

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

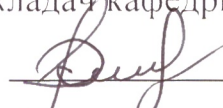
ПОЯСНЮВАЛЬНА ЗАПИСКА

до випускної кваліфікаційної роботи бакалавра
на тему: «Дослідження використання методів та інструментів
OSINT при розслідуванні кіберінцидентів»

Виконав студент 4-го курсу групи КБ-19-2
спеціальності 125 «Кібербезпека»

 Віктор Герасимчук

Керівник старший викладач кафедри КІ та КБ

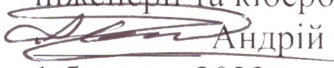
 Єлизавета Байлюк

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

 Андрій Єфіменко

Житомир – 2023

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
1 березня 2023 р.

ЗАВДАННЯ

на випускню кваліфікаційну роботу бакалавра

Студент: Герасимчук Віктор Вячеславович

Тема роботи: «Дослідження використання методів та інструментів OSINT при розслідуванні кіберінцидентів»

затверджена Наказом університету від 1 березня 2023 р. № 99

Термін здачі студентом закінченої роботи 19 червня 2023 р.

Вихідні дані роботи (зазначається предмет і об'єкт дослідження):

- методи виявлення та аналізу кіберзлочинів;
- використання методів та інструментів OSINT при розслідуванні кіберінцидентів.

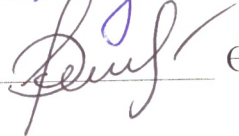
Обладнання та програмне забезпечення:

1. Kali Linux (v. 2023.1)
2. Програмне забезпечення «Holehe» (v. 1.0)
3. Програмне забезпечення «theHarvester» (v. 4.2.0)
4. Програмне забезпечення «Recon-ng» (v. 5.1.2)
5. Програмне забезпечення «Maltego» (v. 4.4.1)
5. Програмне забезпечення «Metagoofil» (v. 1.2.0)

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

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Байлюк Є.М..	13.03.2023	13.03.2023
2	Байлюк Є.М.	29.03.2023	29.03.2023
3	Байлюк Є.М.	14.04.2023	14.04.2023

Студент  Віктор Герасимчук

Керівник  Єлизавета Байлюк

Календарний план

№ з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка завдання	19.02.2023	Виконано
2	Аналіз об'єкта дослідження	14.03.2023	Виконано
3	Постановка задачі дослідження	18.03.2023	Виконано
4	Опрацювання літературних джерел	05.04.2023	Виконано
5	Пошук програмного забезпечення	07.04.2023	Виконано
6	Розробка методології розслідування кіберінцидентів	20.04.2023	Виконано
7	Налагодження робочого середовища	21.04.2023	Виконано
8	Розслідування кіберінциденту спам-розсилки фішингового листа	28.04.2023	Виконано
9	Збір інформації про домен з використанням спеціалізованого програмного забезпечення	10.05.2023	Виконано
10	Аналіз веб-сайду за допомогою метаданих контенту	17.05.2023	Виконано
11	Розробка рекомендацій щодо використання OSINT	28.05.2023	Виконано
12	Оформлення пояснювальної записки	08.06.2023	Виконано
13	Отримання відгуку керівника та рецензії на кваліфікаційну роботу		Виконано
14	Захист		Виконано

Студент  Віктор Герасимчук

Керівник  Єлизавета Байлюк

АНОТАЦІЯ

Випускна робота бакалавра складається з пояснювальної записки. Пояснювальна записка до випускої бакалаврської роботи містить 69 сторінок і 23 рисунки. Перелік посилань мість 30 літературних джерел.

За останні десятиліття кіберінциденти стали серйозною загрозою для компаній, урядів та приватних осіб по всьому світу. Ці злочини включають крадіжку конфіденційної інформації, розповсюдження шкідливих програм, фішинг, DDoS-атаки та багато іншого. Для успішного розслідування кіберінцидентів використання методів та інструментів відкритих джерел інформації (OSINT) стає дедалі важливішими.

Метою випускної роботи є дослідження використання методів та інструментів OSINT при розслідуванні кіберінцидентів.

У першому розділі було розглянуто поняття та визначення OSINT, основні принципи та правила використання OSINT, порівняння методів розслідування кіберінцидентів, нормативно-правові аспекти використання OSINT та міжнародний досвід використання OSINT.

У другому розділі було розглянуто методологію дослідження кіберінцидентів за допомогою методів OSINT та програмні засоби, які можуть бути використані для здійснення такого дослідження.

У третьому були застосовані різні методи та інструменти, які дозволили зібрати важливу інформацію та отримати цінні висновки.

Ключові слова: OSINT, КІБЕРБЕЗПЕКА, КІБЕРІНЦИДЕНТИ, РОЗСЛІДУВАННЯ, МЕТОДИ ДОСЛІДЖЕННЯ, ІНСТРУМЕНТИ ДОСЛІДЖЕННЯ, ЦИФРОВІ СЛІДИ, ВІДКРИТЕ ДЖЕРЕЛО ІНФОРМАЦІЇ, АНАЛІЗ ІНФОРМАЦІЇ, ЗБІР ІНФОРМАЦІЇ, ВІРТУАЛЬНІ ПРИВАТНІ МЕРЕЖІ, СОЦІАЛЬНІ МЕРЕЖІ, ЗАХИСТ ВІД КІБЕРАТАК.

ККІКБ.КР.Б – 125 – 23 – ПЗ

					ККІКБ.КР.Б – 125 – 23 – ПЗ			
Змн.	Арк.	№ докум.	Підпис	Дата	Дослідження використання методів та інструментів OSINT при розслідуванні кіберінцидентів	Літ.	Арк.	Аркушів
Розроб.		Герасимчук В.В.		19.08.23				
Керівник		Байлюк С.М.		19.08.23				
Реценз.		Єфіменко А.А.		19.08.23		ФІКТ, Гр. КБ-19-2		
Н. контр.								
Затверд.		Єфіменко А.А.		19.08.23				

ANNOTATION

A bachelor's degree qualification work consists of an explanatory note. The explanatory note to the bachelor's thesis contains 69 pages, and 23 figures. The list of references includes 30 literary sources.

In recent decades, cyber incidents have become a serious threat to companies, governments, and individuals around the world. These crimes include the theft of confidential information, the spread of malware, phishing, DDoS attacks, and much more. For successful cyber incident investigations, the use of open source intelligence (OSINT) methods and tools is becoming increasingly important.

The purpose of this thesis is to study the use of OSINT methods and tools in cyber incident investigation.

The first chapter examined the concept and definition of OSINT, the basic principles and rules of using OSINT, a comparison of cyber incident investigation methods, regulatory aspects of using OSINT, and international experience in using OSINT.

The second section examined the methodology for investigating cyber incidents using OSINT methods and the software tools that can be used to conduct such a study.

In the third section, various methods and tools were used to collect important information and draw valuable conclusions.

Keywords: OSINT, CYBERSECURITY, CYBER INCIDENTS, INVESTIGATION, RESEARCH METHODS, RESEARCH TOOLS, DIGITAL FOOTPRINTS, OPEN SOURCE INFORMATION, INFORMATION ANALYSIS, INFORMATION COLLECTION, VIRTUAL PRIVATE NETWORKS, SOCIAL NETWORKS, PROTECTION AGAINST CYBER ATTACKS.

		Герасимчук В.В.			ККІКБ.КР.Б – 125 – 23 – ПЗ	Арк.
		Байлюк Є.М.				5
Змн.	Арк.	№ докум.	Підпис	Дата		

ЗМІСТ

ВСТУП	8
РОЗДІЛ 1. Теоретичні аспекти використання OSINT	10
1.1 Поняття та визначення OSINT	10
1.2 Основні принципи та правила використання OSINT	13
1.3 Порівняння методів розслідування кіберінцидентів.....	15
1.4 Нормативно-правові аспекти використання OSINT	18
1.5 Міжнародний досвід використання методів OSINT та відомості про відомі розслідування.	23
РОЗДІЛ 2. Методи та інструменти збору інформації в OSINT	28
2.1. Методологія дослідження кіберінцидентів за допомогою методів OSINT..	28
2.2. Програмне забезпечення Maltego.....	31
2.3. Програмне забезпечення Shodan.	33
2.4. Програмне забезпечення Recon-ng.	34
2.5. Програмне забезпечення theHarvester.....	37
РОЗДІЛ 3. Практичний досвід використання OSINT.....	43
3.1. Розслідування кіберінциденту спам-розсилки фішингового листа.....	43
3.2. Збір інформації про домен з використанням спеціалізованого програмного забезпечення.	48
3.3. Аналіз веб-сайту за допомогою метаданих контенту.	56
3.4. Рекомендації щодо використання OSINT.	60
ВИСНОВКИ.....	64
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ	66

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

OSINT - Open source intelligence

DDoS - denial-of-service

ASD - AeroSpace and Defence Industries Association of Europe

IDS - Intrusion Detection System

IPS - Intrusion prevention systems

DNS - Domain Name System

		Герасимчук В.В.			ККІКБ.КР.Б – 125 – 23 – ПЗ	Арк.
		Байлюк Є.М.				7
Змн.	Арк.	№ докум.	Підпис	Дата		

ВСТУП

Актуальність теми. Кібербезпека є однією з найважливіших галузей в інформаційній технології. З поширенням комп'ютерів і Інтернету з'явилися нові виклики для кібербезпеки, а саме: кібератаки, крадіжки даних та інші кіберінциденти. У багатьох випадках розслідування таких інцидентів може бути складним завданням, адже злочинці досить ретельно приховують свої сліди.

Тема "Дослідження використання методів та інструментів OSINT при розслідуванні кіберінцидентів" є дуже актуальною в сучасному світі, де кібербезпека стає все більшою проблемою. Кіберінциденти можуть стати серйозною загрозою для роботи підприємств, державних інституцій та приватних осіб.

Використання методів та інструментів OSINT (відкритих джерел інформації) може допомогти розслідувачам в ефективному виявленні та аналізі даних про кіберінциденти. Оскільки багато даних про кібератаки можуть бути знайдені в Інтернеті, методи та інструменти OSINT можуть допомогти розслідувачам зібрати інформацію про виконавців кібератак, їх мотивації та методи.

Дана дипломна робота може виявитися корисною для фахівців у сфері кібербезпеки, правоохоронних органів та будь-яких організацій, які хочуть бути захищеними від кібератак. Результати дослідження можуть бути використані для створення більш ефективних стратегій захисту від кіберінцидентів та допомогти виявляти та перешкоджати кіберзлочинності.

Метою кваліфікаційної роботи є дослідження використання методів та інструментів OSINT при розслідуванні кіберінцидентів

Визначена мета обумовлює наступні завдання:

- вивчення методів та інструментів OSINT для збору та аналізу відкритої інформації про кіберінциденти;
- аналіз принципів функціонування кіберзлочинців та їхніх методів атак;
- вивчення інструментів та методів захисту від кіберінцидентів та їх ефективності;
- розробка методики використання методів та інструментів OSINT для розслідування кіберінцидентів;

		Герасимчук В.В.			ККІКБ.КР.Б – 125 – 23 – ПЗ	Арк.
		Байлюк Є.М.				8
Змн.	Арк.	№ докум.	Підпис	Дата		

- оцінка ефективності розробленої методики та її порівняння з існуючими підходами до розслідування кіберінцидентів;
- аналіз отриманих результатів та розробка рекомендацій щодо підвищення ефективності розслідування кіберінцидентів.

Об’єктом дослідження є дослідження використання методів та інструментів OSINT при розслідуванні кіберінцидентів.

Предметом дослідження є методи виявлення та аналізу кіберзлочинів, включаючи роботу з відкритими базами даних та соціальними мережами для ідентифікації злочинців та аналізу їхньої діяльності.

		Герасимчук В.В.			ККІКБ.КР.Б – 125 – 23 – ПЗ	Арк.
		Байлюк Є.М.				9
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 1. ТЕОРЕТИЧНІ АСПЕКТИ ВИКОРИСТАННЯ OSINT

1.1 Поняття та визначення OSINT

Методи OSINT - це підхід до збору та аналізу інформації, який базується на використанні публічної інформації, що доступна у відкритих джерелах. Даний метод широко використовується у різних галузях, таких як державна безпека, правоохоронні органи, журналістика та бізнес[2].

Концепція OSINT була розроблена у середині 20-го століття, коли військові та розвідувальні служби почали використовувати інформацію, яка була доступна через публічні джерела. З поширенням Інтернету і соціальних мереж, які дозволяють швидко та ефективно ділитися інформацією, OSINT став ще більш розповсюдженим та важливим інструментом для виконання розвідувальних та аналітичних завдань.

Сьогодні OSINT використовується у правоохоронних органах для збору інформації про злочинні діяння та їх авторів, військових структурах для виявлення та аналізу потенційних загроз, в інформаційній безпеці для виявлення та протидії кібератакам, в державному управлінні для моніторингу громадської думки та збору інформації про громадські рухи та ініціативи.

OSINT також знаходить своє використання у бізнесі. Він допомагає компаніям аналізувати своїх конкурентів та їх продукти, відстежувати ринок та нові тенденції, а також знаходити нові можливості для розвитку бізнесу. Використання OSINT дозволяє підвищити ефективність маркетингових стратегій та зменшити ризики прийняття неправильних рішень.

У наукових дослідженнях також можна використовувати OSINT для збору та аналізу інформації про певні теми. Наприклад, для дослідження громадської думки або вивчення певних соціальних проблем.

OSINT також може бути корисним для громадських організацій та активістів. Вони можуть використовувати його для збору інформації про своїх опонентів, виявлення корупції та порушень прав людини, а також для підвищення обізнаності громадськості щодо певних проблем.

		Герасимчук В.В.			ККІКБ.КР.Б – 125 – 23 – ПЗ	Арк.
		Байлюк Є.М.				10
Змн.	Арк.	№ докум.	Підпис	Дата		

Один з основних принципів методів OSINT - це збір інформації з відкритих джерел. Це означає, що для збору інформації не потрібно мати спеціальний доступ або використовувати нелегальні методи. Замість цього, збір інформації здійснюється шляхом використання публічних баз даних, веб-сайтів, соціальних мереж та інших джерел, які є публічними і у відкритому доступі.

Методи OSINT можуть включати етапи збору, оцінки та аналізу інформації. Збір інформації може бути автоматизованим за допомогою спеціальних програм та інструментів, таких як веб-скрапери, веб-кроулер та інші. Ці інструменти дозволяють збирати велику кількість інформації за короткий час, що значно збільшує продуктивність інформаційного пошуку. Після збору інформація проходить етап оцінки, де вона перевіряється на достовірність, актуальність та інші критерії. Далі, вона аналізується для виявлення певних залежностей, закономірностей та трендів.

Одним з основних переваг методів OSINT є їх доступність інформації. Більшість інформації, що знаходиться у відкритому доступі, може бути зібрана безкоштовно і анонімно. Крім того, методи OSINT є ефективними при використанні великих обсягів даних та дозволяють знайти зв'язки між різними джерелами інформації.

Існує багато різних джерел інформації, які можна використовувати при застосуванні методів OSINT. Наприклад, веб-сайти, які містять публічну інформацію про компанії, людей, ринки та інші предмети. Також до джерел OSINT відносяться соціальні мережі, форуми та інші ресурси, де користувачі діляться інформацією про свої дії та думки.

Одним з важливих аспектів методів OSINT є безпека і конфіденційність. При зборі та аналізі інформації необхідно дотримуватися вимог законодавства, в тому числі щодо захисту персональних даних. Крім того, необхідно використовувати безпечні інструменти та методи для захисту власної безпеки при використанні методів OSINT.

За допомогою методів OSINT також можливо збирати інформацію про потенційних злочинців, їх діяльність, інструменти, які вони використовують, а

		Герасимчук В.В.			ККІКБ.КР.Б – 125 – 23 – ПЗ	Арк.
		Байлюк Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		11

також отримати різноманітну інформацію про жертв інцидентів. Іншим із найбільш важливих аспектів використання методів OSINT при розслідуванні кіберінцидентів є збір інформації про зловмисників. Інформація про злочинців, їх мотивації, методи інфільтрації, інструменти та тактики можуть допомогти виявити слабкі місця і вразливості, які можуть бути використані для забезпечення захисту від подібних атак у майбутньому.

Крім того, методи OSINT можуть бути використані для збору інформації про нові види кіберінцидентів та для збору статистичної інформації про їх поширеність і тренди. Наприклад, за допомогою методів OSINT можна відстежувати поширення різноманітних видів шкідливого програмного забезпечення, таких як віруси, троянські коні, рекламний злочинний програмний засіб тощо. Також, методи OSINT можуть бути використані для збору інформації про нові технології та інновації, які можуть бути використані для кібератак. Така інформація може допомогти виявити нові загрози та прийняти заходи для запобігання потенційних кіберінцидентів.

Кіберінцидент - це подія, яка відбувається в інформаційній системі та може завдати шкоди її конфіденційності, цілісності або доступності. Кіберінциденти можуть бути спричинені різними причинами, такими як кіберзлочинці, хакери, внутрішні витоки даних або технічні проблеми.

Існує безліч видів кіберінцидентів, які можуть стати причиною великої шкоди для інформаційних систем і організацій. Деякі з найпоширеніших видів кіберінцидентів включають[9]:

- ransomware - це вид шкідливих програм, які заблоковують доступ до файлів на комп'ютері користувача та вимагають викуп за їхнє розблокування;
- DDoS-атака - це спроба затопити сайт або сервер запитами, що надходять з багатьох джерел одночасно, з метою перевантаження та зниження доступності цієї системи;
- phishing - це вид кібератак, при якому зловмисник намагається шахрайським шляхом отримати конфіденційну інформацію (наприклад, логіни та

		Герасимчук В.В.			ККІКБ.КР.Б – 125 – 23 – ПЗ	Арк.
		Байлюк Є.М.				12
Змн.	Арк.	№ докум.	Підпис	Дата		

паролі) від потенційної жертви, використовуючи підроблені електронні листи або веб-сайти;

- соціальний інженеринг - це метод атак на людський фактор, який заснований на психологічному маніпулюванні та використанні довіри до інших людей з метою отримання доступу до конфіденційної інформації.

Для успішного розслідування кіберінцидентів слід знати та розуміти різноманітні види кібератак, а також мати навички використання методів та інструментів OSINT, що дозволяють ефективно збирати та аналізувати відкриту інформацію для встановлення ідентичності зловмисника, виявлення його місцезнаходження та ідентифікації інших деталей, що можуть допомогти в розслідуванні.

1.2 Основні принципи та правила використання OSINT

Ефективне використання методів OSINT передбачає дотримання певних принципів та правил. Зокрема, це включає принципи збору, обробки та аналізу інформації, а також забезпечення конфіденційності та безпеки даних. До правил використання OSINT відносяться питання правової відповідальності за збір та використання інформації, взаємодії з іншими учасниками процесу, а також необхідності враховувати особливості та обмеження різних джерел інформації.

