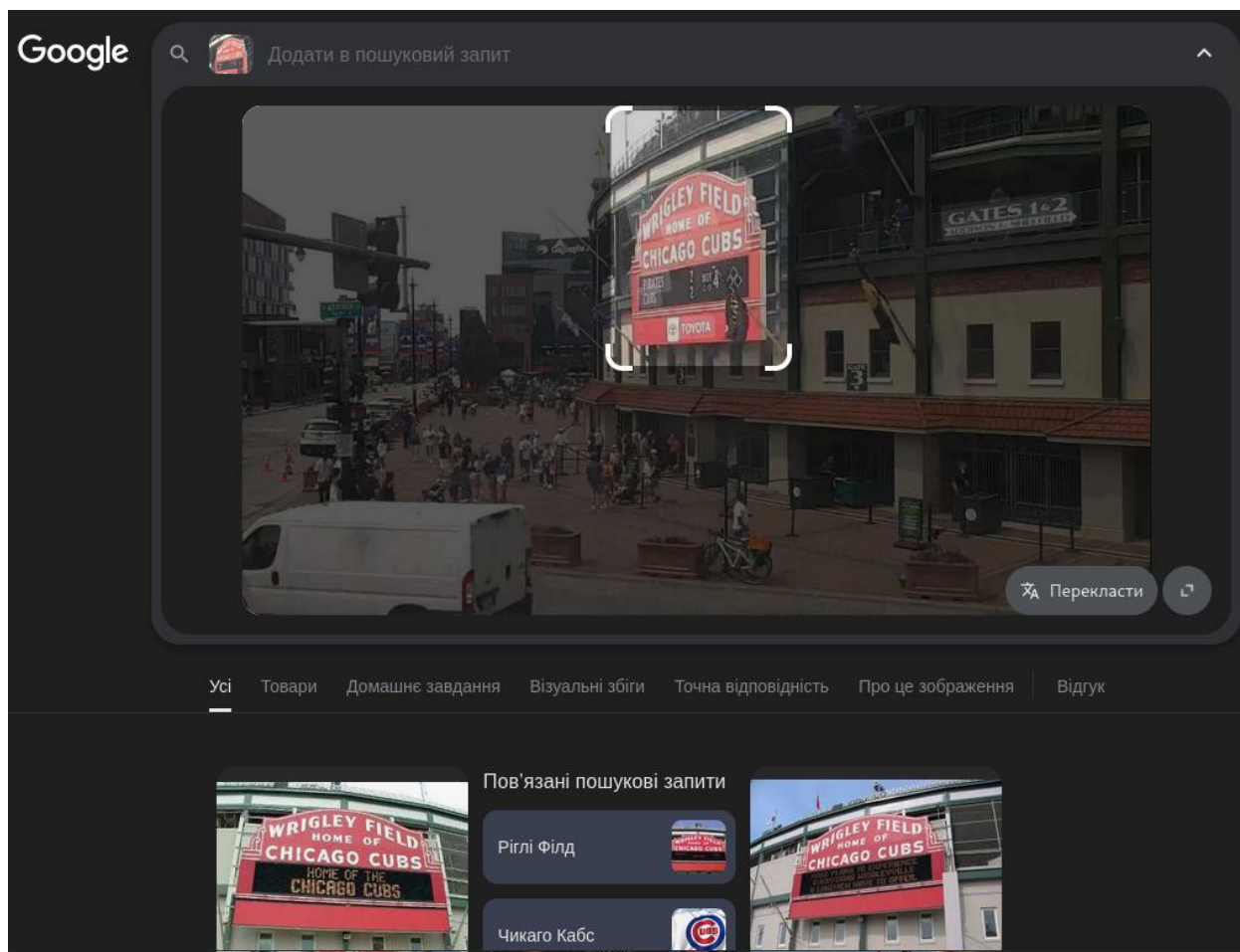


Рис. 3.22 – Використання Google Lens

Далі було проаналізовано табличку з написом “Addison St”, яка за зовнішнім виглядом нагадує вуличний покажчик (рис. 3.23). Для підтвердження місцезнаходження та уточнення деталей було здійснено пошук у пошуковій системі Google з використанням спеціального оператора `site:google.com/maps`, що обмежує результати лише даними з карт Google. На рисунку 3.24 показано скріншот пошукового запиту, який дав змогу підтвердити, що Addison St – це вулиця в місті Чикаго, штат Іллінойс, США. Таким чином, завдяки аналізу елементів на зображенні та пошуковим інструментам, було встановлено точне місце розташування камери

