Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя
(повне найменування вищого навчального закладу)
Факультет комп'ютерно-інформаційних систем і програмної інженерії
(назва факультету)
Кафедра кібербезпеки
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

бакалавр
(освітній рівень)

на тему: "Оцінка можливостей OSINT для виявлення та реагування на кіберзагрози"

Виконав: студент (ка)
Спеціальності:
125 «Кібербезпека»
(шифр і назва напряму підготовки, спеціальності)
Містерман Іван Михайлович
підпис (прізвище та ініціали)

Керівник Стадник М.А.
підпис (прізвище та ініціали)

Нормоконтроль Тимощук Д.І.
підпис (прізвище та ініціали)

Завідувач кафедри Загородна Н.В.
підпис (прізвище та ініціали)

Рецензент
підпис (прізвище та ініціали)

м. Тернопіль – 2024

Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)

Кафедра кібербезпеки
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Загородна Н.В.
(підпис) (прізвище та ініціали)
«__» _____ 2024 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня Бакалавр
(назва освітнього ступеня)

за спеціальністю 125 Кібербезпека
(шифр і назва спеціальності)

Студенту Містерман Івану Михайловичу
(прізвище, ім'я, по батькові)

1. Тема роботи Оцінка можливостей OSINT для виявлення та реагування на кіберзагрози

Керівник роботи Стадник Марія Андріївна, кандидат технічних наук, доцент кафедри КБ
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від «03» 04 2024 року № 4/7-349

2. Термін подання студентом завершеної роботи 14.06.2024

3. Вихідні дані до роботи Дослідження відкритих джерел інформації, аналіз кіберзагроз та застосування технологій OSINT

4. Зміст роботи (перелік питань, які потрібно розробити)
Проаналізувати значущість та методологію використання OSINT у кібербезпеці.
Проаналізувати основи та інструменти OSINT у сучасній кібербезпеці.
Розробити та протестувати методику проведення OSINT-досліджень, включаючи реальні
Приклади виявлення кіберзагроз, аналіз ефективності використання OSINT та стратегії реагування на кіберзагрози.
Проаналізувати правові та етичні аспекти використання OSINT, включаючи законодавчі обмеження, етичні питання та випадки порушення прав і конфіденційності.
Безпека життєдіяльності, основи охорони праці
Висновки

5. Перелік графічного матеріалу
Теоретичні основи OSINT. Роль OSINT у виявленні кіберзагроз. Інструменти OSINT.
Методика проведення OSINT-досліджень. Реагування на кіберзагрози зи допомогою OSINT.
Приклади використання OSINT. Приклад як за допомогою Shodan виявити вразливість пристрою. Приклад використання Maltego для виявлення вразливості електронного ресурсу.
Спам листів на електронну пошту. Правові та етичні аспекти OSINT. Висновки.

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Безпека життєдіяльності, основи хорони праці			

7. Дата видачі завдання 29.01.2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1.	Ознайомлення з завданням до кваліфікаційної роботи	16.02 – 19.02	Виконано
2.	Підбір джерел для аналізу OSINT в сучасній кібербезпеці	20.02 – 27.02	Виконано
3.	Опрацювання джерел в галузі дослідження	28.02 – 16.03	Виконано
4.	Провести аналіз інструментів які використовуються в OSINT	22.02 – 12.03	Виконано
5.	Здійснення пошуку інформації про сайт gazeta.uz з допомогою інструмента Maltego	15.03-25.03	Виконано
6.	Перевірка на вразливіть відеокамери за допомогою інструмента Shodan	25.02 – 10.04	Виконано
7.	Оформлення розділу «Значущість та методологія використання OSINT у кібербезпеці»	10.02 – 05.03	Виконано
8.	Оформлення розділу «Основи та інструменти OSINT в сучасній кібербезпеці»	26.03 – 04.05	Виконано
9.	Оформлення розділу «Практичне застосування OSINT: методики, ефективність та етичні аспекти»	12.04-20.04	
10.	Виконання завдання до підрозділу «Безпека життєдіяльності, основи охорони праці»	14.05 – 21.05	Виконано
11.	Оформлення кваліфікаційної роботи	22.05 – 05.06	Виконано
12.	Нормоконтроль	06.06 – 12.06	Виконано
13.	Перевірка на плагіат	10.06 – 16.06	Виконано
14.	Попередній захист кваліфікаційної роботи	18.06 – 21.06	Виконано
15.	Захист кваліфікаційної роботи	25.06.2024	

Студент _____ Містерман І.М.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Стадник М.А.
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Оцінка можливостей OSINT для виявлення та реагування на кіберзагрози // Кваліфікаційна робота ОР «Бакалавр» // Містерман Іван Михайлович // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра кібербезпеки, група СБ-41 // Тернопіль, 2024 // С. 75 , рис. – 24, табл. – 0, кресл. – 0, додат. – 0.

КЛЮЧОВІ СЛОВА: Open Source Intelligence (OSINT), кіберзагрози, виявлення загроз, реагування на загрози, кібербезпека, інструменти OSINT.

Дана кваліфікаційна робота присвячена дослідженню можливостей Open Source Intelligence (OSINT) для виявлення та реагування на кіберзагрози.