Можна виділити наступні основні принципи та правила використання OSINT:

Принцип збору інформації з дотриманням законів та правових норм є основним принципом використання OSINT. Збір інформації, отриманої незаконними методами, є недопустимим і може бути використаним проти вас у судовому процесі. При зборі інформації необхідно дотримуватись нормативно-правових актів, що регулюють збір та обробку персональних даних, права на інтелектуальну власність та інші правові аспекти, які пов'язані зі збором та використанням інформації. З метою забезпечення дотримання законів та правових норм, слід докладати зусиль для знаходження відкритої та легальної інформації, а також уникати використання незаконних методів її отримання. Всі отримані дані

		Герасимчук В.В.			ККІКБ.КР.Б – 125 – 23 – ПЗ	Арк.
		Байлюк Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		13

повинні бути перевірені на достовірність та правдивість, а також оброблені з дотриманням правил конфіденційності та безпеки. Зібрана інформація повинна бути перевірена та заснована на достовірних джерелах. Для цього використовуються різні методи та інструменти, такі як перевірка авторитетності джерел, порівняння різних джерел, перевірка фактів тощо[11].

Використання OSINT повинно здійснюватися компетентними особами з необхідним рівнем знань та навичок. Цей принцип відображає необхідність компетентності та відповідальності осіб, які займаються збором та аналізом інформації з використанням OSINT. Вони повинні мати необхідні знання та навички, щоб здійснювати ці процеси з ефективністю та точністю. Крім того, такі особи повинні розуміти технології та інструменти, що використовуються для збору та аналізу інформації, а також вміти інтерпретувати та використовувати отримані дані відповідно до мети дослідження. Цей принцип покликаний забезпечити ефективне та відповідальне використання OSINT та зменшити можливі ризики та помилки, які можуть виникнути через недостатню компетентність збирачів та аналітиків інформації.

Третій принцип використання OSINT передбачає, що отримана інформація повинна бути актуальною та відображати сучасну ситуацію. Для забезпечення цього, зібрана інформація повинна бути перевірена на правильність та достовірність. При зборі та аналізі інформації необхідно мати на увазі, що деяка інформація може бути застарілою або вже змінилася. Крім того, результати аналізу повинні бути перевірені на правильність та точність, оскільки неправильна інтерпретація даних може призвести до неправильних висновків та рішень.

Четвертий принцип використання OSINT передбачає, що зібрана інформація повинна бути проаналізована та інтерпретована для отримання її справжнього значення. Для цього необхідно здійснювати аналіз в контексті конкретної ситуації та враховувати різні фактори, що можуть впливати на інтерпретацію. Наприклад, інформація може бути дезінформацією або частковою правдою, що може викривлювати її сенс та призвести до неправильних висновків.

		Герасимчук В.В.			ККІКБ.КР.Б – 125 – 23 – ПЗ	Арк.
		Байлюк Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		14

Для забезпечення правильної інтерпретації інформації необхідно мати достатній рівень знань та досвіду в конкретній області, в якій здійснюється дослідження. Крім того, важливо враховувати контекст інформації, так як той самий факт може мати різне значення в залежності від обставин, в яких він стався.

Отже, здійснення пошуку з використанням OSINT може бути досить складним, проте завдяки використанню даних принципів та правил, можливо досягти значних результатів у розслідуванні кіберінцидентів та в інших галузях.

1.3 Порівняння методів розслідування кіберінцидентів

Порівняння методів розслідування кіберінцидентів є важливою складовою дослідження використання методів OSINT при розслідуванні кіберінцидентів. З одного боку, традиційні методи розслідування, такі як проведення слідчих дій, збір доказів та їх аналіз, досі залишаються важливими. З іншого боку, методи OSINT, які базуються на використанні відкритих джерел інформації, можуть бути корисними при виявленні та аналізі кіберінцидентів.

До класичних методів розслідування кіберінцидентів належать:

- метод обліку системних подій є одним з основних методів розслідування кіберінцидентів, який використовується для збору та аналізу інформації про події, які відбуваються в операційній системі та додаткових програмах;
- аналіз журналів (логів) системи - цей метод полягає у зборі та аналізі журналів (логів) системи, що містять інформацію про активність користувачів та системи в цілому;
- метод сканування портів - це метод визначення відкритих та закритих мережових портів на комп'ютері або віддаленому сервері. Використовуючи цей метод, можна визначити, які порти відкриті на комп'ютері, ідентифікувати служби, що використовуються та визначити рівень безпеки мережі;
- аналіз мережевого трафіку - цей метод полягає у зборі та аналізі мережевого трафіку, що протікає через мережу, з метою виявлення аномальних дій та потенційних загроз;

		Герасимчук В.В.			ККІКБ.КР.Б – 125 – 23 – ПЗ	Арк.
		Байлюк Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		15

• форензичний аналіз - цей метод полягає у зборі та аналізі цифрових доказів, що залишаються на комп'ютерах та інших цифрових пристроях, з метою виявлення дій зловмисників та ідентифікації їхньої особи[1].

З іншого боку, методи OSINT можуть включати:

• пошук інформації в Інтернеті: це включає в себе використання пошукових систем, соціальних мереж, блогів, форумів та інших джерел відкритої інформації;

• моніторинг та аналіз соціальних мереж: цей метод включає в себе збір інформації з соціальних мереж, аналіз змін у профілях користувачів, відстеження публікацій та тегів;

• аналіз зображень та відео: це включає в себе аналіз зображень та відео, використовуючи інструменти, які дозволяють виявляти та аналізувати відомості, що містяться в медіафайлах;

• аналіз веб-сторінок та метаданих: цей метод полягає в аналізі веб-сторінок та їх метаданих, таких як дата та час публікації, автор, зміни тощо;

• аналіз публічних баз даних: цей метод включає в себе пошук та аналіз інформації з публічних баз даних, таких як реєстри компаній, бази даних судових рішень тощо;

• аналіз візуального контенту включає в себе аналіз зображень, відео та іншого мультимедійного матеріалу, що розміщено в Інтернеті. Цей метод може допомогти в ідентифікації та локації об'єктів, їхнього стану, дій та процесів. Для аналізу використовують різноманітні інструменти, включаючи засоби комп'ютерного зору та штучного інтелекту.

Один з найбільш суттєвих відмінностей між традиційними методами розслідування та методами OSINT полягає в тому, що традиційні методи зазвичай базуються на обмеженому колі джерел інформації, що є доступними правоохоронним органам, тоді як методи OSINT дозволяють отримувати інформацію з різноманітних джерел, включаючи відкриті джерела, соціальні мережі, форуми тощо. Однак, методи OSINT також мають свої обмеження, зокрема, що зібрана інформація може бути неточною або неповною.

		Герасимчук В.В.			ККІКБ.КР.Б – 125 – 23 – ПЗ	Арк.
		Байлюк Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		16

Крім того, в рамках порівняння методів розслідування кіберінцидентів, можна відзначити, що традиційні методи, такі як ручний аналіз журналів, паперових документів та іншої інформації, є дуже часо- та працезатратними. Також, у багатьох випадках такі методи не є достатньо ефективними, оскільки кіберзлочинці дедалі більше використовують технічні засоби для маскування своєї діяльності. Застосування методів OSINT дозволяє значно прискорити та спростити процес розслідування кіберінцидентів. Зокрема, автоматизація процесу збору та аналізу інформації дозволяє значно зменшити час, необхідний для збору та аналізу даних, що в свою чергу дозволяє швидше виявляти та реагувати на кіберінциденти.

Іншою перевагою використання методів OSINT є можливість отримувати доступ до інформації, яка може бути недоступна для традиційних методів розслідування, наприклад, інформації, що зберігається на серверах, що перебувають за межами юрисдикції держави.

Однак, використання методів OSINT має й свої недоліки, такі як великий обсяг інформації, яку необхідно обробляти. У порівнянні з іншими методами розслідування кіберінцидентів, такими як методи аналізу логів, обробки великих даних, віртуальні машини та інші, методи OSINT можуть бути менш точними та потребувати більше часу для збору та обробки інформації. Також варто враховувати, що використання методів OSINT може бути менш ефективним при розслідуванні високорівневих та добре організованих кібератак, які можуть бути пов'язані зі складними мережами та використанням криптографії.

Також існує можливість отримати не точні або не достовірні. Наприклад, деякі джерела можуть містити неправдиву чи недостовірну інформацію, що може призвести до неправильних висновків та помилок при розслідуванні. Також, використання методів OSINT може бути залежне від рівня технічної освіти розслідувача та доступності певних інструментів. Тому важливо дотримуватись відповідних етичних стандартів та проводити додаткову перевірку отриманої інформації.

У цілому, використання методів OSINT є ефективним інструментом для розслідування кіберінцидентів, оскільки вони дозволяють отримувати доступ до

		Герасимчук В.В.			ККІКБ.КР.Б – 125 – 23 – ПЗ	Арк.
		Байлюк Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		17

великої кількості відкритої інформації, яка може бути корисною для виявлення та ідентифікації злочинців. Однак, важливо зазначити, що методи OSINT не можуть бути використані як єдиний інструмент для розслідування кіберінцидентів, оскільки вони не дозволяють отримати повну картину подій та дій винних осіб. Крім того, відкрита інформація може бути неповною, недостовірною або недостатньою для прийняття рішення щодо подальших кроків.

Отже, для досягнення успіху в розслідуванні кіберінцидентів варто поєднувати методи OSINT з іншими методами, такими як аналіз логів та використання спеціального програмного забезпечення, а також розглядати можливість використання експертів з кібербезпеки для отримання додаткової інформації та порад. Методи OSINT є корисними для збору відкритої інформації у Соціальних мережах, форумах, блогах, новинних статтях та інших джерелах. Дані джерела дозволяють отримувати доступ до інформації, яка може допомогти у встановленні злочинців та їхнього місця знаходження, виявленні мотивів, підозрілих дій та зв'язків між окремими особами.

1.4 Нормативно-правові аспекти використання OSINT

Збір та аналіз інформації з відкритих джерел являє собою сферу діяльності, що повинна відбуватися в рамках нормативно-правового поля держави. Основним принципом є забезпечення конституційних прав у сфері пошуку, збору, передачі та використання інформації у всіх демократичних країнах. Законодавство різних світових держав сприяє впровадженню систем розвідки з відкритих джерел у практику. Наприклад, ще в 1996 році у США був прийнятий Закон про свободу інформації, який зобов'язує спеціальні федеральні відомства забезпечувати вільний доступ громадян до їх власної інформації. Закон встановив лише певні обмеження, які стосуються матеріалів, що стосуються національної оборони, фінансових та особистих документів, а також документації правоохоронних органів держави. Однак в деяких країнах законодавець встановлює обмеження на подібну діяльність, що фактично забороняє здійснювати розвідку з відкритих джерел.

		Герасимчук В.В.			ККІКБ.КР.Б – 125 – 23 – ПЗ	Арк.
		Байлюк Є.М.				18
Змн.	Арк.	№ докум.	Підпис	Дата		

В Україні використання відкритих джерел інформації (OSINT) регулюється різними нормативно-правовими актами[5]. Найважливішими з них є Конституція України, Закон України "Про захист персональних даних", Кодекс України про адміністративні правопорушення, Кримінальний кодекс України та Цивільний кодекс України.

Один з основних нормативно-правових аспектів використання OSINT - це захист персональних даних. Використання OSINT для збору персональних даних повинно бути дотримано відповідних законів про захист персональних даних, таких як загальний регламент про захист персональних даних (GDPR) в Європейському Союзі або законодавстві України.

На сьогоднішній день основними європейськими правовими стандартами у сфері захисту персональних даних є Конвенція Ради Європи "Про захист осіб у зв'язку з автоматичною обробкою персональних даних" від 28 січня 1981 року (ETS №108)[12] та "Пакет захисту даних" Європейського Парламенту та Ради від 27 червня 2016 року[30]. Вони є обов'язковими для всіх держав-членів Європейського Союзу та є прикладом для наслідування в законодавстві, включаючи нашу країну. Країни Європейського Союзу повинні привести своє законодавство у відповідність із зазначеними правовими стандартами.

Конвенція Ради Європи "Про захист осіб у зв'язку з автоматичною обробкою персональних даних" від 28 січня 1981 року, яку Україна ратифікувала 06.07.2010 р., встановлює положення щодо передачі персональних даних, що підлягають автоматизованій обробці або зібрані з метою їх автоматизованої обробки, через національні кордони за допомогою будь-яких засобів. Наведені нижче дані, які зазвичай використовуються для ідентифікації особи, визначені Управлінням США з управління та бюджету як особистий:

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

		Герасимчук В.В.			ККІКБ.КР.Б – 125 – 23 – ПЗ	Арк.
		Байлюк Є.М.				19
Змн.	Арк.	№ докум.	Підпис	Дата		

- цифрова ідентифікація (цифровий підпис);
- дата народження;
- місце народження;
- генетична інформація.

Згідно з Конституцією України, кожна особа має право на захист своєї честі та гідності, приватного життя, інтимної та сімейної таємниці. Тому збір, обробка та використання персональних даних без дозволу власника цих даних є незаконним та може бути кваліфіковано як порушення прав людини. Тому організації повинні забезпечувати безпеку персональних даних, збирати їх лише за певною метою, зберігати обмежений період часу та надавати можливість особам відмовитися від збору своїх даних.

При неправильному або неетичному використанні OSINT можуть бути порушені наступні статті Конституції України[7]:

- стаття 32: Гарантується право на таємницю переписки, телефонних розмов та інших засобів комунікації. Використання OSINT може призвести до порушення цієї статті, якщо отримана інформація була отримана незаконно, без дозволу власника таємниці;

- стаття 34: Кожен має право на таємницю свого життя, а також на захист від її порушення. Використання OSINT може також призвести до порушення цієї статті, якщо отримана інформація стосується особистого життя людини та її використання може порушити її права;

- стаття 38: Кожен має право на свободу думок та вираження своїх поглядів. Використання OSINT може призвести до обмеження цієї статті, якщо зібрана інформація використовується для перешкоджання вільному вираженню думок та поглядів;

- стаття 41: Кожен має право на вільне збирання, зберігання, використання та поширення інформації. Однак, використання OSINT може призвести до порушення цієї статті, якщо отримання та поширення інформації проводиться незаконно та/або може завдати шкоди правам людини та її гідності.

		Герасимчук В.В.			ККІКБ.КР.Б – 125 – 23 – ПЗ	Арк.
		Байлюк Є.М.				20
Змн.	Арк.	№ докум.	Підпис	Дата		

Закон України "Про захист персональних даних" також містить норми, які регулюють збір, обробку та використання персональних даних[14]. Згідно з цим законом, персональні дані можуть бути зібрані, оброблені та використані лише за умови, що особа, до якої вони належать, надала на це згоду або це передбачено законом. Крім того, власник персональних даних має право звернутися до суду у разі порушення своїх прав на захист персональних даних.

Під час використання OSINT можуть бути порушені різні положення Закону України "Про захист персональних даних" в залежності від того, які саме дані збираються та їх подальше використання. Наприклад:

- збір персональних даних без дозволу суб'єкта даних (стаття 6) - у разі, коли використовувані методи та інструменти OSINT дозволяють збирати персональні дані про особу без її дозволу;
- обробка персональних даних без повідомлення суб'єкта даних про мету обробки (стаття 8) - у разі, коли отримані персональні дані використовуються без зазначення мети їх обробки;
- несвоєчасне виправлення чи видалення неповних або неточних персональних даних (стаття 10) - у разі, коли отримані персональні дані містять помилки або неправдиву інформацію, але не були виправлені чи видалені;
- передача персональних даних третім особам без дозволу суб'єкта даних (стаття 21) - у разі, коли отримані персональні дані передаються третім особам без дозволу суб'єкта даних;
- використання персональних даних без дозволу суб'єкта даних для здійснення реклами або маркетингу (стаття 23) - у разі, коли отримані персональні дані використовуються для здійснення рекламної діяльності або маркетингу без дозволу суб'єкта даних.

Інший аспект, на який необхідно звернути увагу, це авторське право. При використанні даних з відкритих джерел, таких як інтернет-ресурси, соціальні мережі або публічні бази даних, важливо дотримуватися авторських прав на ці дані. Не можна копіювати та використовувати ці дані без згоди їх власників або з дозволу авторських прав на публікацію цих даних. Крім того, використання OSINT може

		Герасимчук В.В.			ККІКБ.КР.Б – 125 – 23 – ПЗ	Арк.
		Байлюк Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		21

підпадати під законодавство про захист національної безпеки та боротьбу з кіберзлочинністю. У багатьох країнах законодавство може обмежувати збір та використання інформації про національну безпеку та кіберзлочинність.

Щодо кримінальної відповідальності за використання OSINT, Кримінальний кодекс України містить статті, які передбачають відповідальність за розголошення та збір інформації, яка є державною або службовою таємницею[6]. Також згідно з цим кодексом, збирання та обробка персональних даних з порушенням вимог законодавства можуть бути кваліфіковані як порушення прав людини.

Під час використання методів OSINT може бути порушена стаття 182 ККУ - порушення недоторканості приватного життя. Ця стаття передбачає відповідальність за незаконне збирання, використання та поширення конфіденційної інформації, в тому числі шляхом їх отримання з використанням методів OSINT без належного дозволу власника даних. Іншою статтею є стаття 361 ККУ - несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж. Незаконний доступ до комп'ютерних матеріалів, що зберігаються у комп'ютерних системах або мережах, зокрема з використанням методів OSINT, може бути кваліфіковано як злочин за цією статтею. Також може бути порушені статті 361-1 ККУ - розповсюдження шкідливих програм та 361-2 ККУ - створення, продаж або розповсюдження засобів для порушення цілісності комп'ютерних систем або мереж. Використання методів OSINT для створення, продажу або розповсюдження засобів, які призначені для порушення цілісності комп'ютерних систем або мереж, також може бути кваліфіковано як злочин за цією статтею. Ще однією потенційно порушеною статтею є стаття 362 ККУ - несанкціоновані дії з інформацією, яка обробляється в електронно-обчислювальних машинах. Якщо використання OSINT включає в себе шахрайство, крадіжку ідентифікаторів або паролів, підробку документів, то це також може бути кваліфіковано як порушення цієї статті.