		Новіцький В.С.			ККІКБ.КР.Б – 125 – 33 – ПЗ	Арк.
		Покотило О.А.				55
Змн.	Арк.	№ докум.	Підпис	Дата		



Рис. 3.24 – Табличка з написом “Addison st”

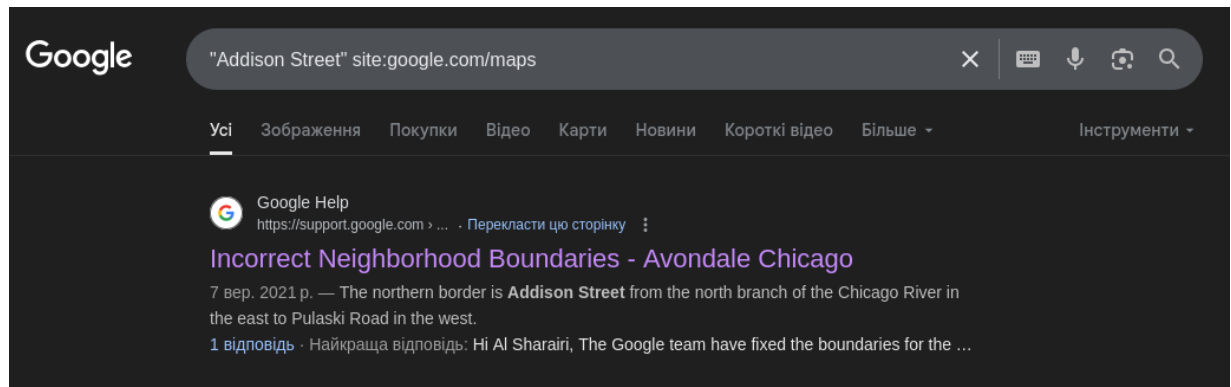


Рис. 3.25 – Пошуковий запит у Google

На завершальному етапі розслідування для верифікації отриманої інформації було використано сервіс Google Maps. За допомогою функції перегляду вулиць (Street View) вдалося знайти ту саму локацію, яку було зафіксовано на зображенні з камери (рис. 3.26). Всі характерні елементи – вивіска Wrigley Field, табличка Addison St, архітектура будівель та розміщення камер – збігаються з реальним виглядом місцевості у Google Maps.