Метою роботи є аналіз ефективності та можливостей інструментів OSINT, таких як: Shodan та Maltego у контексті виявлення та реагування на кіберзагрози.

Практична частина роботи містить методику проведення OSINT-досліджень та аналіз реальних випадків виявлення кіберзагроз з використанням відкритих джерел. Розглянуто стратегії реагування на виявлені загрози та приклади успішного використання OSINT у запобіганні кіберінцидентам.

Також досліджено правові та етичні аспекти використання OSINT, включаючи законодавчі обмеження та етичні питання у зборі та аналізі відкритих даних.

Результати дослідження підтверджують, що OSINT є ефективним інструментом для виявлення та реагування на кіберзагрози, а також надають рекомендації щодо покращення методів використання відкритих джерел інформації у сфері кібербезпеки.

ANNOTATION

Evaluation of OSINT capabilities for detecting and responding to cyber threats // Qualification work for bachelor's degree // Miisterman Ivan Mykhailovych // Ternopil National Technical University named after Ivan Puluj, Faculty of Computer Information Systems and Software Engineering, Department of Cybersecurity, group SB-41 // Ternopil, 2024 // P. 75, fig. – 24, tables – 0, drawings – 0, supplement – 0.

KEYWORDS: Open Source Intelligence (OSINT), cyber threats, threat detection, threat response, cybersecurity, OSINT tools.

This qualification work is devoted to the study of the capabilities of Open Source Intelligence (OSINT) for detecting and responding to cyber threats.

The aim of the work is to analyze the effectiveness and capabilities of OSINT tools, such as: Shodan and Maltego in the context of detecting and responding to cyber threats.

The practical part of the work contains a methodology for conducting OSINT research and analysis of real cases of cyber threat detection using open sources. Strategies for responding to identified threats and examples of successful use of OSINT in preventing cyber incidents are considered.

The legal and ethical aspects of using OSINT, including legal restrictions and ethical issues in collecting and analyzing open data, are also investigated.

The results of the study confirm that OSINT is an effective tool for detecting and responding to cyber threats, and provide recommendations for improving the methods of using open sources of information in the field of cybersecurity.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

OSINT – Open Source Intelligence (розвідка на основі відкритих джерел інформації)

Malware – Шкідливе програмне забезпечення

DDoS – Distributed Denial of Service

IDS – Системи виявлення вторгнень

IPS – Системи запобігання вторгнень

ВСТУП

Сучасне інформаційне суспільство стрімко розвивається, що приносить не лише нові можливості, а й нові виклики. Одним із найактуальніших викликів сьогодення є кіберзагрози, які можуть завдати значних збитків як окремим особам, так і організаціям та державам. З огляду на це, забезпечення кібербезпеки стає пріоритетним завданням для багатьох країн, компаній і приватних користувачів. У цьому контексті особливої уваги заслуговує розвідка на основі відкритих джерел інформації (OSINT).

OSINT, або Open Source Intelligence, є методикою збору та аналізу інформації з відкритих джерел, таких як інтернет-ресурси, соціальні медіа, наукові публікації, форуми та інші доступні для загалу дані. Використання OSINT дозволяє отримувати цінну інформацію без необхідності проникнення в закриті або захищені інформаційні системи, що робить цей підхід особливо привабливим у контексті кібербезпеки.

Зростання кількості кіберзагроз, таких як фішинг, шкідливе програмне забезпечення, атаки на веб-додатки та інші види кіберзлочинів, вимагає нових підходів до їх виявлення та реагування. Традиційні методи захисту часто виявляються недостатніми, що спонукає до пошуку нових рішень і технологій. У цьому контексті OSINT виступає як ефективний інструмент, здатний доповнити існуючі системи кібербезпеки та забезпечити вчасне виявлення загроз.

Мета даної кваліфікаційної роботи полягає у всебічному аналізі можливостей OSINT для виявлення та реагування на кіберзагрози. У процесі дослідження будуть розглянуті теоретичні основи OSINT, його історичний розвиток та класифікація джерел відкритої інформації. Особливу увагу буде приділено класифікації кіберзагроз та методам їх виявлення за допомогою OSINT, а також огляду основних інструментів і платформ, які використовуються для збору та аналізу відкритих даних.

Практична частина роботи спрямована на демонстрацію методик проведення OSINT-досліджень та аналіз реальних випадків виявлення кіберзагроз за допомогою відкритих джерел. Будуть розглянуті стратегії реагування на виявлені загрози, а також приклади успішного використання OSINT у запобіганні кіберінцидентам. Крім того, буде досліджено правові та етичні аспекти використання OSINT, включаючи законодавчі обмеження та моральні питання, пов'язані зі збором та аналізом відкритих даних.

Важливим аспектом дослідження є визначення ефективності OSINT у виявленні та реагуванні на кіберзагрози, а також розробка рекомендацій щодо покращення методів використання відкритих джерел інформації у сфері кібербезпеки. У підсумку, результати дослідження мають продемонструвати, що OSINT є потужним інструментом, який може значно підвищити рівень захисту інформаційних систем та сприяти зменшенню ризиків, пов'язаних з кіберзагрозами.