Також згідно з чинним Кримінальним кодексом України, незаконне збирання з метою використання або використання відомостей, що становлять комерційну

		Герасимчук В.В.			ККІКБ.КР.Б – 125 – 23 – ПЗ	Арк.
		Байлюк Є.М.				22
Змн.	Арк.	№ докум.	Підпис	Дата		

таємницю, а також розголошення комерційної таємниці є кримінальною діяльністю, за яку передбачена відповідальність. Однак ці дії не входять до сфери розвідки з відкритих джерел

У свою чергу, Цивільний кодекс України передбачає відповідальність за порушення прав на інтелектуальну власність, включаючи авторські права, патенти та товарні знаки[8]. Під час використання OSINT можуть порушуватися наступні статті Цивільного кодексу України:

Таким чином, при використанні методів та інструментів OSINT необхідно дотримуватися певних правил та принципів. Перш за все, важливо збирати лише ту інформацію, яка є відкритою та доступною для загального використання. Крім того, необхідно дотримуватися правил збору та обробки персональних даних, а також уникати порушення прав на захист інтелектуальної власності. Важливо також пам'ятати про те, що збір та використання інформації з метою шкоди іншим особам може бути кваліфіковано як злочин та мати серйозні наслідки.

Найкращим підходом до використання OSINT є дотримання правових норм та етичних принципів, що забезпечує не тільки законність дій, але й ефективність отриманої інформації.

1.5 Міжнародний досвід використання методів OSINT та відомості про відомі розслідування.

У 1947 році аналітик ЦРУ Кен Шерман зазначив, що держава отримує з відкритих джерел інформації майже 80 %, пізніше (генерал-лейтенант, керівник Розвідувального управління міністерства оборони США) Самуель Уілсон стверджував що 90 % всієї розвідувальної інформації надходить з відкритих джерел, а лише 10 % – з роботи агентури

Сьогодні OSINT найбільше використовується у США. Цим методом успішно користуються наступні організації:

- академія відкритих джерел;
- департамент передових систем (ASD);
- рада із захисту відкритих джерел;

		Герасимчук В.В.			ККІКБ.КР.Б – 125 – 23 – ПЗ	Арк.
		Байлюк Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		23

- розвідувальне управління Міністерства оборони США;
- командування розвідки і безпеки ЗС США;
- дослідницька служба бібліотеки Конгресу США (Congressional Research Service).

Експерти високо оцінюють потенціал OSINT через те, що він забезпечує можливість обміну перевіреною інформацією з іноземними партнерами. Така інформація надходить з відкритих джерел та не використовує приховані методи або заборонені у використанні секретні джерела. Це означає, що регулятор лобістської діяльності може використовувати таку інформацію і не лише подавати її до правоохоронних органів для проведення розслідування та притягнення до відповідальності потенційних правопорушників, а й до медійних структур. Ця практика може допомогти у боротьбі з інформаційними атаками недобросовісних суб'єктів лобіювання, звинуваченням в упередженості та обмеженні їх прав. Відкритість і публічність регулятора є одним з найбільш ефективних методів захисту репутації останнього від перекручування інформації та відвертої «демонізації» у громадянському суспільстві.

Одним з найбільш відомих прикладів OSINT дослідження кіберінциденту є розслідування компанією FireEye відомої хакерської групи APT29, яку також називають Cozy Bear[15].

У грудні 2020 року, FireEye повідомив про те, що їх власна система була скомпрометована і хакери вкрали деяку кількість інструментів, які використовувала компанія для виявлення інших кібератак. Згодом виявилось, що це була частина широкомасштабної кампанії, яку проводив APT29.

APT29 (також відомий як Cozy Bear) - це хакерська група, яка вважається однією з найбільш продуктивних і стійких кіберзлочинних організацій. Група відома своїми нападами на урядові та приватні організації по всьому світу, зокрема в США, Канаді, Німеччині та Італії. Одним із найвідоміших нападів APT29 був кібератака на Державний департамент США у 2014 році, коли група здобула доступ до системи електронної пошти дипломатів та інших службових осіб. В цьому нападі група використала продвинуті методи атаки, такі як розповсюдження

		Герасимчук В.В.			ККІКБ.КР.Б – 125 – 23 – ПЗ	Арк.
		Байлюк Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		24

шкідливого ПЗ через email та використання "задніх дверей" у програмному забезпеченні.

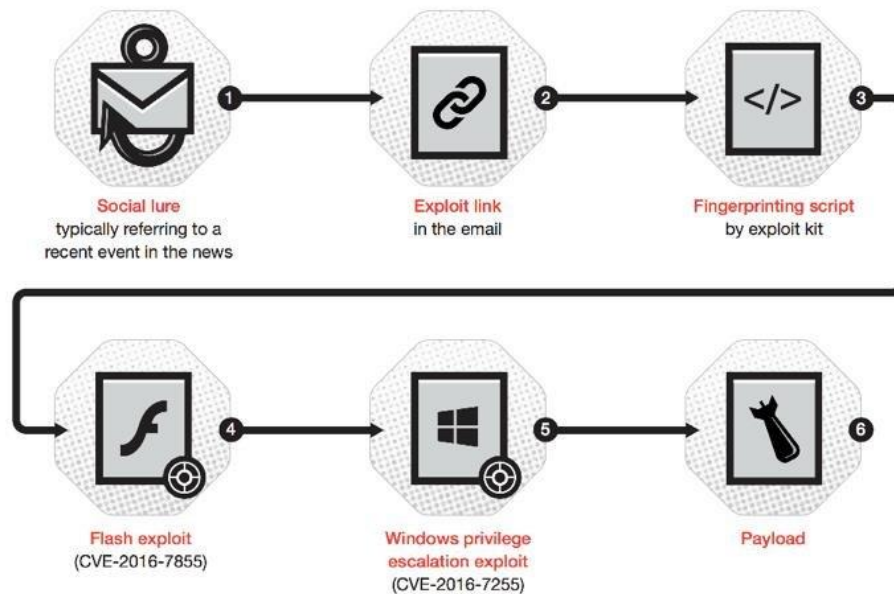


Рисунок 1.1 – Типовий алгоритм виконання атаки за допомогою email, якого притримувалася організація APT29

Розслідування нападів APT29 вимагало використання різноманітних методів, включаючи аналіз мережевого трафіку, виявлення вразливостей у програмах і операційних системах, аналіз витоків інформації, моніторинг поведінки шкідливих програм та зломисників, а також використання інструментів OSINT для збору і аналізу відкритої інформації про можливі джерела атак та інших деталей нападу. Крім того, необхідно здійснювати постійний моніторинг мережі та системи безпеки, щоб вчасно виявляти та реагувати на будь-які зміни, що можуть свідчити про злам.

FireEye використовувала комплексний підхід для пошуку інформації про APT29, включаючи різні методи аналізу інформації. Зокрема, вони вивчали мережевий трафік, який проходив через компрометовані системи, щоб зрозуміти, як саме вірус поширюється і як він взаємодіє з іншими системами. Крім того, вони використовували різноманітні інструменти для виявлення вразливостей у програмах та веб-сайтах, які використовувалися APT29 для здійснення атак.

FireEye також використовувала велику кількість інформації з відкритих джерел для аналізу діяльності APT29. Зокрема, вони аналізували блоги, форуми та

		Герасимчук В.В.			ККІКБ.КР.Б – 125 – 23 – ПЗ	Арк.
		Байлюк Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		25

інші відкриті джерела для збору інформації про потенційні цілі та методи атак АРТ29. Крім того, вони використовували інструменти для аналізу мови та інших параметрів тексту, щоб встановити можливу локалізацію індивідів, які стоять за нападами.

FireEye збрала досить інформації, щоб зрозуміти, як саме працює АРТ29, їхні методи і цілі. На основі цих даних, FireEye надала детальну звітність щодо діяльності АРТ29, включаючи їхні методи інфільтрації, цілі та можливі зв'язки з іншими кіберзлочинними організаціями.. Результатом цього дослідження став більший інтерес до проблеми кібербезпеки та збільшення заходів для захисту компаній і організацій від кібератак.

Ще одним відомим прикладом є дослідження компанії Dragos про хакерську групу Xenotime, яка відома також під назвою Triton або Trisis. Ця група вперше була виявлена в 2017 році після атаки на один з підприємств нафтогазової промисловості в Саудівській Аравії, яка призвела до зупинки систем безпеки та аварійного вимкнення промислового обладнання[16].

Дослідження Dragos було проведено з використанням методів OSINT та інших відкритих джерел інформації, таких як дослідження відкритих баз даних та інтернет-ресурсів, що дозволило зібрати достатньо інформації про цю хакерську групу та її дії.

Дослідження показало, що Xenotime є вельми складною та витонченою хакерською групою, яка спеціалізується на атаках на об'єкти критичної інфраструктури, такі як електростанції та інші енергетичні підприємства. Для своїх атак група використовує різноманітні інструменти та техніки, включаючи вразливості у програмному забезпеченні та фішингові атаки на співробітників цільової організації.

Дослідження також виявило, що Xenotime не є звичайною хакерською групою, але є частиною складнішої кіберзлочинної структури, яка має зв'язки з іншими відомими групами. Таким чином, дослідження компанії Dragos дало можливість отримати детальний аналіз дій цієї групи та встановити зв'язки з іншими кіберзлочинними групами. Дослідження компанії Dragos стало важливим

		Герасимчук В.В.			ККІКБ.КР.Б – 125 – 23 – ПЗ	Арк.
		Байлюк Є.М.				26
Змн.	Арк.	№ докум.	Підпис	Дата		

кроком у забезпеченні кібербезпеки країни та всього світу, оскільки Xenotime вважається однією з найнебезпечніших кіберзлочинних груп, яка може бути задіяна в атаках на критичну інфраструктуру. В результаті, дослідження дозволило розробити більш ефективні стратегії протидії її діяльності та захисту вразливих об'єктів від можливих атак.

Висновки до першого розділу

У цьому розділі ми розглянули поняття та визначення OSINT, основні принципи та правила використання OSINT, порівняння методів розслідування кіберінцидентів, нормативно-правові аспекти використання OSINT та міжнародний досвід використання OSINT.

Основна ідея OSINT полягає у зборі та аналізі відкритої інформації з метою вирішення різних завдань. Використання OSINT може бути дуже корисним в дослідженні кіберінцидентів та може допомогти виявити причину та знайти винних.

Основними принципами використання OSINT є використання лише відкритої інформації, перевірка джерел інформації та збір даних з різних джерел. Крім того, для використання OSINT необхідно мати відповідні знання та навички в зборі та аналізі інформації.

Порівняння методів розслідування кіберінцидентів показало, що використання OSINT може бути дуже ефективним у розслідуванні кібератак та допомагає знайти відповіді на багато запитань.

Нормативно-правові аспекти використання OSINT мають велике значення, оскільки нерозсудливе використання цієї інформації може призвести до порушення законодавства.

Також розглянутий міжнародний досвід та відомості про відомі OSINT розслідування, такі як FireEye та Dragos, підтверджують ефективність використання OSINT у розслідуванні кіберінцидентів та забезпеченні кібербезпеки.

		Герасимчук В.В.			ККІКБ.КР.Б – 125 – 23 – ПЗ	Арк.
		Байлюк Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		27

РОЗДІЛ 2. МЕТОДИ ТА ІНСТРУМЕНТИ ЗБОРУ ІНФОРМАЦІЇ В OSINT

2.1. Методологія дослідження кіберінцидентів за допомогою методів OSINT.

Дослідження кіберінциденту є складним процесом, який вимагає наявності адекватної методології та спеціалізованих інструментів. Використання OSINT є ефективним методом при проведенні таких досліджень, оскільки дозволяє зібрати та проаналізувати велику кількість інформації з відкритих джерел.

Отримання інформації за допомогою розвідки OSINT зазвичай здійснюється трьома основними типами: пасивного, напівпасивного та активного. Ефективність вибору типу залежить від сценарію та типу даних, які цікавлять суб'єкта збору інформації.

Пасивний збір інформації є найбільш поширеним типом збору та обробки даних. Він заснований на використанні загальнодоступних ресурсів.

Під час застосування напівпасивного типу збору даних технічні засоби обмежують трафік, який надсилається до цільових серверів, з метою отримання загальної інформації про них. Трафік, що надсилається, повинен схожим на типовий інтернет-трафік, щоб не привертати увагу до розвідувальної діяльності відповідних структур з боку громадськості.

Активний тип збору інформації включає безпосередню взаємодію з системою, що стосується об'єкта розвідки. Власник системи може знати про інформаційну розвідку, оскільки особа або організація, яка збирає дані, використовує новітні методи збору технічних даних про цільову ІТ-інфраструктуру, такі як сканування вразливостей, сканування додатків веб-сервера, доступ до відкритих портів та інші. Такий трафік може викликати підозру або тлумачитися як зловмисна поведінка, і залишить сліди у системі виявлення вторгнень (IDS) або системі запобігання таких вторгнень (IPS). Атаки з боку соціальної інженерії є одним з видів активного збору інформації.

Для ефективного здійснення подібної розвідки необхідно притримуватися наведених кроків[10].

		Герасимчук В.В.			ККІКБ.КР.Б – 125 – 23 – ПЗ	Арк.
		Байлюк Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		28

Перший крок полягає в зборі максимальної кількості інформації про сам кіберцінцідент, щоб мати повне розуміння ситуації та наслідків, які він призвів. Для цього необхідно скористатись різними джерелами, такими як соціальні мережі, форуми, блоги тощо, де можуть знаходитись корисні деталі та описи інциденту від очевидців. Також корисно взяти інтерв'ю у постраждалих та працівників компанії, які можуть надати додаткову інформацію про те, що сталося та як це вплинуло на компанію. Важливо зафіксувати всю зібрану інформацію та відсортувати її за категоріями, щоб було легше аналізувати та використовувати далі у дослідженні.

Другим кроком у проведенні дослідження кіберцінціденту є аналіз отриманої інформації. Після збору інформації необхідно провести її детальний аналіз. Для цього можна скористатись спеціальними інструментами, які дозволяють аналізувати мережевий трафік, системні журнали, лог-файли та інші дані.

Аналіз отриманої інформації має на меті визначити, які конкретно дані були скомпрометовані, які системи були атаковані та які методи були використані зловмисниками. Наприклад, можна з'ясувати, чи використовувалися вразливості в програмному забезпеченні, які порти були відкриті, які додатки були запущені, які файли були змінені або видалені, та інші важливі деталі.

Для проведення аналізу можна використати спеціальні інструменти, такі як Wireshark для аналізу мережевого трафіку, Sysinternals Suite для аналізу системних журналів та лог-файлів, а також інші інструменти, які дозволяють отримати необхідну інформацію. Крім того, можна скористатись знаннями про типові атаки та вразливості для визначення можливих методів атаки.

Після аналізу отриманої інформації можна визначити можливі причини інциденту та найбільш вразливі місця в інфраструктурі компанії, що дозволить розробити план заходів щодо підвищення кібербезпеки.

Третім кроком є детальний аналіз всіх доказів, що були зібрані, з метою перевірки гіпотез, визначених на попередньому етапі. Це може включати аналіз мережевого трафіку, електронної пошти та інших елементів, що були зібрані в ході розслідування.

		Герасимчук В.В.			ККІКБ.КР.Б – 125 – 23 – ПЗ	Арк.
		Байлюк Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		29

Аналіз зібраних доказів дозволяє підтвердити або спростувати попередні гіпотези щодо мотивів, методів та злочинних схем зловмисників. Крім того, цей етап може допомогти визначити масштаб та характер кібератаки, а також ідентифікувати зловмисників. Останнє є особливо важливим, оскільки дозволяє надійно встановити та використовувати інформацію про зловмисників при подальшому розслідуванні та судовому переслідуванні.

Після того, як інформація про кіберцінцідент була зібрана та проаналізована, наступним етапом є ідентифікація зловмисників та їх мотивів. Для досягнення цієї мети, можна використовувати різні інтернет-ресурси, які дозволяють відслідковувати діяльність кіберзлочинців та збирати інформацію про їх зв'язки, методи та прийоми роботи. Але для успішної ідентифікації зловмисників потрібно спочатку аналізувати та класифікувати зібраний матеріал, виявляючи можливі зв'язки між ними. На цьому етапі можуть використовуватися інструменти для аналізу великих обсягів даних, такі як інструменти візуалізації даних та аналізу графів, щоб знайти зв'язки між окремими даними та встановити послідовність дій зловмисників. Таким чином, ідентифікація зловмисників є надзвичайно важливою задачею, яка потребує аналізу великої кількості даних та використання спеціалізованих інструментів.

Останнім кроком є підготовка детального звіту про кібератаку, який містить інформацію про всі аспекти атаки. Звіт може бути використаний для інформування керівництва компанії або органів правопорядку про деталі кібератаки та її наслідки. Звіт повинен містити інформацію про методи, які використовувалися зловмисниками, шляхи, якими вони отримували доступ до систем, зібрані докази, аналіз результатів і рекомендації щодо покращення системи безпеки, усунення вразливостей, вдосконалення моніторингу та реагування на подібні загрози. Детальний звіт є важливим інструментом для подальшого розслідування та захисту від кібератак в майбутньому.

Основний підхід до дослідження кіберінцидентів з використанням OSINT полягає у ретельному зборі та аналізі доказів. Головна мета цього підходу - виявити та ідентифікувати зловмисників. Аналіз доказів, зібраних за допомогою методів

		Герасимчук В.В.			ККІКБ.КР.Б – 125 – 23 – ПЗ	Арк.
		Байлюк Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		30

OSINT, дозволяє встановити посилання між різними джерелами інформації, розкрити індивідуальні аспекти та особливості діяльності зловмисників, а також з'ясувати можливі шляхи ідентифікації або притягнення їх до відповідальності.

Крім того, використання даного підходу до дослідження кіберінцидентів з використанням OSINT допомагає зменшити наслідки кібератак. Ретельний аналіз доказів дозволяє отримати більше інформації про характер атаки та її виконавців, що в свою чергу допомагає прийняти ефективні заходи для запобігання подібним інцидентам у майбутньому.

2.2. Програмне забезпечення Maltego.

Використання програмного забезпечення є важливим елементом розслідування кіберінцидентів через великий обсяг даних, який потрібно обробити та аналізувати. Для збору даних з відкритих джерел можуть використовуватися спеціальні інструменти, які дозволяють автоматизувати процес збору та аналізу даних з різних джерел.

Наприклад, програмне забезпечення Maltego є потужним інструментом для збору, аналізу та візуалізації даних з різних джерел. Воно дозволяє збирати інформацію з різних джерел, таких як соціальні мережі, форуми, бази даних та інші ресурси, та об'єднувати її в єдину карту зв'язків, яка допомагає визначити зв'язки між різними сутностями та ідентифікувати можливих зловмисників.

Maltego - це програмне забезпечення для аналізу даних та візуалізації зв'язків між об'єктами, яке використовується в багатьох галузях, включаючи кібербезпеку та розслідування кіберінцидентів[17].