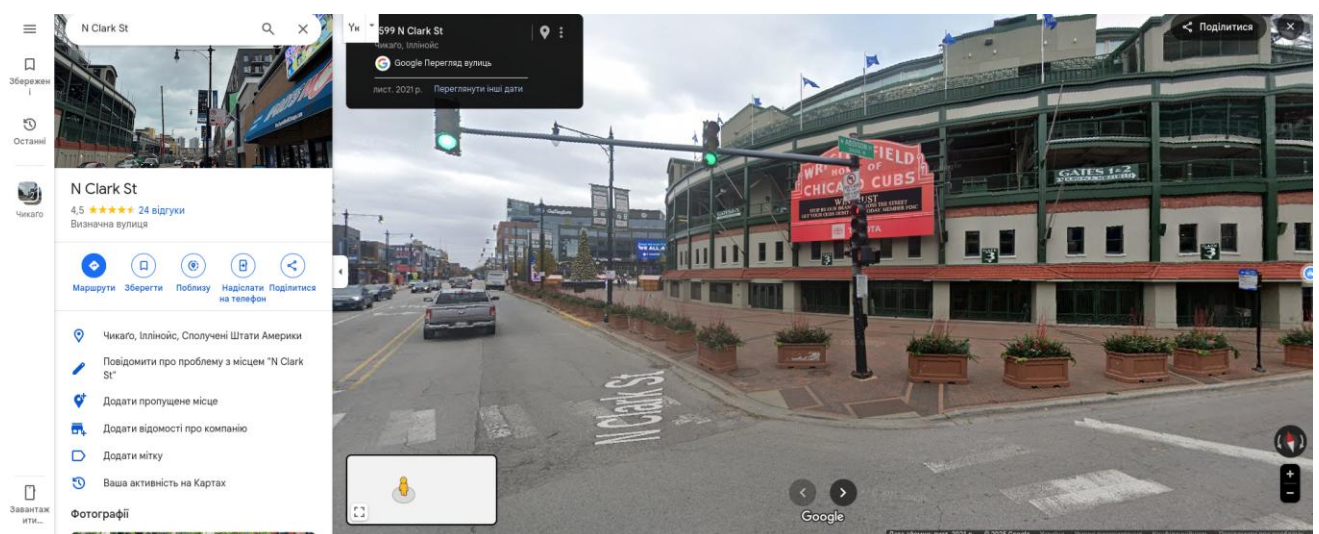


Рис. 3.26 – Вигляд знайденої локації у Google Maps

		Новіцький В.С.			ККІКБ.КР.Б – 125 – 33 – ПЗ	Арк.
		Покотило О.А.				56
Змн.	Арк.	№ докум.	Підпис	Дата		

Це остаточно підтверджує, що камера фізично встановлена в місті Чикаго, поруч зі стадіоном Wrigley Field, і дозволяє зробити висновок про точне її розташування, що може бути використано для подальших дій у межах кіберінциденту. Визначення геолокації дозволяє встановити юрисдикцію, звернутися до відповідних органів, а також дослідити можливі шляхи фізичного доступу до обладнання.

3.5 Узагальнення результатів OSINT-розслідувань

У ході дослідження було змодельовано три практичні сценарії використання OSINT для розслідування кіберінцидентів.

У першому сценарії досліджувався фішинговий лист, отриманий електронною поштою. Аналіз заголовка показав, що IP-адреса відправника належить інфраструктурі Google, що свідчить про використання стороннього поштового сервісу. За допомогою WHOIS було зібрано дані про домен, а VirusTotal підтвердив наявність шкідливого ПЗ у вкладенні. Сервіс urlscan.io надав інформацію про поведінку сайту, на який вело посилання. Holeyhe не виявив активності пошти на платформах, що вказує на її одноразове використання. Maltego дозволив встановити, що домен належить навчальному закладу, а також визначити його географічне розташування. У результаті підтверджено фішинговий характер листа та встановлено потенційне джерело загрози. Результатом стало підтвердження фішингового характеру повідомлення, виявлення джерела доставки та отримання даних про потенційне походження загрози.

У другому сценарії розслідувалася IP-адреса, яка могла бути пов'язана з підозрілою активністю. За допомогою Recon-ng було встановлено домен, пов'язаний із цією адресою, а також перелік інших IP-адрес, що використовують той самий домен, що дало змогу припустити використання VPN або хостинг-сервісу. Цю гіпотезу підтвердили додатково за допомогою сервісів VPNAPI.io та IPQualityScore, які надали інформацію про репутацію IP-адреси, зокрема її зв'язок із VPN-інфраструктурою. Завершальний етап полягав у скануванні IP-адреси за допомогою Nmap, яке показало, що всі порти закриті, і подальший технічний аналіз у цьому напрямку

		Новіцький В.С.			ККІКБ.КР.Б – 125 – 33 – ПЗ	Арк.
		Покотило О.А.				57
Змн.	Арк.	№ докум.	Підпис	Дата		

неможливий. Результатом стало встановлення приналежності IP до VPN, що обмежило можливості точної ідентифікації користувача, але дало розуміння характеру активності.

У третьому сценарії було досліджено фотографію з камери спостереження, завданням стало визначення її точного місцезнаходження. За допомогою Google Lens і Google Search було ідентифіковано характерні об'єкти на зображенні – вивіски та будівлі. Далі, використовуючи Google Maps, вдалося порівняти знайдені елементи з реальною місцевістю та з високою точністю встановити координати точки, з якої зроблене фото. Результатом стало успішне геолокування камери.

У таблиці 3.1 узагальнено основні характеристики трьох розглянутих сценаріїв, у тому числі джерела даних, інструменти, які застосовувалися в ході дослідження, та отримані результати.