З огляду на вищезазначене, дана кваліфікаційна робота не лише актуальна, але й має вагоме практичне значення. Її результати можуть бути корисними як для фахівців у галузі кібербезпеки, так і для широкого кола користувачів, які прагнуть захистити свої інформаційні ресурси від потенційних загроз. Робота спрямована на розширення знань про OSINT та його застосування у сфері кібербезпеки, що сприятиме розвитку ефективних стратегій боротьби з кіберзагрозами у сучасному інформаційному суспільстві.

1 ЗНАЧУЩІСТЬ ТА МЕТОДОЛОГІЯ ВИКОРИСТАННЯ OSINT У КІБЕРБЕЗПЕЦІ

1.1 Актуальність теми

Сучасний розвиток інформаційних технологій значно розширив можливості для бізнесу, державного управління та особистого спілкування. Однак, разом із цим зростає і кількість кіберзагроз, які можуть завдати серйозної шкоди інформаційним системам, даним і репутації. Кіберзлочини стають дедалі витонченішими, що вимагає від фахівців з кібербезпеки нових підходів і методів для виявлення та нейтралізації цих загроз.

1.1.1 Актуальність використання OSINT

Одним із найбільш перспективних методів у боротьбі з кіберзагрозами є використання розвідки на основі відкритих джерел інформації (OSINT). OSINT дозволяє отримувати важливі дані з відкритих джерел, таких як інтернет, соціальні медіа, форуми, публікації та інші доступні ресурси, що можуть містити інформацію про потенційні загрози та вразливості.

Використання OSINT стає особливо актуальним у контексті зростання кількості атак на інформаційні системи. За даними звітів провідних компаній з кібербезпеки, кількість кіберінцидентів щорічно збільшується, що підтверджує необхідність впровадження нових технологій для їх виявлення та запобігання. Наприклад, згідно зі звітом Symantec, лише у 2023 році кількість атак зросла на 18% порівняно з попереднім роком [1].

1.1.2 Переваги OSINT

OSINT має кілька вагомих переваг перед традиційними методами кіберрозвідки. По-перше, це доступність даних, оскільки вони знаходяться у відкритому доступі і не вимагають спеціальних дозволів для їх отримання. По-друге, OSINT дозволяє отримувати актуальну інформацію в режимі реального часу, що є критично важливим для своєчасного виявлення та реагування на загрози. По-третє, цей метод є економічно вигідним, оскільки не потребує великих фінансових витрат на розвідувальні операції [2].

1.1.3 Зростання важливості кібербезпеки

Загалом, кібербезпека стає ключовим елементом захисту інформаційних ресурсів у сучасному світі. Згідно зі звітом Міжнародного союзу електрозв'язку, у 2023 році обсяг глобальних витрат на кібербезпеку сягнув 150 мільярдів доларів США, що свідчить про високу пріоритетність цієї сфери [3]. Інвестування у нові технології та методи, такі як OSINT, стає невід'ємною частиною стратегій кібербезпеки багатьох організацій.

1.2 Мета та завдання дослідження

Метою даного дослідження є всебічний аналіз можливостей використання OSINT для виявлення та реагування на кіберзагрози. Зважаючи на зростання кількості та складності кіберзагроз, важливо визначити, як саме OSINT може допомогти в їх своєчасному виявленні та ефективному реагуванні.

Для досягнення поставленої мети були визначені наступні завдання:

1) Дослідити теоретичні основи та історичний розвиток OSINT.
2) Класифікувати джерела відкритої інформації, що використовуються в OSINT.

3) Вивчити основні види кіберзагроз та методи їх виявлення.
4) Провести огляд інструментів та платформ OSINT, які застосовуються для збору та аналізу даних.
5) Розробити методику проведення OSINT-досліджень.
6) Проаналізувати реальні випадки виявлення кіберзагроз за допомогою OSINT.
7) Оцінити ефективність використання OSINT у реагуванні на кіберзагрози.
8) Дослідити правові та етичні аспекти використання OSINT у контексті кібербезпеки [35].
9) Надати рекомендації щодо покращення методів використання відкритих джерел інформації у сфері кібербезпеки.

Результати даного дослідження мають сприяти глибшому розумінню ролі OSINT у забезпеченні кібербезпеки та допомогти у формуванні ефективних стратегій боротьби з кіберзагрозами.

1.3 Опис об'єкта дослідження: кіберзагрози та методи їх виявлення

Кіберзагрози являють собою сукупність дій або подій, що можуть призвести до порушення конфіденційності, цілісності або доступності інформаційних систем та даних. Серед основних видів кіберзагроз можна виділити наступні:

1) Шкідливе програмне забезпечення (Malware) – програми або коди, створені з метою пошкодження, порушення або несанкціонованого доступу до комп'ютерних систем. Види Malware включають віруси, троянські програми, черв’яки, шпигунське програмне забезпечення та програми-вимагачі [2].
2) Фішинг – метод соціальної інженерії, який використовується для викрадення конфіденційної інформації, такої як логіни, паролі та фінансові дані, через обманні електронні листи або веб-сайти.