Maltego дозволяє швидко та ефективно аналізувати великі обсяги даних, які можуть бути зібрані з різних джерел, таких як соціальні мережі, бази даних компаній, державних установ та інших джерел відкритого доступу. Maltego використовує графічний інтерфейс для відображення зібраної інформації та її взаємозв'язків. За допомогою цього інструменту можна відстежувати зв'язки між різними сутностями, такими як особи, компанії, домени та інші елементи, що можуть бути використані зловмисниками для проведення кібератак.

		Герасимчук В.В.			ККІКБ.КР.Б – 125 – 23 – ПЗ	Арк.
		Байлюк Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		31

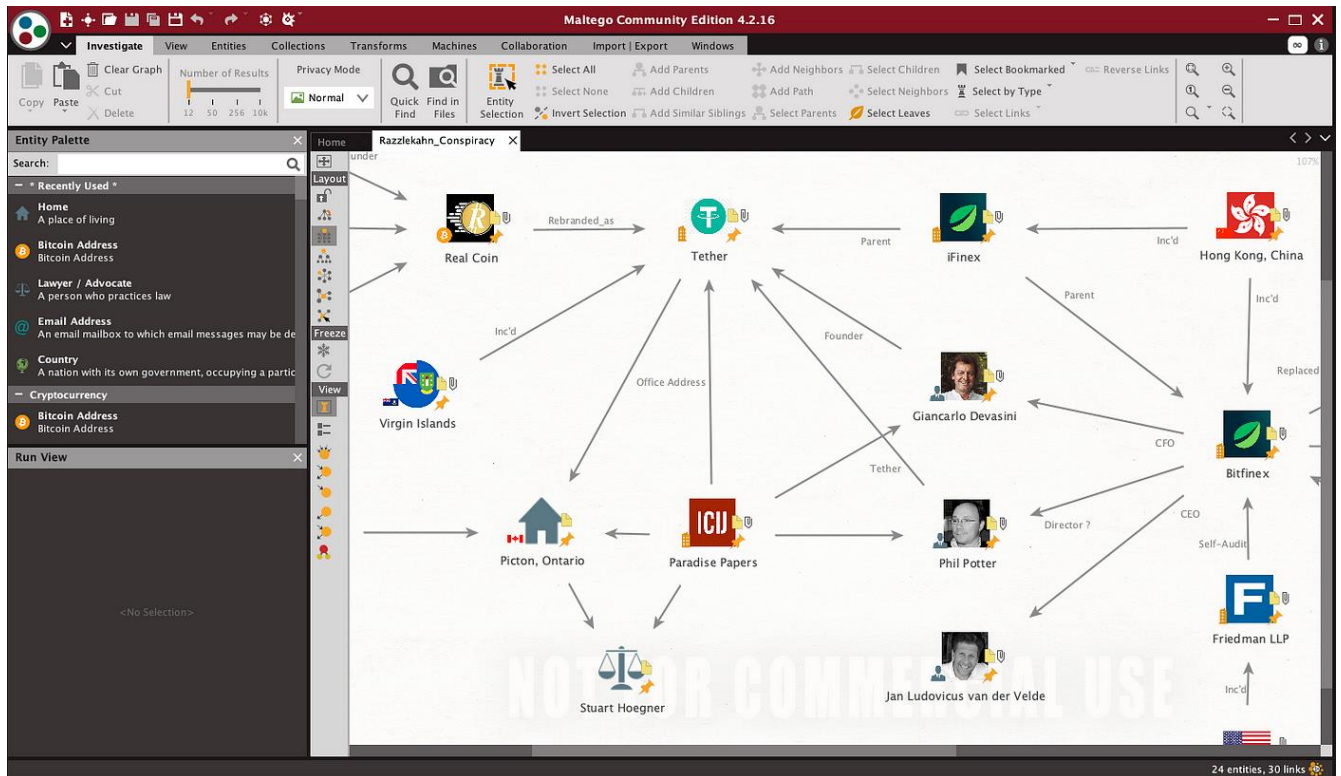


Рисунок 2.1 – Графічний інтерфейс програмного забезпечення Maltego

Maltego має інтуїтивний інтерфейс та включає в себе набір інструментів, які дозволяють швидко і ефективно аналізувати та візуалізувати дані. Наприклад, за допомогою Maltego можна знайти зв'язки між різними елементами, такими як електронні адреси або IP-адреси, що можуть бути пов'язані з однією та самою особою або групою зловмисників. Також, Maltego може допомогти в ідентифікації потенційних зловмисників та їх зв'язків, а також детально проаналізувати їх діяльність.

Крім того, Maltego дозволяє експортувати зібрану інформацію у різних форматах, таких як CSV, XML, PDF та інші. Це дозволяє дослідникам кібербезпеки поділитися зібраною інформацією з іншими членами своєї команди або з іншими організаціями, що займаються боротьбою з кіберзлочинністю[18].

Maltego є потужним інструментом для дослідження, який допомагає виявляти зв'язки між об'єктами та аналізувати їх в контексті кібербезпеки. Він може бути використаний для відслідковування та аналізування даних про кібератаки, створення звітів та рекомендацій щодо захисту від них у майбутньому[27].

2.3. Програмне забезпечення Shodan.

Іншим програмним забезпеченням корисним під час розслідування є Shodan.

Shodan - це програмне забезпечення для пошуку та аналізу підключених до Інтернету пристроїв, таких як камери відеоспостереження, маршрутизатори, сервери та інші. Це пошукова система, яка використовує відкриті джерела інформації для сканування Інтернету та збору даних про підключені пристрої[19].

Shodan працює як пошукова система, що сканує Інтернет на наявність підключених до нього пристроїв. За допомогою різних методів, включаючи сканування відкритих портів та доменних імен, Shodan знаходить підключені до Інтернету пристрої та збирає про них інформацію.

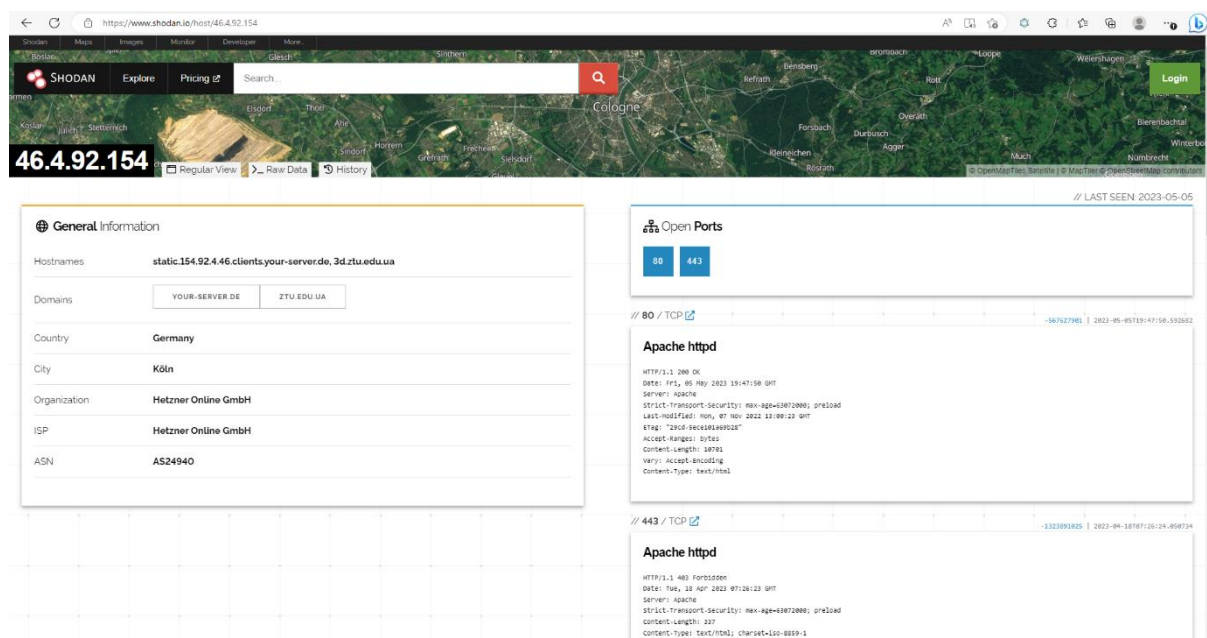


Рисунок 2.2 – Інтерфейс програмного забезпечення Shodan

Одним з ключових компонентів роботи Shodan є його база даних, яка містить інформацію про різні типи пристроїв, що підключені до Інтернету. Ця база даних постійно оновлюється зібраною інформацією про нові пристрої, що з'являються в мережі.

Крім того, Shodan має вбудовані інструменти для пошуку вразливостей у пристроях, що були знайдені. Для цього він використовує відкриті джерела, такі як бази даних вразливостей та інформацію про експлойти, щоб знайти потенційні загрози безпеці.

		Герасимчук В.В.			ККІКБ.КР.Б – 125 – 23 – ПЗ	Арк.
		Байлюк Є.М.				33
Змн.	Арк.	№ докум.	Підпис	Дата		

Додатково Shodan дозволяє користувачам складати власні запити для пошуку інформації про підключені до Інтернету пристрої, використовуючи різноманітні фільтри та параметри. Це дає користувачам більш гнучкий та точний пошук інформації, яка їм потрібна.

Shodan також має можливості для пошуку вразливостей у пристроях, які він знайшов, що дозволяє виявляти потенційні загрози безпеці мережі. Крім того, Shodan надає користувачам можливість складати власні запити та фільтрувати результати пошуку, щоб знайти саме ту інформацію, яку вони потребують.

Аналіз кіберінциденту за допомогою Shodan передбачає використання різних функцій та можливостей цієї платформи. Основним кроком є пошук пристроїв та сервісів, які були задіяні в інциденті, за допомогою ключових слів або фільтрів.

Наступним кроком є аналіз результатів, отриманих з пошуку, для визначення конфігурацій, портів та сервісів, які були використані в інциденті. Також можна досліджувати інформацію про підключені пристрої, технічну інформацію та конфігурацію мережі. Також Shodan надає можливість сканування підключених пристроїв для виявлення вразливостей, а також отримання додаткової інформації про сертифікати та інші деталі, які можуть бути корисними при розслідуванні інциденту.

Крім цього, Shodan може використовуватися для візуалізації мережі та з'ясування зв'язків між пристроями та сервісами, що може бути корисно при визначенні масштабу кіберінциденту та виявленні можливих злоумисників.

Використання Shodan у процесі розслідування кіберінцидентів дозволяє отримати значну кількість інформації про мережі та пристрої, які можуть бути задіяні в інциденті, а також інформацію про можливі вразливості та дії злоумисників.

2.4. Програмне забезпечення Recon-ng.

Recon-ng - це програмне забезпечення з відкритим вихідним кодом, яке використовується для автоматизації збору відкритої інформації з Інтернету (OSINT). Його можна використовувати як інструмент для тестування на

		Герасимчук В.В.			ККІКБ.КР.Б – 125 – 23 – ПЗ	Арк.
		Байлюк Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		34

проникнення, дослідження інформації про конкурентів або для забезпечення безпеки мережі[21].

Основна мета Reson-ng полягає у полегшенні розвідки та збору інформації з різних джерел. Воно використовує концепцію модульності, що дозволяє користувачам додавати власні модулі інтеграції з новими джерелами даних або іншими інструментами. Reson-ng володіє потужною інтерактивною оболонкою командного рядка, що дозволяє користувачам ефективно взаємодіяти з інструментом.

Reson-ng підтримує різні модулі збору інформації, такі як модулі для сканування веб-сайтів, електронної пошти, соціальних мереж та інших джерел відкритої інформації. Він може збирати інформацію про домени, IP-адреси, електронні адреси, веб-сайти, соціальні мережі та інші дані, які можуть бути корисні для аналізу та вирішення проблем безпеки.

Один з головних переваг Reson-ng полягає у його здатності до автоматизації збору інформації. Це дозволяє користувачам ефективно збирати інформацію про цільову систему та проводити аналіз цифрових слідів з мінімальною втратою часу. Крім того, Reson-ng може інтегруватись з іншими інструментами для тестування на проникнення, що забезпечує зручну інтеграцію з іншими інструментами та складними процесами автоматизації.

Усі зібрані дані можна зберегти у базі даних, що дозволяє легко знаходити та аналізувати зібрану інформацію в майбутньому. Додатково, Reson-ng надає користувачам засоби для взаємодії з іншими інструментами та сервісами, такими як бази даних, пошукові системи та інші, що дозволяє зробити прикладні програми більш ефективними та гнучкими.

Reson-ng має підтримку плагінів, які дозволяють користувачам додавати нові функції та можливості до програмного забезпечення. Це дозволяє розширювати можливості Reson-ng та використовувати його для збору специфічної інформації або для вирішення конкретних задач.

		Герасимчук В.В.			ККІКБ.КР.Б – 125 – 23 – ПЗ	Арк.
		Байлюк Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		35

```

[recon-ng][default] > db delete contacts
rowid(s) (INT): 3
[*] 1 rows affected.
[recon-ng][default] > show contacts

+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| rowid | first_name | middle_name | last_name | email | title | region | country | phone | notes | module |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| 1 | Craig | | Fancy | @bbc.com | Whois contact | Chicago, IL | United States | | | whois_pocs |
| 2 | Charles | | Keating | @kbbcc.com | Whois contact | Tualatin, OR | United States | | | whois_pocs |
| 4 | Justin | | Van Abrahams | @dbbc.com | Whois contact | Sacramento, CA | United States | | | whois_pocs |
| 5 | Justin | | VanAbrahams | @dbbc.com | Whois contact | Fresno, CA | United States | | | whois_pocs |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+

[*] 4 rows returned
[recon-ng][default] > insert contacts
first_name (TEXT): k1sec
middle_name (TEXT): k1sec
last_name (TEXT): k1sec
email (TEXT): test@k1sec.com
title (TEXT): k1sec
region (TEXT): KOREA
country (TEXT): seoul
phone (TEXT):
notes (TEXT):
[*] 1 rows affected.
[recon-ng][default] > show contacts

+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| rowid | first_name | middle_name | last_name | email | title | region | country | phone | notes | module |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| 1 | Craig | | Fancy | @bbc.com | Whois contact | Chicago, IL | United States | | | whois_pocs |
| 2 | Charles | | Keating | @kbbcc.com | Whois contact | Tualatin, OR | United States | | | whois_pocs |
| 4 | Justin | | Van Abrahams | @dbbc.com | Whois contact | Sacramento, CA | United States | | | whois_pocs |
| 5 | Justin | | VanAbrahams | @dbbc.com | Whois contact | Fresno, CA | United States | | | whois_pocs |
| 6 | k1sec | | k1sec | test@k1sec.com | k1sec | KOREA | seoul | | | user_defined |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+

[*] 5 rows returned
[recon-ng][default] >

```

Рисунок 2.3 – Інтерфейс програмного забезпечення Recon-ng

Загальна структура Recon-ng базується на модульній системі, де кожен модуль відповідає за збір певного виду інформації. Модулі можуть бути запущені окремо або в комплексі для збору більш широкого спектру інформації. Крім того, користувачі можуть налаштовувати параметри модулів, щоб збирати конкретну інформацію та контролювати процес збору.

Для того, щоб почати використовувати Recon-ng, користувачам потрібно буде налаштувати його конфігурацію та додати необхідні модулі. Для цього вони можуть скористатися документацією, яка містить детальний опис функцій та параметрів модулів, або скористатися плагінами та скриптами, щоб зробити налаштування більш простим та швидким.

Наведемо приклад команд для збору інформації з веб-сайту[20]:

```

$ recon-ng
[recon-ng][default] > marketplace search domained
[recon-ng][default] > marketplace install recon/domained
[recon-ng][default] > modules load recon/domained
[recon-ng][default][domained] > set source example.com
[recon-ng][default][domained] > run

```

У цьому прикладі ми використовуємо модуль recon/domained в рамках Recon-ng для збору інформації про домени з вказаного джерела. Починаємо з виклику команди marketplace search domained, яка дозволяє знайти модуль recon/domained в

репозиторії модулів, доступних в Recon-ng. Після цього виконуємо команду `marketplace install recon/domained`, яка завантажує та встановлює модуль `recon/domained` у нашій локальній копії Recon-ng. Далі, виконуємо команду `modules load recon/domained`, щоб завантажити модуль `recon/domained` і підготувати його до виконання.

Наступною командою є `set source example.com`, де ми встановлюємо вихідне джерело, яким є `example.com`. Це означає, що ми будемо збирати інформацію про домени з вказаного вихідного джерела `example.com`.

Нарешті, ми виконуємо команду `run`, яка запускає модуль `recon/domained` і починає процес збору інформації про домени з вказаного джерела `example.com`. Результати цього збору інформації будуть виведені на екран або збережені для подальшого використання.

Іншим прикладом є команди для збору інформації з соціальних мереж про певного користувача:

```
$ recon-ng
[recon-ng][default] > marketplace search social
[recon-ng][default] > marketplace install recon/social
[recon-ng][default] > modules load recon/social
[recon-ng][default][social] > set username example_user
[recon-ng][default][social] > run
```

У цьому прикладі ми завантажуємо модуль `recon/social`, який дозволяє збирати інформацію з соціальних мереж за іменем користувача. Встановлюємо ім'я користувача `example_user` і запускаємо модуль для збору інформації.

В цілому, Recon-ng - це потужний та гнучкий інструмент для збору відкритої інформації, який може бути використаний для вирішення різних задач, включаючи тестування на проникнення, дослідження конкурентів та забезпечення безпеки мережі. Завдяки своїй модульній структурі та підтримці плагінів, Recon-ng може бути налаштований та розширений залежно від потреб користувача.

2.5. Програмне забезпечення theHarvester.

theHarvester - це спеціалізоване програмне забезпечення, яке використовується для збору інформації з відкритих джерел для проведення розвідки або пентестів. Воно дозволяє здійснювати пошук та витягувати

		Герасимчук В.В.			ККІКБ.КР.Б – 125 – 23 – ПЗ	Арк.
		Байлюк Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		37

різноманітну інформацію про цільову компанію, включаючи електронні адреси, піддомени, імена хостів, веб-сервери, поштові сервери, номери телефонів, а також посилання на соціальні мережі та інше[25].

theHarvester працює на основі пошукових запитів до відкритих джерел, таких як пошукові системи (Google, Bing), соціальні мережі, DNS-сервери тощо. Він сканує ці джерела за допомогою API або прямого взаємодії з ними, а потім обробляє отримані результати, витягуючи необхідну інформацію.

theHarvester може шукати електронні адреси, пов'язані з цільовою компанією, використовуючи різні джерела, такі як веб-сайти, соціальні мережі, публічні бази даних тощо. Це дозволяє зібрати списки електронних адрес, які можуть бути використані для подальшої аналізу або для виявлення потенційних вразливостей. Також theHarvester може сканувати DNS-сервери, щоб виявити піддомени та імена хостів, пов'язані з цільовою компанією. Це допомагає відкрити ширший обсяг ресурсів, які належать компанії, та виявити можливі слабкі місця або ризики.