Таблиця 3.1

Характеристика досліджених OSINT-сценаріїв

№	Назва сценарію	Джерело даних	Застосовані інструменти	Основні результати
1	Аналіз фішингового листа	Електронна пошта	WHOIS, VirusTotal, urlscan.io, Holehe, Maltego	Виявлено використання серверів Google; підтверджено наявність шкідливого ПЗ; встановлено зв'язок домену з навчальним закладом
2	Аналіз IP-адреси зловмисника	IP-адреса	recon-ng, VPNAPI.io, IPQualityScore, Nmap	Ідентифіковано пов'язані домени; підтверджено використання VPN; всі порти закриті
3	Геолокація камери за зображенням	Фотографія	Google Lens, Google Search, Google Maps	Встановлено точне місцезнаходження камери за характерними об'єктами на фото

Проведений аналіз трьох різнотипних сценаріїв дозволяє виділити як спільні риси, так і суттєві відмінності в процесі застосування OSINT-методів. В усіх випадках базовим етапом було збирання даних з відкритих джерел, їх верифікація та подальше аналітичне опрацювання. Спільною рисою є використання комбінованого підходу – поєднання кількох інструментів задля отримання повнішої картини. Наприклад, для фішингового листа було застосовано одночасно WHOIS, VirusTotal, urlscan.io, Holey та Maltego, що дало змогу охопити як технічну, так і контекстну інформацію. Аналогічно, під час дослідження IP-адреси чи геолокації фото результати досягались лише шляхом послідовного залучення декількох джерел даних.

Водночас, відмінності полягають у природі самих задач. У випадку з IP-адресою основний акцент був на технічному аналізі мережевої інфраструктури, тоді як аналіз фото вимагав візуального зіставлення та використання картографічних сервісів. Це вказує на необхідність адаптації інструментарію відповідно до типу об'єкта розвідки. Важливим практичним висновком стало те, що найбільш результативним є поєднання як технічних, так і контекстно-аналітичних методів: просте виявлення IP чи домену є недостатнім без подальшого аналізу їх зв'язків, поведінки та походження.

Ефективність OSINT у великій мірі залежить від таких чинників, як доступність джерел, актуальність даних, досвід аналітика, а також наявність правильно обраних інструментів. У сценаріях, де було можливо простежити цифрові сліди (наприклад, у випадку фішингової атаки), результати були глибшими та інформативнішими. Натомість аналіз IP-адреси, що виявилася VPN-ресурсом з закритими портами, продемонстрував певні обмеження: навіть при використанні кількох сервісів результат залишився частково невизначеним. Це підкреслює, що не завжди OSINT дозволяє отримати вичерпну відповідь, що деякі джерела можуть бути навмисно обмежені або замасковані.

Таким чином, OSINT – це ефективний, але не універсальний інструмент. Його користь зростає за умови системного підходу, коли для кожного етапу до-

		Новіцький В.С.			ККІКБ.КР.Б – 125 – 33 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		59

слідження обираються релевантні інструменти, а отримані дані проходять подальшу аналітичну обробку. У підсумку можна стверджувати, що OSINT найбільш ефективний у випадках, коли цифрові сліди доступні у відкритих джерелах, а також коли аналітик володіє навичками комбінування різних методів і критичного оцінювання результатів.

Висновки до третього розділу

У третьому розділі було змодельовано три практичні сценарії OSINT-розслідувань, що демонструють можливості відкритого збору інформації у реальних умовах кіберінцидентів. Перший сценарій охоплював аналіз фішингового листа, в рамках якого вдалося виявити шкідливе програмне забезпечення, ідентифікувати поштову інфраструктуру та дослідити домен, з яким була пов'язана підозріла електронна адреса. У другому сценарії було розглянуто аналіз IP-адреси, пов'язаної з атакою на мережу – шляхом застосування OSINT-інструментів було підтверджено використання VPN-сервісу для приховування справжнього джерела атаки. У третьому сценарії виконувалось геолокаційне дослідження камери відеоспостереження, в ході якого вдалося встановити її точне розташування в місті Чикаго завдяки аналізу зображень та вулиць.

Усі три кейси підтверджують ефективність OSINT як методу початкового збору та аналізу інформації при інцидентах у сфері кібербезпеки. Отримані дані можуть бути передані відповідним службам або використані для подальшого, глибшого аналізу із залученням закритих джерел чи правових інструментів.

		Новіцький В.С.			ККІКБ.КР.Б – 125 – 33 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		60

ВИСНОВКИ

У кваліфікаційній роботі було проведено дослідження методів, технік та інструментів OSINT для розслідування кіберінцидентів. Основну увагу зосереджено на аналізі можливостей відкритих джерел інформації для виявлення технічних і непрямих ознак інцидентів, а також на ефективному використанні сучасного інструментарію в умовах обмеженого доступу до внутрішніх систем. Було розглянуто низку сервісів та утиліт, які дозволяють здійснювати збір і перевірку даних про IP-адреси, домени, електронні скриньки, шкідливі посилання та файли.