Фішинг може бути спрямований як на окремих користувачів, так і на організації [1].

3) Атаки на веб-додатки – включають SQL-ін'єкції, Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF) та інші вразливості, що використовуються для компрометації веб-додатків та отримання несанкціонованого доступу до даних [4].
4) DDoS-атаки (Distributed Denial of Service) – атаки, спрямовані на перевантаження мережевих ресурсів з метою виведення їх з ладу. Це досягається шляхом одночасного надсилання великої кількості запитів з різних джерел [5].
5) Інсайдерські загрози – дії співробітників або інших осіб, які мають доступ до внутрішніх систем компанії та використовують цей доступ для здійснення шкідливих дій. Інсайдерські загрози можуть бути як навмисними, так і ненавмисними [6].

Для ефективного виявлення кіберзагроз використовуються різноманітні методи та інструменти, які дозволяють своєчасно виявляти та реагувати на потенційні атаки. Основні методи включають:

1) Системи виявлення вторгнень (IDS) – програмне або апаратне забезпечення, що моніторить мережевий трафік та системні дії для виявлення підозрілих або шкідливих активностей. IDS можуть бути мережевими (NIDS) або хостовими (HIDS) [7].
2) Системи запобігання вторгнень (IPS) – розширення функціональності IDS, що не лише виявляють, але й блокують виявлені загрози в режимі реального часу [8].
3) Антивірусне програмне забезпечення – програми, що здійснюють сканування, виявлення та видалення шкідливих програм. Сучасні антивірусні рішення використовують як сигнатурний аналіз, так і евристичні методи для виявлення нових видів шкідливого ПЗ [1].
4) Аналіз логів – методика аналізу журналів подій, згенерованих різними компонентами інформаційних систем, для виявлення

аномальних або підозрілих активностей. Інструменти аналізу логів можуть автоматично визначати шаблони, що вказують на можливі загрози [9].

5) Технології машинного навчання та штучного інтелекту (AI/ML) – використання алгоритмів AI/ML для аналізу великих обсягів даних з метою виявлення аномалій та нових загроз, що не піддаються виявленню традиційними методами [6].
6) OSINT – методика збору та аналізу інформації з відкритих джерел для виявлення потенційних загроз та вразливостей. OSINT дозволяє отримувати дані про можливі атаки ще до їх здійснення, що робить цей підхід особливо цінним для проактивного захисту [2].

Загалом, ефективна кібербезпека вимагає комплексного підходу, що включає використання різноманітних методів виявлення загроз, їх аналізу та реагування на них. У цьому контексті OSINT є важливим інструментом, що доповнює традиційні методи кіберзахисту та забезпечує додатковий рівень безпеки.

1.4 Предмет дослідження: можливості OSINT для виявлення та реагування на кіберзагрози

OSINT (Open Source Intelligence) є потужним інструментом для виявлення кіберзагроз завдяки своїй здатності використовувати відкриті джерела інформації. Основна перевага OSINT полягає в доступності великого обсягу даних, які можуть бути проаналізовані для виявлення потенційних загроз ще до їх реалізації.

1) Моніторинг соціальних медіа**.** Соціальні медіа є багатим джерелом інформації, оскільки кіберзлочинці часто використовують ці платформи для координації своїх дій або обговорення вразливостей. Аналіз соціальних медіа може допомогти виявити потенційні атаки на ранніх стадіях.

2) Аналіз форумів і даркнету. Форумами часто користуються зловмисники для обміну знаннями та продажу викрадених даних або шкідливого програмного забезпечення. Використання OSINT для моніторингу таких форумів дозволяє отримувати інформацію про нові загрози та інструменти, що використовуються для атак.
3) Пошук інформації в відкритих базах даних. Відкриті бази даних, що містять інформацію про вразливості програмного забезпечення, IP-адреси, домени та інші технічні деталі, можуть бути використані для виявлення потенційних цілей та підготовки до атаки. OSINT дозволяє збирати ці дані автоматично, що підвищує ефективність процесу виявлення загроз [36].
4) Аналіз публікацій та звітів**.** Відкриті звіти про кіберінциденти, дослідження та публікації експертів у галузі кібербезпеки є цінним джерелом інформації про нові методи атак та захисту. OSINT може використовувати ці дані для створення актуальних профілів загроз [37].

Окрім виявлення, OSINT також може бути ефективно використаний для реагування на кіберзагрози. Важливими аспектами цього процесу є:

1) Швидке розслідування інцидентів**.** Збір та аналіз даних з відкритих джерел дозволяє оперативно отримувати інформацію про інциденти, визначати їх причини та масштаби. Це прискорює процес реагування та зменшує час, необхідний для нейтралізації загроз.
2) Ідентифікація зловмисників. Використання OSINT може допомогти у виявленні особистостей або груп, відповідальних за кіберзагрози. Моніторинг їхньої активності у відкритих джерелах надає можливість зібрати докази та передати їх до правоохоронних органів.
3) Підтримка процесу усунення вразливостей. Виявлення та аналіз вразливостей у відкритих джерелах дозволяє своєчасно розробити та

впровадити заходи щодо їх усунення. OSINT надає інформацію про актуальні вразливості та рекомендації щодо їхнього виправлення.