Іншою здатністю даного програмного забезпечення є сканування веб-сайтів та виявлення різноманітних деталей, а саме: використані веб-сервери, поштові сервери, зареєстровані домени та інше. Це дозволяє отримати технічну інформацію про інфраструктуру компанії та ідентифікувати можливі вразливості або слабкі місця.

Додатково, підтримується Інтеграція з іншими інструментами: theHarvester може використовуватися в поєднанні з іншими програмними засобами для проведення комплексного збору інформації та розвідки. Він підтримує інтеграцію з іншими інструментами, такими як Maltego, Recon-ng та інші.

		Герасимчук В.В.			ККІКБ.КР.Б – 125 – 23 – ПЗ	Арк.
		Байлюк Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		38

- публічні бази даних: theHarvester перевіряє публічні бази даних, такі як публічні реєстри, форуми, списки розсилок тощо, для пошуку витоків електронних адрес, пов'язаних з цільовою компанією. Він може аналізувати великі обсяги даних, шукаючи збіги з доменами або ключовими словами, що вказують на належність електронної адреси до компанії;

- додаткові джерела: theHarvester також може використовувати інші джерела інформації, такі як пошукові системи, блоги, форуми тощо, для пошуку електронних адрес, пов'язаних з цільовою компанією. Він може адаптуватися до різних джерел та форматів даних, щоб забезпечити максимальний охоплення інформації.

Після збору електронних адрес theHarvester може зберегти їх у вигляді списку або іншої структури даних, яка легко інтегрується з іншими інструментами аналізу даних або для подальшої обробки. Зібрані електронні адреси можуть бути використані для різних цілей, включаючи контактування, проведення фішингових атак, виявлення потенційних вразливостей та іншого аналізу[23].

Синтаксис команди є наступним[22]:

```
theHarvester [-h] -d DOMAIN [-l LIMIT] [-S START] [-p] [-s]
               [--screenshot SCREENSHOT] [-v] [-e DNS_SERVER] [-t]
               [-r [DNS_RESOLVE]] [-n] [-c] [-f FILENAME] [-b SOURCE]
```

theHarvester є потужним інструментом для збору інформації про компанії з використанням відкритих джерел. Використовуючи його можливості, дослідники, пентестери та аналітики можуть отримати важливі відомості для проведення аналізу, виявлення потенційних загроз або підвищення рівня безпеки компанії.

2.6. Програмне забезпечення MetaGoofil.

MetaGoofil є програмним забезпеченням з відкритим вихідним кодом, призначеним для збору метаданих з різних документів, що розміщені в Інтернеті. Використовуючи OSINT-підходи (Open Source Intelligence), MetaGoofil дозволяє здійснювати аналіз цих метаданих і отримувати корисну інформацію про документи та їх власників.

		Герасимчук В.В.			ККІКБ.КР.Б – 125 – 23 – ПЗ	Арк.
		Байлюк Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		40

MetaGoofil дозволяє встановлювати параметри пошуку, такі як ключові слова, обмеження за розміром файлів, типами файлів та інші параметри, що допомагають точніше налаштувати процес збору метаданих. Після виконання пошуку MetaGoofil здійснює аналіз знайдених документів та витягує з них метадані, які можуть включати імена авторів, електронні адреси, дати створення та редагування, версії програмного забезпечення та багато іншої корисної інформації.

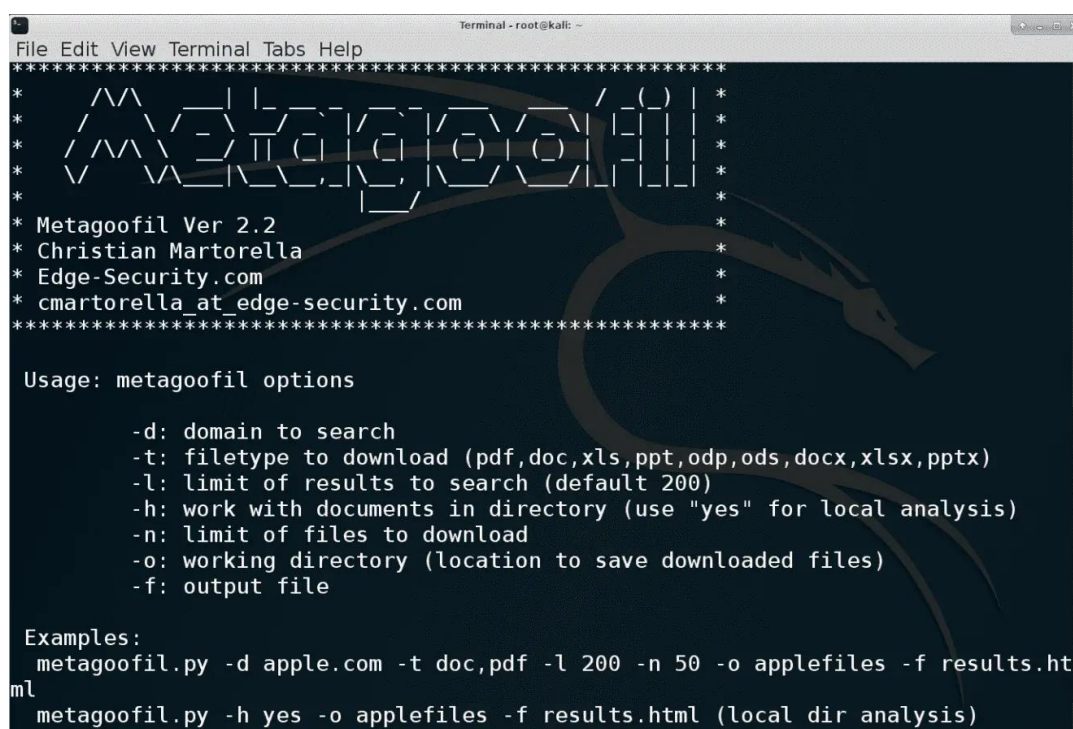


Рисунок 2.5 – Интерфейс программного обеспечения «Metagoofil»

Отримані метадані можуть бути використані для різних цілей, включаючи аналіз документів, виявлення зв'язків між різними суб'єктами, ідентифікацію можливих загроз та вразливостей, а також побудову загального зображення про діяльність та структуру організації або особи.

```
metagoofil -d [domain] -l [count] -n [count] -t [document types] -o [target folder]
```

		Герасимчук В.В.			ККІКБ.КР.Б – 125 – 23 – ПЗ	Арк.
		Байлюк Є.М.				41
Змн.	Арк.	№ докум.	Підпис	Дата		

MetaGoofil є потужним інструментом для збору та аналізу метаданих, що дозволяє дослідникам та кібербезпековим спеціалістам отримати цінну інформацію з відкритих джерел і використовувати її для дослідження, аналізу кіберінцидентів та забезпечення кібербезпеки.

Висновки до другого розділу

У цьому розділі ми розглянули методологію дослідження кіберінцидентів за допомогою методів OSINT та програмні засоби, які можуть бути використані для здійснення такого дослідження.

Методологія дослідження кіберінцидентів за допомогою методів OSINT передбачає збір та аналіз відкритих даних з різних джерел, таких як соціальні мережі, форуми, блоги, новинні сайти та інші. Такий аналіз може допомогти виявити злочинців, з'ясувати мотиви їх дій та забезпечити підстави для подальшого юридичного переслідування.

		Герасимчук В.В.			ККІКБ.КР.Б – 125 – 23 – ПЗ	Арк.
		Байлюк Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		42

РОЗДІЛ 3. ПРАКТИЧНИЙ ДОСВІД ВИКОРИСТАННЯ OSINT

3.1. Розслідування кіберінциденту спам-розсилки фішингового листа.

Уявімо, що ми отримали електронний лист на корпоративну пошту, який містить фішинговий контент. Такий лист може намагатися видати себе за офіційне повідомлення від компанії, банку або іншої організації для подальшого отримання конфіденційних даних.

Важливо зауважити, що фішингові листи можуть дуже вміло маскуватися під офіційні повідомлення. Вони можуть містити просунуті техніки соціальної інженерії, аби змусити вас надати свої особисті дані, такі як паролі, номери кредитних карток або інші конфіденційні відомості.

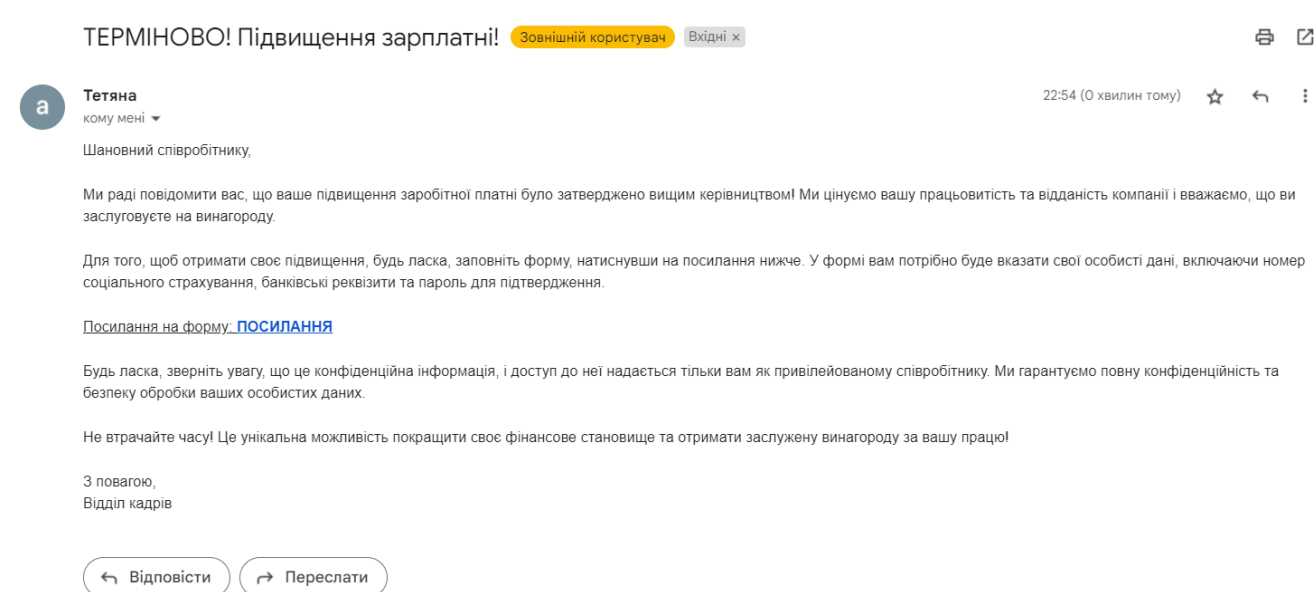


Рисунок 3.1 – Отриманий фішинговий лист

Фішингові листи часто містять такі ознаки:

- вимога негайної дії: Лист може намагатися створити почуття терміновості, наголошуючи, що вам потрібно негайно надати свої дані або здійснити певні дії;
- посилання на підроблені веб-сторінки: Фішинговий лист може містити посилання, яке здається офіційним, але фактично веде до підробленої веб-сторінки, де ваші дані будуть викрадені;
- неперевірені відправники: Лист може мати відправника, який не пов'язаний з вашою компанією;

		Герасимчук В.В.			ККІКБ.КР.Б – 125 – 23 – ПЗ	Арк.
		Байлюк Є.М.				43
Змн.	Арк.	№ докум.	Підпис	Дата		

- нестандартний запит: Лист може містити запити про надання конфіденційної інформації, яка не є звичайною для вашої організації.

Очевидно, що даний лист має фішинговий характер та використовує психологічні хитрощі, аби змусити кінцевого користувача натиснути на посилання. Цей тип атаки є одним з найпоширеніших методів соціального інженерінгу, який спрямований на отримання конфіденційної інформації або нелегітимний доступ до системи.

Відправників таких фішингових листів можна поділити на 2 групи. Перша група - це новачки, які вирішили протестувати компанію у площині усвідомленості працівників щодо кібербезпеки.. Друга група - це професійні хакери, які володіють високим рівнем експертизи у кібербезпеці. Вони використовують фішингові листи як один з методів для збору інформації та виявлення точки входу в мережу підприємства.

Отже, працівникам відповідальним за кібербезпеку підприємства варто дослідити даний лист та прийняти рішення щодо покращення інформаційної безпеки підприємства.

Відправною точкою у даному розслідуванні буде адреса електронної скриньки відправника та його IP-адреса.

Завантажимо лист на персональний комп'ютер та відкриємо його у текстовому редакторі. Таким чином ми можемо побачити Ір-адресу відправника або назву сервіса через який була здійснена пересилка. Приклад відкритого листа можна побачити на рисунку 3.2.

Для відкриття листа ми використали програмне забезпечення "VS Code". Під час перегляду файлу листа, який зображений на рисунку 3.19, було помічено, що в 25-му рядку міститься IP-адреса сервісу відправника: 209.85.220.41.

		Герасимчук В.В.			ККІКБ.КР.Б – 125 – 23 – ПЗ	Арк.
		Байлюк Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		44

```

TERMINOVO! Підвищення зарплатні!.eml
C: > Users > a1222 > Downloads > TERMINOVO! Підвищення зарплатні!.eml
21      dmn4sG1xrYx+YgkbK2JvVwM3j3GfXpGYHnY309QmVE+fBrSimvi+ayw/o842Tk1Br7D
22      5p5Q==
23      ARC-Authentication-Results: i=1; mx.google.com;
24      dkim=pass header.i=@gmail.com header.s=20221208 header.b="IXVxf/3F";
25      spf=pass (google.com: domain of a122212221a@gmail.com designates 209.85.220.41 as permitted sender) smtp.mailfrom=a122212221a@gmail.com;
26      dmarc=pass (p=NONE sp=QUARANTINE dis=NONE) header.from=gmail.com
27      Return-Path: <a122212221a@gmail.com>
28      Received: from mail-sor-f41.google.com (mail-sor-f41.google.com. [209.85.220.41])
29      by mx.google.com with SMTPS id f12-20020ac840cc00000b003ef3b631288sor7683970qtm.8.2023.05.30.12.54.09
30      for <kb192_gvv@student.ztu.edu.ua>
31      (Google Transport Security);
32      Tue, 30 May 2023 12:54:10 -0700 (PDT)
33      Received-SPF: pass (google.com: domain of a122212221a@gmail.com designates 209.85.220.41 as permitted sender) client-ip=209.85.220.41;
34      Authentication-Results: mx.google.com;
35      dkim=pass header.i=@gmail.com header.s=20221208 header.b="IXVxf/3F";
36      spf=pass (google.com: domain of a122212221a@gmail.com designates 209.85.220.41 as permitted sender) smtp.mailfrom=a122212221a@gmail.com;
37      dmarc=pass (p=NONE sp=QUARANTINE dis=NONE) header.from=gmail.com
38      DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
39      d=gmail.com; s=20221208; t=1685476449; x=1688068449;
40      h=to:subject:message-id:date:from:mime-version:from:to:cc:subject
41      :date:message-id:reply-to;
42      bh=7EZsiVfsJISyc7tIXQmTbfQsfz0FVsbjndM7JrEUK6I=;
43      b=IXVxf/3FHRSSHF7s0Wp1lw0hLEois4uVW6QG9P3FRLC/nMT+fIZTwEGt5mdN5aFB
44      ceREAWiW32o5xqS40du/XZ7LxwSzmMqfURf1Qxw3BSx0L6md7zdUPYd/sJkf8Upv9qp
45      tDwlt6FG601N8qWAXSSsqITpQ7YmGmfWRMuRDZgQsKP+IxMRzyt6SFLH6Trr9hZKi
46      RYh2B2QEZlWlFYrxxxGmth+Rz sMlowu/sPxb4W0ZF4gtYGIbN8vUucuVFWBfB1KSgjrJ
47      S3bJebSfaP2rKncpLzHGOGORNI3dbnKMAJVIrEkW1IeL+pVB6FnQzWOMf4MCCGD+2RSX
48      dFLQ==
49      X-Google-DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
50      d=gmail.com; s=20221208; t=1685476449; x=1688068449;

```

Рисунок 3.2 – Деталі отриманого листа

Для отримання додаткової інформації про цей IP-адресу, ми скористалися інструментом "Whois". За допомогою веб-ресурсу "<https://whoer.net/ru/checkwhois>" ми здійснили перевірку та дізналися інформацію про хостинг-провайдера, який надає послуги для даної IP-адреси.

Використання інструменту "Whois" дозволяє нам отримати деталі про власника IP-адреси, включаючи назву компанії або організації, контактну інформацію та інші відомості, які можуть бути корисні при подальшому розслідуванні. Цей інструмент є потужним засобом для визначення джерела атаки та встановлення зв'язків між різними IP-адресами та хостинг-провайдерами.

IP address: **209.85.220.41**

Location: United States (US), N/A

Region: N/A

City: N/A

ZIP: N/A

Hostname: mail-sor-f41.google.com → 209.85.220.41

IP range: 209.85.192.0 - 209.85.255.255

ISP: Google

Organization: Google

Blacklist: No

TOR: No

Zone: America/Chicago

Local: Mon Jan 30 2023 15:30:17 GMT-0600 (CST)

Рисунок 3.3 – Відомості про IP-адресу з якого було надіслано лист

Отже, після отримання базової інформації про хостинг-провайдера, через який здійснювалась пересилка листа, ми маємо можливість зробити запит до

		Герасимчук В.В.			ККІКБ.КР.Б – 125 – 23 – ПЗ	Арк.
		Байлюк Є.М.				45
Змн.	Арк.	№ докум.	Підпис	Дата		

даного провайдера та отримати деталі про користувача, який стояв за фішинговою атакою на корпоративну мережу підприємства.

Проте, інформації, яку ми отримали, може бути недостатньою для виявлення особистості зловмисника. Тому, для подальшого розслідування, ми використаємо програмне забезпечення, яке дозволяє виявити перелік веб-сайтів, для яких використовується пошта зловмисника. Цей крок дозволить нам отримати додаткові деталі, які можуть бути корисними для передачі інформації компетентним органам з метою вжиття правових заходів або для встановлення наміру та рівня злочинця.

Використання спеціалізованого програмного забезпечення дозволяє автоматизувати процес виявлення пов'язаних зловмисником веб-сайтів та забезпечує більш ефективне збирання інформації. Це дозволяє нам розширити обсяг даних, які ми можемо отримати про зловмисника та його діяльність.