У процесі роботи систематизовано та перевірено на практиці низку популярних OSINT-інструментів, зокрема Holehe, Maltego, Recon-ng, Nmap, Whois, urlscan.io, VirusTotal, VPNAPI.io та інші. Також розглянуто можливості екосистеми сервісів Google (Google Lens, Search, Maps) у контексті геолокаційного аналізу. Для захисту особистості дослідника під час збору інформації використовувалися безпечні середовища, зокрема TraceLabs OSINT VM, VPN-сервіси (Windscribe), а також браузер Tor.

Практична частина охоплює три модульні сценарії OSINT-розслідувань: аналіз фішингового листа, дослідження анонімної IP-адреси та геолокацію камери спостереження. На основі зібраних даних було встановлено джерела загроз, визначено інфраструктуру VPN, виявлено легітимність відправника, перевірено небезпечність домену limewire.com та локалізовано камеру в місті Чикаго. У результаті встановлено, що OSINT дає змогу формувати первинний інформаційний зріз, який може бути переданий для подальшого технічного, правового або оперативного аналізу.

Результати дослідження підтверджують доцільність використання OSINT у кіберрозслідуваннях як швидкого та доступного методу збору доказів і встановлення первинних зв'язків. Отримані навички та інструменти можуть бути застосовані для підвищення ефективності реагування на інциденти, а також для побудови процесів інформаційної розвідки в межах організаційного захисту.

		Новіцький В.С.			ККІКБ.КР.Б – 125 – 33 – ПЗ	Арк.
		Покотило О.А.				61
Змн.	Арк.	№ докум.	Підпис	Дата		

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Що таке OSINT – розвідка на основі відкритих джерел [Електронний ресурс] – Режим доступу до ресурсу: <https://thetransmitted.com/adlucem/shho-take-osint-open-source-intelligence-rozvidka-na-osnovi-vidkrytyh-dzherel/>.
2. Курс OSINT – розвідка з відкритих джерел та інформаційна безпека [Електронний ресурс] – Режим доступу до ресурсу: https://apps.prometheus.org.ua/learning/course/course-v1:Prometheus+OSINT101+2024_T3/home.
3. What is Open Source Intelligence? [Електронний ресурс] – Режим доступу до ресурсу: <https://www.sans.org/blog/what-is-open-source-intelligence/>.
4. Open Source Intelligence Strategy [Електронний ресурс] – Режим доступу до ресурсу: <https://www.state.gov/open-source-intelligence-strategy>.
5. Open-Source Intelligence (OSINT) Use by Governments [Електронний ресурс] – Режим доступу до ресурсу: <https://hackernoon.com/open-source-intelligence-osint-use-by-governments-802t37gn>.
6. Cyber Intelligence [Електронний ресурс] – Режим доступу до ресурсу: <https://www.cyberint.com>.
7. VirtualBox SDK Reference [Електронний ресурс] – Режим доступу до ресурсу: https://download.virtualbox.org/virtualbox/7.0.22/SDKRef.pdf?source=:ow:o:p:nav:mmddyyVirtualBoxHero_ua.
8. Tor – Інструкція по використанню [Електронний ресурс] – Режим доступу до ресурсу: <https://www.kali.org/docs/tools/tor/>.
9. How to Set Up Windscribe on Linux [Електронний ресурс] – Режим доступу до ресурсу: <https://windscribe.com/knowledge-base/articles/how-to-set-up-windscribe-on-linux/>.
10. KeePass – Official Website [Електронний ресурс] – Режим доступу до ресурсу: <https://keepass.info/>.
11. Windscribe Knowledge Base [Електронний ресурс] – Режим доступу до ресурсу: <https://windscribe.com/knowledge-base/>.