4) Попередження майбутніх атак. OSINT може бути використаний для створення прогнозів щодо можливих майбутніх атак. Аналізуючи тренди та патерни поведінки зловмисників, організації можуть розробляти проактивні стратегії захисту та запобігати майбутнім загрозам.

1.5 Інтеграція OSINT з іншими системами кібербезпеки

Для максимізації ефективності, OSINT повинен бути інтегрований з іншими системами кібербезпеки, такими як SIEM (Security Information and Event Management), IDS/IPS (Intrusion Detection/Prevention Systems) та антивірусні програми. Така інтеграція дозволяє:

1) Забезпечити комплексний підхід до безпеки**.** Об'єднання даних з різних джерел та систем надає більш повну картину загроз та підвищує точність виявлення [10].
2) Автоматизувати процеси. Інтеграція дозволяє автоматизувати процес збору, аналізу та реагування на загрози, що знижує навантаження на фахівців з кібербезпеки та прискорює реакцію на інциденти [8].
3) Поліпшити якість аналізу. Використання даних з різних джерел покращує якість аналізу, дозволяючи більш точно визначати пріоритети та відповідні заходи щодо реагування на загрози [9].

Таким чином, OSINT є важливим інструментом у забезпеченні кібербезпеки, який, за умови правильного використання та інтеграції, може значно підвищити ефективність виявлення та реагування на кіберзагрози.

1.6 Методологія дослідження

У цьому дослідженні для оцінки можливостей OSINT у виявленні та реагуванні на кіберзагрози використовуються різні методи збору, обробки та аналізу даних. Методологія дослідження включає кілька ключових етапів, що забезпечують комплексний підхід до вивчення предмета.

Методи збору даних:

1) Аналіз відкритих джерел інформації (OSINT)

   Цей метод передбачає систематичний збір інформації з відкритих джерел, які доступні для загального користування. Це можуть бути:

a) Інтернет-ресурси: новинні сайти, блоги, спеціалізовані форуми, де обговорюються питання кібербезпеки.

b) Наукові та технічні публікації: статті, звіти, дослідження в області кібербезпеки та IT.Офіційні веб-сайти організацій: публікації державних органів, компаній, що працюють у сфері кібербезпеки, міжнародних організацій.

2) Веб-сервіси та онлайн-інструменти

   Для збору даних використовуються різні веб-сервіси та онлайн-інструменти, що дозволяють автоматизувати процес збору інформації. Це можуть бути спеціалізовані пошукові системи та інструменти для збору OSINT, такі як Shodan, Censys, Maltego та інші. Ці інструменти дозволяють знаходити інформацію про вразливості, відкриті порти, конфігурації систем і багато іншого.

3) Соціальні медіа

   Соціальні медіа, такі як Twitter, Facebook, LinkedIn, Reddit та інші, є важливими джерелами інформації. Зловмисники часто використовують соціальні платформи для обговорення своїх дій, пошуку вразливих цілей або розповсюдження шкідливих програм. Моніторинг соціальних медіа дозволяє виявляти ранні ознаки кіберзагроз.

Методи обробки та аналізу даних:

1) Кількісний аналіз

Кількісний аналіз включає обробку числових даних, отриманих з відкритих джерел. Основні етапи кількісного аналізу включають:

a) Збір статистичних даних**:** кількість виявлених вразливостей, кількість згадувань про кіберзагрози у соціальних медіа, обсяг даних, що стосуються конкретних інцидентів.

b) Аналіз тенденцій**:** вивчення змін у кількості кіберзагроз за певний період часу, визначення пікових періодів активності зловмисників.

c) Створення діаграм і графіків: візуалізація даних для кращого розуміння тенденцій і кореляцій між різними змінними.

2) Якісний аналіз

Якісний аналіз фокусується на інтерпретації та розумінні змісту зібраних даних. Основні етапи якісного аналізу включають:

a) Контент-аналіз: аналіз змісту повідомлень у соціальних медіа, блогах, форумах. Визначення основних тем, обговорюваних у контексті кіберзагроз, і виділення ключових слів та фраз.

b) Кейс-стаді**:** детальний аналіз конкретних випадків кіберінцидентів. Опис дій зловмисників, використовуваних методів атаки та засобів захисту.

c) Аналіз взаємозв’язків**:** вивчення взаємозв’язків між різними джерелами інформації, визначення впливу соціальних медіа на поширення інформації про кіберзагрози.

3) Інтеграція методів

Для досягнення максимальної ефективності дослідження використовуються обидва методи – кількісний і якісний аналіз. Це дозволяє отримати як загальну картину кіберзагроз, так і глибоке розуміння окремих аспектів та механізмів їх реалізації. Інтеграція різних методів збору, обробки та аналізу даних забезпечує комплексний підхід до дослідження можливостей OSINT у виявленні та реагуванні на кіберзагрози.

1.7 Висновки до першого розділу

У даному розділі було розглянуто актуальність використання OSINT (Open Source Intelligence) в сучасній кібербезпеці. Встановлено, що OSINT стає все більш важливим інструментом у контексті зростаючих кіберзагроз. Основні переваги OSINT полягають у його здатності забезпечувати доступ до великого обсягу публічно доступної інформації, що дозволяє вчасно виявляти та реагувати на потенційні загрози.