Для досягнення цієї мети використаємо програмне забезпечення "Holehe", яке спеціалізується на встановленні прив'язок між електронною поштою та обліковими записами на веб-сайтах[26]. Це програмне забезпечення дозволяє виявити, які облікові записи пов'язані з вказаною електронною адресою. Важливо зазначити, що "Holehe" не розкриває ідентифікатори облікових записів і використовує законні методи для встановлення зв'язку між електронною поштою і веб-сайтом.

Шляхом введення цієї електронної адреси в програмне забезпечення, ми отримуємо результат, який показує, на яких веб-сайтах ця адреса була використана для створення облікових записів. Це дозволить нам отримати додаткову інформацію про зловмисника та його діяльність.

		Герасимчук В.В.			ККІКБ.КР.Б – 125 – 23 – ПЗ	Арк.
		Байлюк Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		46

```
[x] patreon.com
[+] pinterest.com
[x] pipedrive.com
[-] plurk.com
[-] pornhub.com
[-] protonmail.ch
[-] quora.com
[-] rambler.ru
[-] redtube.com
[-] replit.com
[x] rocketreach.co
[x] samsung.com
[-] seoclerks.com
[-] 7cups.com
[-] smule.com
[x] snapchat.com
[x] soundcloud.com
[-] sporcle.com
[-] spotify.com
[-] strava.com
[-] taringa.net
[x] teamleader.eu
[-] teamtreehouse.com
[-] tellonym.me
[-] thecardboard.org
[-] forums.therian-guide.com
[x] thevapingforum.com
[-] tumblr.com
[x] tuneind.com
[+] twitter.com
[x] venmo.com
[x] vivino.com
[-] voxmedia.com
[-] vrbo.com
[x] vsco.co
[-] wattpad.com
[-] wordpress.com
[-] xing.com
[-] xnxx.com
[-] xvideos.com
[x] yahoo.com
[-] zoho.com

[+] Email used, [-] Email not used, [x] Rate limit
121 websites checked in 11.97 seconds
Twitter : @palenath
Github : https://github.com/megadose/holehe
For BTC Donations : 1FHDm49QfZX6pJmhjLE5tB2K6CaTLMzPzXZ
100%
```

Рисунок 3.4 – Звіт про використання данної електронної адреси

Отже, після використання програмного забезпечення "Holehe" ми бачимо, що електронна адреса відправника фактично прив'язана до деяких сервісів. Це вказує на наявність облікових записів, які були створені з використанням цієї адреси. Щоб отримати більше інформації про користувача та ідентифікувати його, ми можемо провести подальший пошук інформації щодо кожного з цих сервісів.

Подальший пошук може включати перевірку публічних профілів користувача на соціальних мережах, форумах або інших платформах, де він може бути активним. Також можна виконати пошук інформації в публічних базах даних, що містять відомості про користувачів. Це допоможе зібрати більше відомостей про особу, яка стоїть за фішинговим листом.

Проте в рамках даного завдання, ми припиняємо подальший пошук інформації про користувача. Вже наявна інформація про облікові записи, пов'язані з вказаною електронною адресою, може бути достатньою для нашої цілі. Дані, які

		Герасимчук В.В.			ККІКБ.КР.Б – 125 – 23 – ПЗ	Арк.
		Байлюк Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		47

ми отримали, можуть бути використані для подальшого розслідування, вжиття відповідних заходів або передачі інформації правоохоронним органам.

Таким чином, використавши, тільки методи та інструменти OSINT ми дізналися через який сервіс здійснювалась розсилка повідомлення, де зберігається інформація про відправника та отримали список аккаунтів, які прив'язані до даної пошти. Зібрана інформація в подальшому, звісно, якщо ми будемо звертатися до правоохоронних органів, пришвидшить розслідування справи та дасть можливість оперативного реагування на такий випадок.

3.2. Збір інформації про домен з використанням спеціалізованого програмного забезпечення.

Збір інформації про компанію з використанням спеціалізованого програмного забезпечення є процесом, в якому використовуються інструменти та ресурси відкритих джерел розвідки для збору інформації про певну компанію. Цей підхід дозволяє отримати доступ до публічно доступної інформації, яка може бути корисною для різних цілей, а саме: конкурентний аналіз, перевірка довіри, оцінка репутації та розслідування кіберінцидентів.

У першу чергу використаємо програмне забезпечення «theHarvester». Пошук електронних адрес є однією з ключових функцій програмного забезпечення theHarvester. Він дозволяє знаходити електронні адреси, які пов'язані з цільовою компанією або її співробітниками, шляхом сканування різних джерел інформації, таких як веб-сайти, соціальні мережі, публічні бази даних тощо.

Основні аспекти пошуку електронних адрес за допомогою theHarvester:

- збір електронних адрес з веб-сайтів: theHarvester може переглядати веб-сайти, пов'язані з цільовою компанією, і витягувати електронні адреси, які можуть бути вказані на цих веб-сторінках. Він аналізує різні розділи веб-сайтів, такі як "Контакти", "Про нас", "Команда" тощо, а також знаходить електронні адреси, які можуть бути розміщені у текстових блоках, посиланнях або зображеннях;

- пошук електронних адрес в соціальних мережах: theHarvester використовує API соціальних мереж, таких як Twitter, LinkedIn, Facebook і інші,

		Герасимчук В.В.			ККІКБ.КР.Б – 125 – 23 – ПЗ	Арк.
		Байлюк Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		48

для пошуку публічно доступних електронних адрес, пов'язаних з цільовою компанією або її співробітниками. Він може переглядати профілі компанії, робочі профілі співробітників, дописи, коментарі тощо, щоб зібрати електронні адреси;

- використання публічних баз даних: theHarvester може перевіряти публічні бази даних, такі як публічні реєстри, форуми, списки розсилок тощо, для пошуку електронних адрес, які пов'язані з цільовою компанією. Він виконує аналіз великих обсягів даних, шукаючи збіги з доменами, іменами співробітників або інших ідентифікаторів компанії.

Зібрані електронні адреси можуть бути використані для різних цілей. Наприклад, їх можна використовувати для зв'язку з компанією чи співробітниками, проведення аналізу комунікаційної мережі компанії, виявлення потенційних вразливостей через публічно доступну інформацію тощо. Важливо зазначити, що використання зібраних електронних адрес повинно відповідати правовим обмеженням та етичним стандартам.

Здійснено пошук для домену «ztu.edu.ua», встановимо ліміт пошукових результатів як 500 та джерелом пошукову систему «Bing».

Отже, після здійснення пошуку були отримані певні результати. За допомогою програмного забезпечення "theHarvester" було знайдено 6 поштових адрес, які пов'язані з цільовим доменом. Ці поштові адреси можуть вказувати на існуючих користувачів, співробітників або контактну інформацію, пов'язану з доменом.

Крім того, під час пошуку було встановлено наявність 25 хостів, які також функціонують у рамках даного домену. Хост - це комп'ютер або пристрій, який забезпечує доступ до мережі Інтернет. В даному випадку, це означає, що домен має 25 різних хостів, які можуть бути використані для хостингу веб-сайтів, електронної пошти або інших онлайн-сервісів.

		Герасимчук В.В.			ККІКБ.КР.Б – 125 – 23 – ПЗ	Арк.
		Байлюк Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		49

```

(kali@kali)-[~]
$ theHarvester -d ztu.edu.ua -l 500 -b bing
*****
* theHarvester 4.2.0
* Coded by Christian Martorella
* Edge-Security Research
* cmartorella@edge-security.com
*****

[*] Target: ztu.edu.ua

    Searching 0 results.
[*] Searching Bing.

[*] No IPs found.

[*] Emails found: 6
-----
kgt_pav@ztu.edu.ua
lib_olga@ztu.edu.ua
liceum@ztu.edu.ua
pr_k@ztu.edu.ua
rvv@ztu.edu.ua
yefimenko.andrii@ztu.edu.ua

[*] Hosts found: 25
-----
conf.ztu.edu.ua:46.4.92.154
cs.ztu.edu.ua:46.4.92.154
docs.ztu.edu.ua:46.4.92.154
ecology.ztu.edu.ua:46.4.92.154
ema.ztu.edu.ua:212.111.212.230
eztuir.ztu.edu.ua:195.69.223.138
gef-news.ztu.edu.ua:46.4.92.154
inteuas.ztu.edu.ua:46.4.92.154
krt-news.ztu.edu.ua:195.69.223.138
languagehub.ztu.edu.ua:46.4.92.154
learn.ztu.edu.ua:46.4.92.154
lib.ztu.edu.ua:195.69.223.138
lyceum.ztu.edu.ua:46.4.92.154
news.ztu.edu.ua:46.4.92.154

```

Рисунок 3.5. – Виконання пошуку

Здійснимо пошук інформації з встановленням джерела пошуку як "all". Це означає, що пошук інформації про цільовий домен буде здійснюватися у всіх наявних пошукових системах, таких як Google, Bing, Yahoo, DuckDuckGo та інші. Використання опції "all" дозволяє охопити максимальну кількість джерел і отримати більш повну інформацію.

Пошук "all" може бути більш результативним, оскільки різні пошукові системи можуть мати свої власні бази даних та алгоритми індексації. Кожна система може відображати різний спектр результатів, тому широкий пошук дозволяє охопити різноманітні джерела та зібрати більше інформації про цільовий домен.

```

AS24940
AS28996

[*] Interesting Urls found: 4

http://ztu.edu.ua/
https://3d.ztu.edu.ua/
https://conf.ztu.edu.ua/wp-content/uploads/2017/01/186.pdf
https://ztu.edu.ua/

[*] LinkedIn Links found: 0

[*] IPs found: 12

46.4.92.154
188.231.212.130
188.231.212.131
188.231.212.133
195.69.223.138
195.69.223.139
195.69.223.140
195.69.223.141
195.69.223.142
212.111.212.230

[*] Emails found: 5

liceum@ztu.edu.ua
pr_k@ztu.edu.ua
rector@ztu.edu.ua
rvv@ztu.edu.ua

[*] Hosts found: 644

1www.ztu.edu.ua:ns.ztu.edu.ua
3d.ztu.edu.ua:ztu.edu.ua.
3d.ztu.edu.ua:ns.ztu.edu.ua.
3d.ztu.edu.ua:46.4.92.154
3d.ztu.edu.ua:ns.ztu.edu.ua
a.ztu.edu.ua:ns.ztu.edu.ua
a.ztu.edu.ua:ns.ztu.edu.ua.
ac.ztu.edu.ua:ns.ztu.edu.ua
ac.ztu.edu.ua:ns.ztu.edu.ua.
acp.ztu.edu.ua:ns.ztu.edu.ua
admin.ztu.edu.ua:ns.ztu.edu.ua
admin.ztu.edu.ua:ns.ztu.edu.ua.
admissions.blog.ztu.edu.ua:ns.ztu.edu.ua
admissions.blog.ztu.edu.ua:ns.ztu.edu.ua.
allinone.ztu.edu.ua:ns.ztu.edu.ua
allinone.ztu.edu.ua:ns.ztu.edu.ua.
allinone.ztu.edu.ua:195.69.223.138
alumni.ztu.edu.ua:ns.ztu.edu.ua

```

Рисунок 3.6. – Результати пошуку

Окрім поштових адрес та хостів, було знайдено Ір-адреси, які використовуються у даному домені. Дані адреси можуть бути використані для визначення географічного розташування, виявлення спільних хостів, аналізу розподілу Ір-адрес та виявлення змін в інфраструктурі організації або пошуку вразливостей безпеки. Також було знайдено значно більшу кількість хостів, що дозволить більш комплексно поглянути на організацію мережі корпорації.

Отже, програмне забезпечення «theHarvester» надало нам дещо обмежену інформацію щодо організацію мережі підприємства. Використаємо дану інформацію як відправну точку під час використання програмного забезпечення “recon-ng”.

		Герасимчук В.В.			ККІКБ.КР.Б – 125 – 23 – ПЗ	Арк.
		Байлюк Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		51

Для отримання відомостей про наявні хости домену, використаємо модуль «brute_hosts».

Модуль "brute_hosts" в програмному забезпеченні "Recon-ng" є одним з модулів, який використовується для здійснення атак на хости (host brute-forcing). Цей модуль дозволяє виконувати перебор хостів з метою знаходження активних хостів у вказаному діапазоні IP-адрес або за допомогою списку хостів.

Основна функціональність модуля "brute_hosts" включає наступні можливості:

- перебір IP-адрес: Модуль "brute_hosts" дозволяє виконувати перебір IP-адрес в заданому діапазоні. Ви можете вказати початкову та кінцеву IP-адреси для сканування, і модуль буде перебирати усі IP-адреси в цьому діапазоні для виявлення активних хостів;
- використання списку хостів: Ви також можете використовувати модуль "brute_hosts" для перебору списку хостів, який ви надаєте. Ви можете ввести список IP-адрес або доменних імен, і модуль буде перебирати ці елементи для виявлення активних хостів;
- налаштування параметрів: Модуль "brute_hosts" надає можливості налаштування різних параметрів для сканування. Ви можете встановити таймаути, кількість паралельних процесів, типи сканування (TCP, UDP тощо) та інші параметри, щоб налаштувати процес перебору хостів відповідно до вашого випадку використання;
- збереження результатів: Модуль "brute_hosts" дозволяє зберігати результати сканування у різних форматах. Ви можете зберегти результати в текстовому форматі, який містить інформацію про знайдені активні хости, їхні IP-адреси та інші відомості.

Встановимо джерело як «ztu.edu.ua» та виконаємо пошук хостів.

		Герасимчук В.В.			ККІКБ.КР.Б – 125 – 23 – ПЗ	Арк.
		Байлюк Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		52

```
[recon-ng][TEST][brute_hosts] > options list
```

Name	Current Value	Required	Description
SOURCE	default	yes	source of input (see 'info' for details)
WORDLIST	/home/kali/.recon-ng/data/hostnames.txt	yes	path to hostname wordlist

```
[recon-ng][TEST][brute_hosts] > options set SOURCE ztu.edu.ua
SOURCE => ztu.edu.ua
[recon-ng][TEST][brute_hosts] > run
```

```
ZTU.EDU.UA

[*] Wildcard DNS entry found for 'ztu.edu.ua' at 'ns.ztu.edu.ua.'.
[*] 11.ztu.edu.ua => Response matches the wildcard.
[*] 12.ztu.edu.ua => Response matches the wildcard.
[*] 0.ztu.edu.ua => Response matches the wildcard.
[*] 13.ztu.edu.ua => Response matches the wildcard.
[*] 02.ztu.edu.ua => Response matches the wildcard.
[*] 10.ztu.edu.ua => Response matches the wildcard.
[*] 01.ztu.edu.ua => Response matches the wildcard.
[*] 17.ztu.edu.ua => Response matches the wildcard.
[*] 1.ztu.edu.ua => Response matches the wildcard.
[*] 03.ztu.edu.ua => Response matches the wildcard.
[*] 18.ztu.edu.ua => Response matches the wildcard.
[*] 15.ztu.edu.ua => Response matches the wildcard.
[*] 3com.ztu.edu.ua => Response matches the wildcard.
[*] 4.ztu.edu.ua => Response matches the wildcard.
[*] 3.ztu.edu.ua => Response matches the wildcard.
[*] 2.ztu.edu.ua => Response matches the wildcard.
[*] 5.ztu.edu.ua => Response matches the wildcard.
[*] 19.ztu.edu.ua => Response matches the wildcard.
[*] 9.ztu.edu.ua => Response matches the wildcard.
[*] 8.ztu.edu.ua => Response matches the wildcard.
[*] 16.ztu.edu.ua => Response matches the wildcard.
[*] 14.ztu.edu.ua => Response matches the wildcard.
[*] 7.ztu.edu.ua => Response matches the wildcard.
[*] a.ztu.edu.ua => Response matches the wildcard.
[*] a.auth-ns.ztu.edu.ua => Response matches the wildcard.
[*] a01.ztu.edu.ua => Response matches the wildcard.
[*] ILMI.ztu.edu.ua => Response matches the wildcard.
[*] a1.ztu.edu.ua => Response matches the wildcard.
[*] a2.ztu.edu.ua => Response matches the wildcard.
[*] access.ztu.edu.ua => Response matches the wildcard.
[*] about.ztu.edu.ua => Response matches the wildcard.
[*] a02.ztu.edu.ua => Response matches the wildcard.
[*] ac.ztu.edu.ua => Response matches the wildcard.
[*] abc.ztu.edu.ua => Response matches the wildcard.
```

Рисунок 3.7 – Процес пошуку хостів за допомогою ПЗ «recon-ng»

Після виконання пошуку ми отримуємо короткий звіт про результати пошуку. У звіті наведено знайдені хости, їхні ір-адреси та додаткову інформацію про місцезнаходження. У нашому випадку модуль не вставляє місцезнаходження хостів, тому дана інформація відсутня.

```
SUMMARY
[*] 49 total (37 new) hosts found.
[recon-ng][TEST][brute_hosts] > show hosts
```

rowid	host	ip_address	region	country	latitude	longitude	notes	module
1	ghs.googlehosted.com							brute_hosts
2	calendar.ztu.edu.ua							brute_hosts
3	calendar.ztu.edu.ua	192.178.25.179						brute_hosts
4	ztu.edu.ua							brute_hosts
5	conf.ztu.edu.ua							brute_hosts
6	conf.ztu.edu.ua	46.4.92.154						brute_hosts
7	cs.ztu.edu.ua							brute_hosts
8	cs.ztu.edu.ua	46.4.92.154						brute_hosts
9	docs.ztu.edu.ua							brute_hosts
10	docs.ztu.edu.ua	46.4.92.154						brute_hosts
11	events.ztu.edu.ua							brute_hosts
12	events.ztu.edu.ua	46.4.92.154						brute_hosts
13	gw.ztu.edu.ua	195.69.223.138						brute_hosts
14	localhost.ztu.edu.ua	127.0.0.1						brute_hosts
15	mail.ztu.edu.ua							brute_hosts
16	mail.ztu.edu.ua	46.4.92.154						brute_hosts
17	network.ztu.edu.ua							brute_hosts
18	network.ztu.edu.ua	46.4.92.154						brute_hosts
19	new.ztu.edu.ua							brute_hosts
20	new.ztu.edu.ua	46.4.92.154						brute_hosts
21	news.ztu.edu.ua							brute_hosts
22	news.ztu.edu.ua	46.4.92.154						brute_hosts
23	media.ztu.edu.ua							brute_hosts
24	media.ztu.edu.ua	46.4.92.154						brute_hosts
25	ns.ztu.edu.ua	195.69.223.138						brute_hosts
26	old.ztu.edu.ua							brute_hosts
27	old.ztu.edu.ua	46.4.92.154						brute_hosts
28	portal.ztu.edu.ua							brute_hosts
29	portal.ztu.edu.ua	46.4.92.154						brute_hosts
30	proxy.ztu.edu.ua	195.69.223.142						brute_hosts
31	reg.ztu.edu.ua	91.200.40.5						brute_hosts
32	tour.ztu.edu.ua							brute_hosts
33	tour.ztu.edu.ua	46.4.92.154						brute_hosts
34	vpn.ztu.edu.ua	195.69.223.138						brute_hosts
35	work.ztu.edu.ua							brute_hosts
36	work.ztu.edu.ua	46.4.92.154						brute_hosts
37	www.ztu.edu.ua	46.4.92.154						brute_hosts

```
[*] 37 rows returned
[recon-ng][TEST][brute_hosts] >
```

Рисунок 3.8 – Результат пошуку хостів у домені «ztu.edu.ua»

Отже, ми отримали повний список хостів, який функціонує у рамках цільового домену. Дана інформація може бути використана спеціалістами з кібербезпеки компанії для подальшого приховування хостів та Ір-адрес, які не повинні бути публічними. У результаті також вказано назву хоста «localhost.ztu.edu.ua» наявність даного хоста серед списку може свідчити про помилки конфігурації або про потенційні вразливості на одному з ресурсів домену.