		Новіцький В.С.			ККІКБ.КР.Б – 125 – 33 – ПЗ	Арк.
		Покотило О.А.				62
Змн.	Арк.	№ докум.	Підпис	Дата		

12. Верховна Рада України; Закон від 01.06.2010 № 2297-VI. Про захист персональних даних.
13. National Security Agency. Signals Intelligence (SIGINT) [Електронний ресурс] – Режим доступу: <https://www.nsa.gov/Signals-Intelligence/Overview/>.
14. Recon-ng Tutorial [Електронний ресурс] – Режим доступу: <https://hackertarget.com/recon-ng-tutorial/>.
15. OSINT Investigation: Its Purposes and Types [Електронний ресурс] – Режим доступу до ресурсу: <https://molfar.com/en/blog/osint-investigation-its-purposes-and-types>
16. What is OSINT? [Електронний ресурс] – Режим доступу до ресурсу: <https://blackdotsolutions.com/blog/what-is-osint/>.
17. Інструменти OSINT – GEOINT [Електронний ресурс] – Режим доступу до ресурсу: <https://thetransmitted.com/security/instrumenty-osint-geoint/>.
18. Посібник з Nmap [Електронний ресурс] – Режим доступу: <https://hackyourmom.com/en/kibervijna/posibnyk-z-nmap/>.
19. Загальний регламент захисту даних (GDPR) [Електронний ресурс] – Режим доступу до ресурсу: <https://gdpr-text.com/uk/>.
20. Freedom of Information Act (FOIA) [Електронний ресурс] – Режим доступу до ресурсу: <https://www.foia.gov/about.html>.
21. Кримінальний процесуальний кодекс України [Електронний ресурс] – Режим доступу до ресурсу: <https://zakon.rada.gov.ua/laws/show/4651-17#Text>.
22. OSINT Research Guide [Електронний ресурс] – Режим доступу до ресурсу: <https://usnwc.libguides.com/c.php?g=494120&p=3381426>.
23. OSINT Virtual Machine by Trace Labs [Електронний ресурс] – Режим доступу до ресурсу: <https://www.tracelabs.org/initiatives/osint-vm>.
24. OSINT Analysis of IP Address [Електронний ресурс] – Режим доступу: <https://kr-labs.com.ua/blog/osint-analysis-of-ip-address/>.
25. OSINT [Електронний ресурс] – Режим доступу: <https://www.maltego.com/categories/osint/>.

		Новіцький В.С.			ККІКБ.КР.Б – 125 – 33 – ПЗ	Арк.
		Покотило О.А.				63
Змн.	Арк.	№ докум.	Підпис	Дата		

26. Holehe – The Email Investigation Tool You Need for OSINT
[Електронний ресурс] – Режим доступу: <https://hacklido.com/blog/341-holehe-the-email-investigation-tool-you-need-for-osint>.

		Новіцький В.С.			ККІКБ.КР.Б – 125 – 33 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		64

ДОДАТКИ

		Новіцький В.С.			ККІКБ.КР.Б – 125 – 33 – ПЗ	Арк.
		Покотило О.А.				65
Змн.	Арк.	№ докум.	Підпис	Дата		

Порівняння OSINT з іншими методами розвідки у мережевій безпеці

Метод	Переваги	Недоліки	Порівняння з OSINT
OSINT	Легальний, етичний, не вимагає доступу до цілі	Лише відкриті джерела	Базовий, універсальний метод; найменш ризикований
	Безкоштовні ресурси	Може бути неповним або застарілим	
	Широка база даних		
SIGINT	Висока точність	Потребує технічного доступу до мережі	Глибший рівень розвідки, ніж OSINT, але потребує повноважень
	Перехоплення реального трафіку в режимі реального часу	Може бути незаконним без дозволу	
NETINT	Дозволяє виявити порти, сервіси, ОС	Активний метод, може бути помічений	Більш технічний і точний, але менш "невидимий", ніж OSINT
	Підходить для виявлення поверхні атаки	Порушує етику без дозволу	
Penetration Testing	Виявляє реальні уразливості	Вимагає повного дозволу	Ефективніше, але не для попереднього збору як OSINT
	Моделює справжні атаки	Складний і трудомісткий	
Traffic Analysis	Виявляє аномалії та зв'язки	Вимагає доступу до маршрутизаторів або логів	Глибша аналітика, ніж OSINT, але менш універсальна
	Не потребує повного вмісту трафіку		
CTI (Threat Intelligence)	Поєднує дані з багатьох джерел	Вимагає експертного аналізу	Ефективніше, ніж OSINT, але часто його використовує як основу
	Виявляє TTPs, IOC	Часто залежить від комерційних платформ	
HUMINT	Живі джерела, інсайдерська інформація	Суб'єктивність	Доповнює OSINT соціальним компонентом, але складніший у реалізації
	Історичні дані	Важко верифікувати	