Методологія дослідження включала аналіз існуючих підходів до виявлення кіберзагроз за допомогою OSINT та оцінку ефективності цих методів у реальних умовах. Кількісний аналіз передбачає збір та обробку статистичних даних, аналіз тенденцій і візуалізацію результатів за допомогою діаграм і графіків. Це дозволяє виявити основні тренди та зміни в активності кіберзагроз. Якісний аналіз фокусується на інтерпретації змісту зібраних даних через контент-аналіз, детальний аналіз конкретних випадків (кейс-стаді) та вивчення взаємозв’язків між різними джерелами інформації. Опис об'єкта дослідження (кіберзагрози та методи їх виявлення) та предмета дослідження (можливості OSINT для виявлення та реагування на кіберзагрози) дозволив сформувати комплексне уявлення про дану проблематику.

Таким чином, розділ показує, що використання OSINT є актуальним і ефективним інструментом для підвищення рівня кібербезпеки. Використання OSINT у поєднанні з сучасними методами збору, обробки та аналізу даних дозволяє значно покращити процеси виявлення та реагування на кіберзагрози. Ця методологія забезпечує комплексний та ефективний підхід до кібербезпеки, що є критично важливим у сучасному інформаційному суспільстві.

2 ОСНОВИ ТА ІНСТРУМЕНТИ OSINT В СУЧАСНІЙ КІБЕРБЕЗПЕЦІ

2.1 Теоретичні основи OSINT

2.1.1 Історія розвитку OSINT

Витоки OSINT можна простежити ще з часів античності, коли уряди та військові стратеги використовували відкриті джерела інформації для отримання важливих даних про ворога. Втім, сучасний розвиток OSINT розпочався у XX столітті, коли розвиток засобів масової інформації та технологій значно розширив можливості для збору інформації з відкритих джерел.

1) Перші кроки. На початку XX століття уряди великих країн почали активно використовувати радіо, газети та інші засоби масової інформації для збору розвідувальних даних. Під час Першої та Другої світових воєн радіопередачі часто прослуховувалися для отримання важливої інформації про плани та пересування ворога [11].
2) Холодна війна. У період Холодної війни OSINT набув більшої значущості. Обидва блоки - США та СРСР - активно використовували відкриті джерела для збору даних про економічний, військовий та науково-технічний потенціал один одного. Особливого значення набув аналіз друкованих видань, радіопередач та наукових публікацій [12].
3) Епоха Інтернету. З розвитком Інтернету у 1990-х роках можливості OSINT значно розширилися. З'явилися нові джерела інформації, такі як веб-сайти, форуми, блоги, соціальні медіа, що дозволило отримувати актуальні дані в режимі реального часу. В цей період OSINT став невід'ємною частиною діяльності розвідувальних служб багатьох країн [13].

4) Сучасний етап. На сьогоднішній день OSINT є ключовим компонентом у сфері кібербезпеки, аналітики та розвідки. Використання передових технологій, таких як машинне навчання та штучний інтелект, дозволяє автоматизувати процеси збору та аналізу інформації, підвищуючи їх ефективність та точність [2].

2.1.2 Концептуальні основи OSINT

OSINT базується на кількох ключових принципах та концепціях, що визначають його сутність та методи застосування:

1) Відкритість джерел. Основний принцип OSINT полягає у використанні відкритих джерел інформації, що доступні для широкої громадськості. Це можуть бути як традиційні медіа, так і сучасні цифрові платформи, такі як соціальні медіа та спеціалізовані веб-сайти [11].
2) Законність та етичність. Всі дії у рамках OSINT повинні відповідати законодавчим та етичним нормам. Використання відкритих джерел інформації не повинно порушувати права на приватність та інші законодавчі обмеження. Це особливо важливо у контексті збору даних з соціальних медіа та інших платформ, де можуть міститися персональні дані [13].
3) Технологічна підтримка. Сучасний OSINT активно використовує технологічні інструменти для автоматизації збору, обробки та аналізу інформації. Це включає використання програмного забезпечення для моніторингу інтернет-ресурсів, аналізу текстів, візуалізації даних та інші технології, що підвищують ефективність роботи аналітиків [2].
4) Аналітичний підхід. Важливим аспектом OSINT є не лише збір даних, але й їх аналіз та інтерпретація. Аналітики OSINT повинні вміти виявляти закономірності, робити висновки та прогнозувати

події на основі зібраної інформації. Це вимагає високого рівня компетентності та досвіду у відповідній сфері [12].

5) Інтеграція з іншими видами розвідки. OSINT часто використовується у поєднанні з іншими видами розвідки, такими як HUMINT (Human Intelligence), SIGINT (Signals Intelligence), та TECHINT (Technical Intelligence). Це дозволяє отримати більш повну та точну картину досліджуваного об'єкта або ситуації [13].