Остаточний пошук інформації здійснимо пошук більш детальної інформації щодо домену та його хостів. Для цього використаємо програмне забезпечення «Maltego».

Спочатку виконаємо початкове налагодження нашого дослідження. Додамо сутність компанії, домену та наявних ір-адрес.

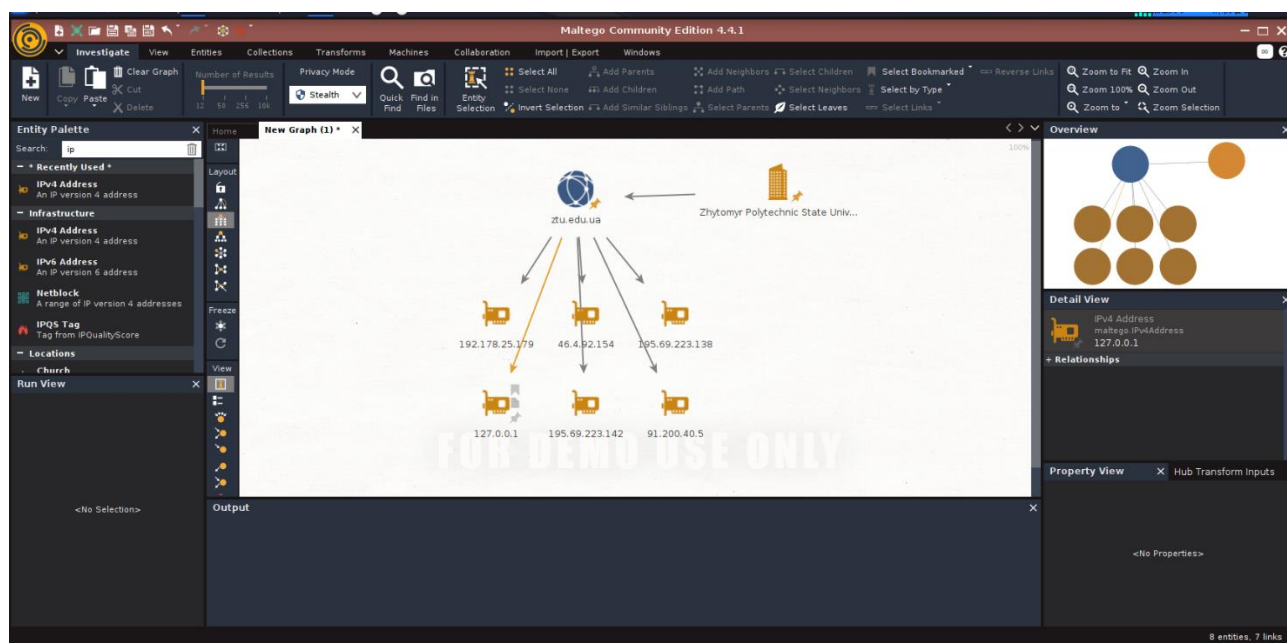


Рисунок 3.9 – Сконфігурований проект у програмному забезпеченні «Maltego».

Запустимо пошук усієї наявної інформації для встановлених Ір-адрес.

		Герасимчук В.В.			ККІКБ.КР.Б – 125 – 23 – ПЗ	Арк.
		Байлюк Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		54

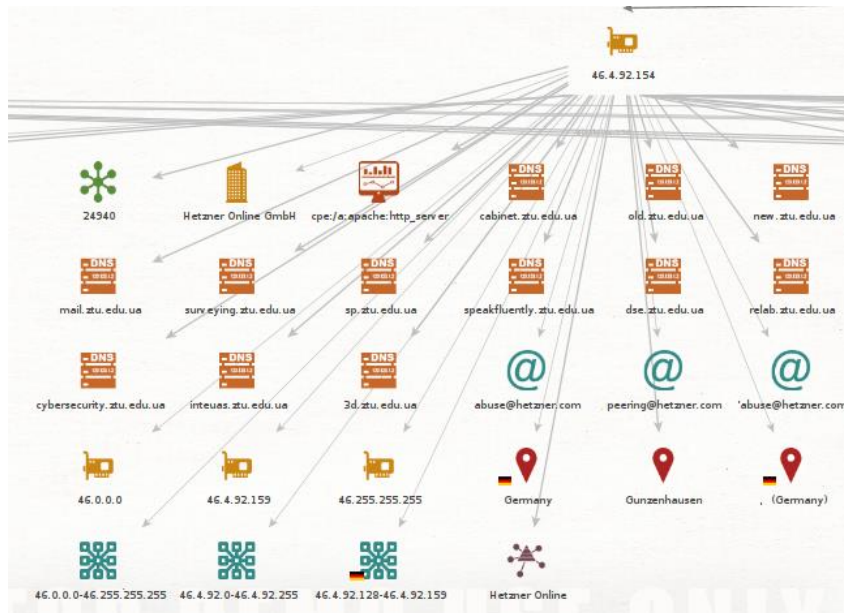


Рисунок 3.10 – Результат встановлення додаткової інформації для Ір-адреси
«46.4.92.154»

Отже, ми встановили, що хост даної Ір-адреси знаходиться у Німеччині. Також ми встановили суміжні діапазони адрес, тим серверу та доменні імена, які належать пов'язані з цією адресою. Продовжимо наші дослідження та дізнаємося додаткові відомості про доменне ім'я «cabinet.ztu.edu.ua».

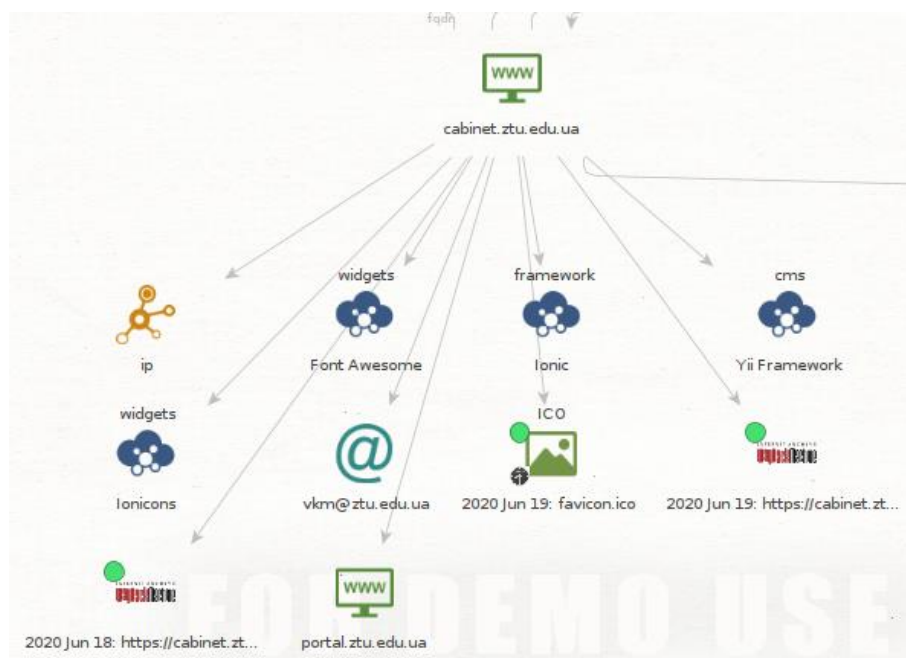


Рисунок 3.11 – Відомості про доменне ім'я «cabinet.ztu.edu.ua»

На даному домені знаходиться веб-сайт за адресою «cabinet.ztu.edu.ua». Також було встановлено, що даний веб-сайт використовує фреймворк «Ionic»,

		Герасимчук В.В.			ККІКБ.КР.Б – 125 – 23 – ПЗ	Арк.
		Байлюк Є.М.				55
Змн.	Арк.	№ докум.	Підпис	Дата		

віджети «Font Awesome» та «Ionicons» і адресу електронної пошти «vkm@ztu.edu.ua».

Знайдені результати пошуку є важливими для подальшого аналізу і дослідження. Дані результати можуть надати цінну інформацію про цільовий домен і його мережу. Наприклад, знайдені поштові адреси можуть використовуватися для встановлення зв'язку з відповідними особами, такими як співробітники, представники компанії чи адміністратори домену. Це може бути корисно для отримання додаткової інформації, обговорення питань, надсилання запитів або встановлення професійних контактів.

Крім того, результати, пов'язані з хостами, можуть бути досліджені для виявлення веб-сайтів, служб або можливих вразливостей, що функціонують у рамках цього домену. Дослідження хостів може розкрити додаткові деталі про інфраструктуру домену, розміщення веб-сайтів, використовувані технології та можливі точки входу для аналізу безпеки. Це може бути важливим для виявлення потенційних вразливостей, вимкнених служб або недостатньо захищених компонентів, що можуть мати вплив на безпеку домену чи компанії.

3.3. Аналіз веб-сайту за допомогою метаданих контенту.

Фотографії та відеозаписи, як відомо, містять метадані, що містять певну інформацію про користувача та пристрій, які використовувалися для їх створення. Однак, багато користувачів забувають, що метадані також присутні в інших типах файлів, таких як документи. У цих метаданих часто можна знайти імена облікових записів, електронні пошти, а іноді навіть повне ім'я автора документа або його телефонний номер. Теоретично, розробники веб-застосунків можуть включити автоматичне очищення метаданих з документів, які завантажуються на їхні платформи, проте в більшості випадків ні розробники, ні користувачі не звертають на це уваги.

Даний аспект надає відмінну можливість здійснювати пошук корисної інформації в документах, що доступні відкрито на веб-сайтах. Особливо цей пошук є ефективним на державних сайтах або великих компаніях, де розміщується значна

		Герасимчук В.В.			ККІКБ.КР.Б – 125 – 23 – ПЗ	Арк.
		Байлюк Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		56

кількість документів від різних користувачів. Аналіз сотень таких документів дозволяє отримати базову інформацію про співробітників компанії та отримати уявлення про ієрархію працівників, начебто маючи доступ до внутрішньої корпоративної мережі підприємства.

Варто зазначити, що цей тип аналізу є законним, оскільки ми працюємо зі загальнодоступними документами, які були добровільно розміщені в мережі. Відвідування та аналіз таких документів є легальною діяльністю, що дозволяє здобувати інформацію, яка може бути важливою для різних цілей, включаючи дослідження, аналітику або виявлення потенційних загроз.

Для вивантаження документів скористаємося застосунком «Metagoofil». Даний застосунок відповідальний за вивантаження публічних документів з певного веб-сайту та подальшого складання звіту по метаданих даних файлів.

Після параметра -d необхідно вказали цільовий домен. Потім встановити ліміт (-l) на кількість результатів пошуку та на кількість (-n) знайдених файлів для подальшого завантаження. Потім вказати необхідні типи файлів (-t). І, наприкінці (-o), необхідно вказати папку куди будуть збережені документи.

Запускаємо та чекаємо поки Metagoofil завантажить знайдені файли.

```
(kali㉿kali)-[~]
└─$ metagoofil -d learn.ztu.edu.ua -l 50 -n 50 -t pdf,doc,xls,docx,xlsx -o fssp
[+] Adding -w for you
[*] Downloaded files will be saved here: fssp
[+] Creating folder: fssp
[*] Searching for 50 .pdf files and waiting 30.0 seconds between searches
[+] Downloading file - [308633 bytes] https://learn.ztu.edu.ua/mod/resource/view.php?id=66003
[+] Downloading file - [191542 bytes] https://learn.ztu.edu.ua/mod/resource/view.php?id=56179
[+] Downloading file - [145575 bytes] https://learn.ztu.edu.ua/mod/resource/view.php?id=61992
[+] Downloading file - [216780 bytes] https://learn.ztu.edu.ua/mod/resource/view.php?id=58008
[+] Downloading file - [350289 bytes] https://learn.ztu.edu.ua/mod/resource/view.php?id=58247
[+] Downloading file - [975145 bytes] https://learn.ztu.edu.ua/mod/resource/view.php?id=1297
[+] Downloading file - [223972 bytes] https://learn.ztu.edu.ua/mod/resource/view.php?id=49586
[+] Downloading file - [503373 bytes] https://learn.ztu.edu.ua/mod/resource/view.php?id=104206
[+] Downloading file - [364133 bytes] https://learn.ztu.edu.ua/mod/resource/view.php?id=84886
[+] Downloading file - [1810801 bytes] https://learn.ztu.edu.ua/mod/resource/view.php?id=84296
```

Рисунок 3.12 – Процес пошуку та завантаження документів

Як ми можемо побачити, пошук документів у домені веб-сайту було здійснено успішно. Результати пошуку показано на рисунку 3.13.

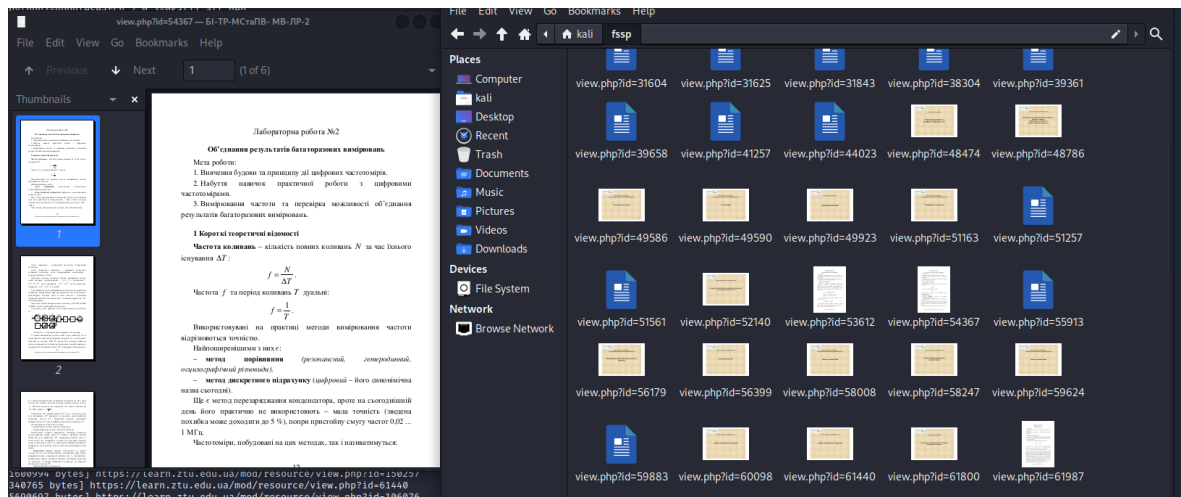


Рисунок 3.13 – Результати пошуку

Ми отримали певну вибірку даних, які ми можемо проаналізувати на наявність корисних метаданих. Для цього скористаємося вбудованою у Kali Linux програмою «Exiftool». Дане програмне забезпечення має мету визначити всі метадані документів. За допомогою команди «egrep» встановимо список тегів які нас цікавлять та відсортуємо їх.

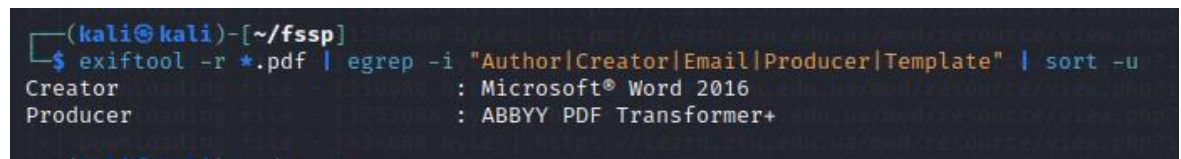


Рисунок 3.14 – Результат перегляду метаданих документів

Отже, ми не знайшли жодної корисної інформації у метаданих раніше завантажених документів. Дана невдача може бути пов'язана з правильно налагодженим фільтром метаданих документів на вебсайті. Останній факт свідчить про гарний рівень захищеності веб-застосунку та персональних даних його користувачів.

Оберемо інший сайт та спробуємо ще раз.

Для наступного пошуку оберемо веб сайт «zrazki-documentiv.com.ua». Даний веб-сайт містить базу актуальних юридичних документів, які можна у подальшому завантажити. Спробуємо віднайти та завантажити документи з типом «doc».

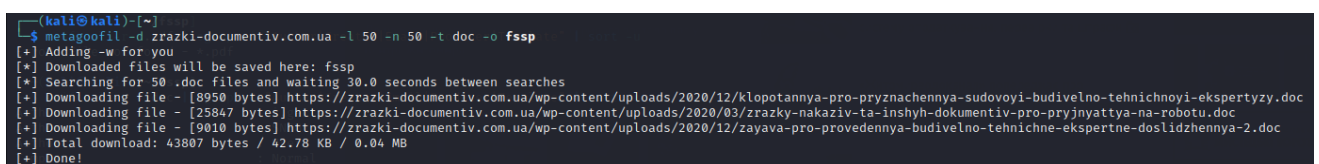


Рисунок 3.15 – Процес пошуку та завантаження файлів з домену «zt.20minut.ua».

		Герасимчук В.В.			ККІКБ.КР.Б – 125 – 23 – ПЗ	Арк.
		Байлюк Є.М.				58
Змн.	Арк.	№ докум.	Підпис	Дата		

Програмний застосунок віднайшов декілька документів. Пробуємо проаналізувати метадані даних документів.

```
(kali@kali)-[~/fssp]
$ exiftool -r *.doc | egrep -i "Author|Creator|Email|Producer|Template" | sort -u
Author          : i.gerts
Author          : SNEU
Author          : User
Template        : Normal
```

Рисунок 3.16 – Знайдені метадані.