Історія розвитку OSINT свідчить про його важливу роль у сфері розвідки та кібербезпеки. Від ранніх етапів використання традиційних медіа до сучасних цифрових платформ, OSINT продовжує еволюціонувати, забезпечуючи надійну підтримку у виявленні та реагуванні на загрози. Концептуальні основи OSINT визначають його ефективність та правомірність, роблячи його незамінним інструментом у сучасному інформаційному суспільстві.

2.1.3 Основні принципи OSINT

OSINT (Open Source Intelligence) базується на кількох ключових принципах, які забезпечують його ефективність та правомірність використання:

1) Відкритість та доступність джерел. OSINT використовує тільки відкриті та доступні джерела інформації. Це можуть бути інтернет-ресурси, соціальні медіа, публікації, форуми та інші джерела, доступні без необхідності отримання спеціальних дозволів [11].
2) Законність. Всі дії в рамках OSINT повинні відповідати законодавчим нормам. Це означає, що інформація повинна збиратися та використовуватися в рамках чинного законодавства, без порушення прав на приватність та конфіденційність даних [13].
3) Етичність. Використання OSINT повинно враховувати етичні стандарти, особливо при зборі та обробці даних з соціальних медіа

та інших джерел, де можуть міститися персональні дані. Необхідно дотримуватись принципів конфіденційності та поваги до прав суб'єктів даних [12].

4) Точність та достовірність. Одним з основних принципів OSINT є забезпечення точності та достовірності зібраної інформації. Це передбачає перевірку джерел інформації, порівняння даних з різних джерел та аналіз їхньої надійності [2].
5) Актуальність. Зібрана інформація повинна бути актуальною та своєчасною, що особливо важливо у контексті кіберзагроз, де ситуація може швидко змінюватися. Це вимагає постійного моніторингу та оновлення даних [13].

2.1.4 Методи OSINT

Методи OSINT включають різноманітні техніки збору, аналізу та інтерпретації даних з відкритих джерел:

1) Веб-скрапінг (Web Scraping). Цей метод передбачає автоматичний збір інформації з веб-сайтів за допомогою спеціальних програм або скриптів. Веб-скрапінг дозволяє швидко збирати великі обсяги даних з різних онлайн-ресурсів [2].
2) Аналіз соціальних медіа. Соціальні медіа є важливим джерелом інформації про актуальні події, настрої в суспільстві та потенційні загрози. Аналіз соціальних медіа включає моніторинг повідомлень, коментарів, хештегів та інших елементів, що дозволяє виявити тенденції та потенційні загрози [11].
3) Моніторинг форумів та даркнету. Форумами та даркнетом часто користуються зловмисники для обговорення своїх планів, продажу шкідливого ПЗ та викрадених даних. Моніторинг цих платформ дозволяє виявити нові загрози та тренди у кіберзлочинності [13].

4) Пошук вразливостей. Використання спеціалізованих інструментів, таких як Shodan, Censys та інших, дозволяє знаходити інформацію про вразливості в інформаційних системах, відкриті порти, конфігурації пристроїв та інші технічні деталі, що можуть бути використані для атак [12].
5) Аналіз контенту. Цей метод включає аналіз змісту текстових даних, зібраних з різних джерел. Аналітики OSINT використовують методи контент-аналізу для виявлення ключових тем, трендів та кореляцій між різними елементами даних [2].
6) Геолокація та візуальний аналіз. Використання геолокаційних даних та візуального аналізу (наприклад, аналізу зображень та відео) дозволяє визначити місцезнаходження об'єктів, ідентифікувати об'єкти на зображеннях та відео, а також отримати інші важливі дані [11].

Основні принципи та методи OSINT забезпечують ефективний підхід до збору та аналізу даних з відкритих джерел. Використання цих принципів та методів дозволяє отримувати актуальну, точну та достовірну інформацію, необхідну для виявлення та реагування на кіберзагрози.

2.1.5 Роль OSINT у виявленні кіберзагроз

OSINT (Open Source Intelligence) відіграє ключову роль у сучасних стратегіях кібербезпеки завдяки своїм унікальним можливостям зі збору та аналізу інформації з відкритих джерел. Ця методика дозволяє виявляти кіберзагрози на ранніх стадіях, забезпечуючи своєчасне реагування та зниження потенційних ризиків.

Моніторинг відкритих джерел є одним із основних елементів OSINT. Завдяки постійному відстеженню широкого спектра ресурсів, таких як новинні сайти, блоги, соціальні медіа та форуми, можна швидко виявляти нові загрози, обговорення вразливостей та підозрілу активність у реальному часі. Це

дозволяє спеціалістам з кібербезпеки оперативно реагувати на нові виклики та мінімізувати ризики, пов'язані з поширенням інформації про вразливості.

Аналіз даних з відкритих джерел дає можливість ідентифікувати патерни поведінки зловмисників, що можуть свідчити про підготовку до атаки. Наприклад, активність у соціальних медіа або обговорення на форумах можуть вказувати на майбутні загрози. Ідентифікація таких патернів дозволяє прогнозувати потенційні атаки та розробляти ефективні заходи захисту.

OSINT також сприяє виявленню технічних вразливостей в інформаційних системах. Використовуючи дані з відкритих баз даних, таких як Shodan і Censys, можна ідентифікувати слабкі місця в системах безпеки. Це дозволяє своєчасно вживати заходів для усунення вразливостей та запобігання можливим атакам, що підвищує загальний рівень захисту інформаційних систем.