Даний пошук увінчався успіхом, адже ми знайшли інформацію про трох авторів даних документів. Це свідчить про те, що є доцільним здійснити більш детальний аналіз метаданих даних документів. Оскільки кількість документів досить невелика, то немає сенсу автоматизувати даний процес, тому розглянемо кожен документ окремо.

```
==== zayava-pro-provedennya-budivselno-tehnicne-ekspertne-doslidzhennya-2.doc
ExifTool Version Number      : 12.55
File Name                    : zayava-pro-provedennya-budivselno-tehnicne-ekspertne-doslidzhennya-2.doc
Directory                    : .
File Size                     : 36 kB
File Modification Date/Time   : 2023:02:05 12:23:58-05:00
File Access Date/Time        : 2023:02:05 12:24:20-05:00
File Inode Change Date/Time   : 2023:02:05 12:23:58-05:00
File Permissions              : -rw-r--r--
File Type                    : DOC
File Type Extension          : doc
MIME Type                    : application/msword
Identification                : Word 8.0
Language Code                 : Russian
Doc Flags                     : Has picture, 1Table, ExtChar
System                       : Windows
Word 97                       : No
Title                        : BAT «Український
Subject                       :
Author                        : SNEU
Keywords                      :
Comments                      :
Template                      : Normal
Last Modified By              : Сергей
Software                      : Microsoft Office Word
Create Date                   : 2020:04:30 15:10:00
Modify Date                   : 2020:12:04 16:34:00
Security                      : None
Company                       : SPecialIST RePack
Char Count With Spaces        : 2032
App Version                   : 15.0000
Scale Crop                    : No
Links Up To Date              : No
Shared Doc                    : No
Hyperlinks Changed            : No
Title Of Parts                 : BAT «Український
Heading Pairs                 : Название, 1
Code Page                     : Windows Cyrillic
Hyperlinks                    : mailto:lubazaria@gmail.com
FLIR DOCUMENT ID              : e5277648-d784-4dde-93e3-5ffa7076c190
Comp Obj User Type Len        : 32
Comp Obj User Type            : ***** Microsoft Word 97-2003
Last Printed                   : 2018:11:21 11:52:00
Revision Number               : 3
Total Edit Time                : 0
Words                         : 303
Characters                    : 1733
Pages                         : 1
Paragraphs                    : 4
Lines                         : 14
```

Рисунок 3.17 – Детальна інформація по метаданих одного з файлів.

Розглянемо інформацію наведену на рисунку 3.14. Ми встановили користувача, який створив даний документ (Author), встановили назву компанії (Company), посилання на електронну пошту (Hyperlinks), програмне забезпечення за допомогою якого файл було створено (Comp Obj User Type) та час останнього друку (Last Printed).

		Герасимчук В.В.			ККІКБ.КР.Б – 125 – 23 – ПЗ	Арк.
		Байлюк Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		59

Особливою важливою деталлю варто зауважити мітку назви компанії. Назва компанії «SPeCialiST RePack» свідчить про те, що автор файлу використовував модифіковане програмне забезпечення, яке, скоріше за все, не було активоване і є піратським. Даний факт дозволяє притягнути автора статті до відповідальності за використання неліцензійного програмного забезпечення.

3.4. Рекомендації щодо використання OSINT.

Наведені рекомендації допоможуть здійснювати більш детальне та комплексне дослідження кіберінцидентів, забезпечуючи необхідну інформацію для ідентифікації злочинців, їхніх методів дії та можливих заходів для запобігання подібним інцидентам у майбутньому.

Першою рекомендацією є встановлення загального контексту шляхом використання OSINT для отримання всебічної інформації щодо інциденту. Важливо здійснити пошук новин, публікацій в соціальних мережах, форумах та інших джерелах, які можуть містити відповідну інформацію про цю подію. Цей підхід допоможе з'ясувати, що саме сталося, а також виявити осіб, які можуть бути зацікавлені в таких діях.

Шляхом ознайомлення з новинними звітами та медійними публікаціями можна отримати початкову інформацію про кіберінцидент. Крім того, соціальні мережі та форуми можуть надати додаткові відомості, які допоможуть з'ясувати важливі деталі події. Цей процес дозволить отримати ширший огляд ситуації та зрозуміти, хто може бути зацікавлений у таких діях. Використання OSINT для отримання загального контексту інциденту є важливою складовою розслідування. Шляхом аналізування різних джерел інформації, ви зможете скласти повнішу картину того, що відбулося, та ідентифікувати можливих зацікавлених сторін.

Другою рекомендацією є збір даних про загрози. Використання OSINT дозволяє отримати доступ до джерел, що надають важливу інформацію про потенційні загрози. Досліджуючи бази даних та інші джерела, пов'язані з безпекою, ви зможете зібрати дані про вразливості програмного забезпечення, які можуть

		Герасимчук В.В.			ККІКБ.КР.Б – 125 – 23 – ПЗ	Арк.
		Байлюк Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		60

бути використані зловмисниками. Крім того, ці джерела надають інформацію про відомі хакерські групи, їхні методи атак та інші важливі відомості.

Цей процес збору даних дозволяє вам отримати об'єктивну інформацію про потенційні загрози, що можуть бути пов'язані з кіберінцидентом. Це допоможе вам краще розуміти характер атаки, виявити можливі вразливості та вжити відповідних заходів безпеки для запобігання подібним інцидентам у майбутньому.

Ще однією порадою є використання інструментів і технологій. За допомогою автоматизованих інструментів OSINT можна швидко та ефективно сканувати великі обсяги даних з різних джерел. Це дозволяє прискорити процес збору інформації і зменшити ручну працю. Автоматизовані інструменти можуть сканувати веб-сайти, соціальні мережі, форуми, бази даних та інші джерела на предмет наявності специфічної інформації, такої як електронні адреси, імена користувачів, домени тощо. Також інструменти та технології OSINT можуть надати можливість аналізувати та візуалізувати зібрану інформацію для отримання корисних інсайтів. Наприклад, графічні інструменти можуть допомогти візуалізувати зв'язки між різними суб'єктами або встановити залежності між доменами, IP-адресами та іншими елементами інфраструктури.

Використання інструментів і технологій OSINT дозволяє ефективно збирати, аналізувати та використовувати великі обсяги відкритої інформації. Важливо добре ознайомитися з цими інструментами, їх функціональністю та можливостями, щоб максимально використовувати їх потенціал під час розслідування кіберінцидентів.

Також оновлення та перевірка інформації є надзвичайно важливим етапом в процесі використання OSINT під час розслідування кіберінцидентів, адже зібрана інформація є динамічною і може змінюватися з часом. Необхідно періодично повертатися до зібраної інформації та оновлювати її, перевіряючи актуальність та точність даних. Також у разі використання автоматизованих інструментів для збору інформації, необхідно переконатися, що вони працюють належним чином і оновлюються. Відстежуйте оновлення і випуски нових версій програмного забезпечення, оскільки це може включати покращення або нові можливості.

		Герасимчук В.В.			ККІКБ.КР.Б – 125 – 23 – ПЗ	Арк.
		Байлюк Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		61

Оновлення та перевірка інформації є важливими компонентами процесу розслідування кіберінцидентів. Це дозволяє підтримувати актуальність даних і забезпечувати, що ваша аналітична робота базується на надійній та точній інформації.

3.5. Перспективи подальших досліджень.

Дослідження кіберінцидентів за допомогою методів OSINT мають значний потенціал для подальших досліджень і вдосконалення. Адже подальше вдосконалення алгоритмів пошуку може допомогти знаходити більш точні та релевантні джерела інформації. Це може включати використання інтелектуальних методів пошуку, які враховують контекст, семантику та інші фактори для покращення результатів. Також розвиток нових методів аналізу даних може сприяти виявленню складних зв'язків та закономірностей між різними джерелами інформації з подальшою кластеризацією даних, виявленням аномалій та побудовою звітів. Це може включати застосування методів машинного навчання, статистичного аналізу та візуалізації даних для отримання більш глибокого розуміння зібраної інформації.

Штучний інтелект (ШІ) та машинне навчання (МН) мають потенціал великої цінності для подальших досліджень розслідування кіберінцидентів з використанням методів OSINT. Використання ШІ та МН може привести до наступних розвитку:

Автоматизація процесу розпізнавання та класифікації інформації: ШІ та МН можуть бути використані для створення моделей, які автоматично розпізнають та класифікують інформацію з різних джерел. Це може допомогти відокремити значущу інформацію від незначної та прискорити процес аналізу.

Персоналізовані рекомендації та прогнозування: Застосування ШІ та МН може допомогти створити моделі, які здатні аналізувати інформацію про конкретні цілі та прогнозувати їхні дії. Це може бути корисно при розслідуванні кіберінцидентів, де важливо передбачити наступні кроки злоумисників.

		Герасимчук В.В.			ККІКБ.КР.Б – 125 – 23 – ПЗ	Арк.
		Байлюк Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		62

Виявлення аномалій та патернів: ІІІ та МН можуть допомогти виявити аномалії та незвичайні патерни в поведінці користувачів, доменів або мереж. Це може допомогти виявити потенційні загрози та ідентифікувати небезпечні або компрометовані ресурси.

Використання штучного інтелекту і машинного навчання в розслідуванні кіберінцидентів з використанням методів OSINT може привести до нових можливостей та покращити точність та ефективність розслідування.

Висновки до третього розділу

У рамках даного розділу були застосовані різні методи та інструменти, які дозволили зібрати важливу інформацію та отримати цінні висновки. Зокрема, використання спеціалізованого програмного забезпечення дозволило провести ефективний збір інформації про домен, виявити його вихідне джерело та отримати важливі дані для подальшого аналізу. Аналіз веб-сайту за допомогою метаданих контенту також дав змогу здобути додаткову інформацію про веб-ресурс та виявити можливі загрози.

Узагальнюючи, використання методів OSINT в розслідуванні кіберінцидентів є потужним інструментом, що дозволяє збирати, аналізувати та оновлювати важливу інформацію. Правильне використання цих методів та технологій може сприяти виявленню загроз, ідентифікації зловмисників та покращенню заходів безпеки.

		Герасимчук В.В.			ККІКБ.КР.Б – 125 – 23 – ПЗ	Арк.
		Байлюк Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		63

ВИСНОВКИ

Отже, використання методів OSINT є надзвичайно важливим при розслідуванні кіберінцидентів. Ці методи дозволяють зібрати велику кількість інформації про потенційних злочинців, їхні мотиви та дії, що значно полегшує подальший процес розслідування.

При цьому, дослідження показали, що успішність використання методів OSINT залежить від якості зібраної інформації та її обробки. Для забезпечення якісного збору інформації слід використовувати різноманітні джерела, включаючи веб-сайти, соціальні мережі, форуми, блоги тощо, а також спеціалізовані інструменти для автоматизації збору інформації.

У першому розділі було розглянуто поняття та визначення OSINT, основні принципи та правила використання OSINT, порівняння методів розслідування кіберінцидентів, нормативно-правові аспекти використання OSINT та міжнародний досвід використання OSINT.

Основна ідея OSINT полягає у зборі та аналізі відкритої інформації з метою вирішення різних завдань. Використання OSINT може бути дуже корисним в дослідженні кіберінцидентів, адже це може допомогти виявити причину та знайти зловмисників.

У другому розділі ми розглянули методологію дослідження кіберінцидентів за допомогою методів OSINT та декілька програмних засобів, які можуть бути використані для здійснення такого дослідження.

Методологія дослідження кіберінцидентів за допомогою методів OSINT передбачає збір та аналіз відкритих даних з різних джерел, таких як соціальні мережі, форуми, блоги, новинні сайти та інші. Такий аналіз може допомогти виявити злочинців, з'ясувати мотиви їх дій та забезпечити підстави для подальшого юридичного переслідування.

У третього розділу були застосовані різні методи та інструменти, які дозволили зібрати важливу інформацію та отримати цінні висновки. Зокрема, використання спеціалізованого програмного забезпечення дозволило провести ефективний збір інформації про домен, виявити його вихідне джерело та отримати

		Герасимчук В.В.			ККІКБ.КР.Б – 125 – 23 – ПЗ	Арк.
		Байлюк Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		64

важливі дані для подальшого аналізу. Аналіз веб-сайту за допомогою метаданих контенту також дав змогу здобути додаткову інформацію про веб-ресурс та виявити можливі загрози.

Узагальнюючи, використання методів OSINT у розслідуванні кіберінцидентів є потужним інструментом, що дозволяє збирати, аналізувати та оновлювати важливу інформацію. Правильне використання цих методів та технологій може сприяти виявленню загроз, ідентифікації зловмисників та покращенню заходів безпеки.

		Герасимчук В.В.			ККІКБ.КР.Б – 125 – 23 – ПЗ	Арк.
		Байлюк Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		65

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Cyberforensics: збір та дослідження цифрових доказів [Електронний ресурс] – Режим доступу до ресурсу: <https://yur-gazeta.com/publications/practice/informaciyne-pravo-telekomunikaciyi/cyberforensics-zbir-ta-doslidzhennya-cifrovih-dokaziv.html>.
2. Розвідка на основі відкритих джерел [Електронний ресурс] – Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/%D0%A0%D0%BE%D0%B7%D0%B2%D1%96%D0%B4%D0%BA%D0%B0_%D0%BD%D0%B0_%D0%BE%D1%81%D0%BD%D0%BE%D0%B2%D1%96_%D0%B2%D1%96%D0%B4%D0%BA%D1%80%D0%B8%D1%82%D0%B8%D1%85_%D0%B4%D0%B6%D0%B5%D1%80%D0%B5%D0%BB.
3. Molfar про OSINT [Електронний ресурс] – Режим доступу до ресурсу: https://t.me/molfar_global.
4. Open-Source Intelligence (OSINT) Use by Governments [Електронний ресурс] – Режим доступу до ресурсу: <https://hackernoon.com/open-source-intelligence-osint-use-by-governments-802t37gn>.
5. Про основні засади забезпечення кібербезпеки України [Електронний ресурс] – Режим доступу до ресурсу: <https://ips.ligazakon.net/document/T172163>.
6. Кримінальний кодекс України [Електронний ресурс] – Режим доступу до ресурсу: <https://zakon.rada.gov.ua/laws/show/2341-14>.
7. Конституція України [Електронний ресурс] – Режим доступу до ресурсу: <https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80>.
8. Цивільний кодекс України [Електронний ресурс] – Режим доступу до ресурсу: <https://zakon.rada.gov.ua/laws/show/435-15>.
9. Types of Cyber Attacks You Should Be Aware of in 2023 [Електронний ресурс] – Режим доступу до ресурсу: <https://www.simplilearn.com/tutorials/cyber-security-tutorial/types-of-cyber-attacks>.
10. How to Investigate a Cyber Incident: 5-Step Guide [Електронний ресурс] – Режим доступу до ресурсу: <https://www.itgovernance.co.uk/blog/how-to-investigate-a-cyber-incident-5-step-guide>.

		Герасимчук В.В.			ККІКБ.КР.Б – 125 – 23 – ПЗ	Арк.
		Байлюк Є.М.				66
Змн.	Арк.	№ докум.	Підпис	Дата		

11. ХАРАКТЕРИСТИКА ПРИНЦИПІВ ФУНКЦІОНУВАННЯ OSINT У СФЕРІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ [Електронний ресурс] – Режим доступу до ресурсу: http://www.lsej.org.ua/9_2021/85.pdf.

12. Про захист осіб у зв'язку з автоматичною обробкою персональних даних : Конвенція Ради Європи від 28 січня 1981 р. № 108. Офіційний вісник України. 2011. № 1. С. 701.

13. NATO Open Source Intelligence Reader (2002). // <http://information-retrieval.info/docs/NATO-OSINT.html>.

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

15. 2020 FIREEYE BREACH [Електронний ресурс] – Режим доступу до ресурсу: <https://www.whiteblueocean.com/newsroom/2020-fireeye-breach/>.

16. New Cyberattack by Group Behind TRITON/TRISIS Reported [Електронний ресурс] – Режим доступу до ресурсу: <https://www.powermag.com/new-cyberattack-by-group-behind-triton-trisis-reported/>.

17. maltego | Kali Linux Tools [Електронний ресурс] – Режим доступу до ресурсу: <https://www.kali.org/tools/maltego/>.

18. How To Use Maltego With Kali Linux [Електронний ресурс] – Режим доступу до ресурсу: <https://linuxhint.com/how-to-use-maltego-with-kali-linux/>.

19. What Is Shodan? How to Use It & How to Stay Protected [2023] [Електронний ресурс] – Режим доступу до ресурсу: <https://www.safetynetec-tives.com/blog/what-is-shodan-and-how-to-use-it-most-effectively/>.

20. recon-ng | Kali Linux Tools [Електронний ресурс] – Режим доступу до ресурсу: <https://www.kali.org/tools/recon-ng/>.

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

22. theharvester | Kali Linux Tools [Електронний ресурс] – Режим доступу до ресурсу: <https://www.kali.org/tools/theharvester/>.

		Герасимчук В.В.			ККІКБ.КР.Б – 125 – 23 – ПЗ	Арк.
		Байлюк Є.М.				67
Змн.	Арк.	№ докум.	Підпис	Дата		

23. how to use theharvester an email harvesting tool in Kali Linux 2022 [Електронний ресурс] – Режим доступу до ресурсу: <https://www.cyberprati-bha.com/blog/kali-linux-theharvester-an-email-harvester/>.

24. metagoofil | Kali Linux Tools [Електронний ресурс] – Режим доступу до ресурсу: <https://www.kali.org/tools/metagoofil/>.

25. Metagoofil Tool Documentation [Електронний ресурс] – Режим доступу до ресурсу: <https://www.kali.org/tools/metagoofil/>.

26. Holehe OSINT - Email to Registered Accounts [Електронний ресурс] – Режим доступу до ресурсу: <https://github.com/megadose/holehe>.

27. OSINT - Maltego [Електронний ресурс] – Режим доступу до ресурсу: <https://www.maltego.com/categories/osint/>.

28. OPEN SOURCE INTELLIGENCE TOOLS AND RESOURCES HANDBOOK 2020 [Електронний ресурс] / Aleksandra Bielska, Noa Rebecca Kurz, Yves Baumgartner, Vytenis Benetis. – 2020. – Режим доступу до ресурсу: https://intelligence.eu/uploads/public-documents/OSINT_Handbook_2020.pdf.

29. AaronCTI's OSINT Resource Collection [Електронний ресурс] – Режим доступу до ресурсу: <https://docs.google.com/spreadsheets/d/1klugQqw6POlBtuzon8S0b18-gpsDwX-5OYRrB7TyNEw/edit#gid=0>

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

		Герасимчук В.В.			ККІКБ.КР.Б – 125 – 23 – ПЗ	Арк.
		Байлюк Є.М.				68
Змн.	Арк.	№ докум.	Підпис	Дата		