Крім того, OSINT надає важливу інформаційну підтримку під час розслідувань кіберінцидентів. Збір та аналіз інформації з відкритих джерел допомагає визначити джерела атак, методи та інструменти, які використовували зловмисники. Це значно підвищує ефективність реагування на інциденти та мінімізує їх наслідки, дозволяючи швидко відновити нормальне функціонування інформаційних систем та зменшити збитки від атак.

Використання OSINT є невід'ємною частиною сучасних стратегій кібербезпеки. Завдяки своїм можливостям зі збору та аналізу інформації з відкритих джерел, OSINT дозволяє виявляти та реагувати на кіберзагрози на ранніх стадіях, забезпечуючи тим самим більш надійний захист інформаційних систем від потенційних атак. Подальший розвиток та впровадження новітніх методик у цій сфері сприятимуть покращенню загального рівня кібербезпеки.

2.1.6 Значення OSINT у виявленні кіберзагроз

OSINT має кілька ключових аспектів, які роблять його незамінним інструментом у сфері кібербезпеки.

Доступність та економічна ефективність є одними з основних переваг OSINT. Використання відкритих джерел інформації дозволяє значно знизити витрати на розвідку порівняно з традиційними методами. OSINT не вимагає значних фінансових ресурсів, оскільки дані збираються з публічно доступних джерел, що робить цей підхід доступним для широкого кола організацій, включаючи ті, що мають обмежені бюджети.

Актуальність та швидкість інформації, зібраної за допомогою OSINT, є критично важливими у контексті сучасних динамічних кіберзагроз. Можливість збору інформації в реальному часі забезпечує своєчасне виявлення загроз та швидке реагування на них. Це особливо важливо у ситуаціях, коли загрози можуть швидко змінюватися та адаптуватися, що вимагає оперативного прийняття рішень.

Широке охоплення джерел інформації дозволяє OSINT забезпечувати комплексний підхід до кібербезпеки. Включаючи технічні деталі, такі як вразливості в програмному забезпеченні, а також соціальні фактори, як обговорення у соціальних медіа, OSINT дозволяє отримувати різноманітні дані про кіберзагрози. Це багатогранне охоплення допомагає краще розуміти контекст загроз та їх потенційний вплив.

Підтримка прийняття рішень є ще одним важливим аспектом OSINT. Інформація, зібрана за допомогою відкритих джерел, надає аналітикам важливу підтримку в процесі прийняття рішень щодо кібербезпеки. Ці дані можуть бути використані для оцінки ризиків, розробки стратегій захисту та планування заходів реагування на інциденти, що значно підвищує ефективність захисту інформаційних систем.

Проактивний підхід, який забезпечує OSINT, дозволяє здійснювати моніторинг та аналіз потенційних загроз на ранніх стадіях. Це дає можливість

попередити атаки ще до їх реалізації, що значно підвищує рівень захисту інформаційних систем та зменшує ризики. Проактивний моніторинг сприяє створенню більш стійкої системи кібербезпеки, яка здатна адаптуватися до нових викликів.

OSINT є невід'ємною частиною сучасної кібербезпеки, забезпечуючи ефективний та економічно вигідний підхід до виявлення та реагування на кіберзагрози. Використання відкритих джерел інформації дозволяє своєчасно ідентифікувати загрози, виявляти вразливості та підтримувати процеси прийняття рішень у сфері кібербезпеки. Це робить OSINT потужним інструментом для захисту інформаційних систем у сучасному цифровому середовищі.

2.2 Огляд основних інструментів та платформ OSINT, їх можливості та недоліки

У сфері OSINT існує безліч інструментів та платформ, що допомагають аналітикам збирати та аналізувати дані з відкритих джерел. Серед найпопулярніших і найефективніших можна виділити Maltego, Shodan, Censys, theHarvester та інші. Кожен з цих інструментів має свої унікальні функції та переваги.

Maltego – це потужний інструмент для візуалізації даних, що дозволяє проводити аналіз зв'язків між різними об'єктами. Він широко використовується для розслідувань у сфері кібербезпеки, збору даних про домени, IP-адреси, соціальні мережі та інші джерела.

Можливості:

1) Візуалізація даних: Maltego дозволяє створювати графічні схеми, що показують зв'язки між об'єктами, що значно спрощує процес аналізу великих обсягів даних [14].

2) Інтеграція з іншими інструментами: Maltego підтримує інтеграцію з різними джерелами даних та іншими інструментами, що розширює його функціональні можливості.
3) Кастомізація: Користувачі можуть налаштовувати інструмент під свої потреби, створюючи власні трансформації для збору специфічних даних.

Недоліки даного інструмента:

1) Висока вартість: Ліцензія на повну версію Maltego може бути досить дорогою, що може бути перешкодою для малих компаній або індивідуальних користувачів.
2) Складність в навчанні: Інструмент має досить складний інтерфейс, що може вимагати значного часу для освоєння.

На рисунку 2.1 показано головну сторінку електоронного ресурсу Maltego.

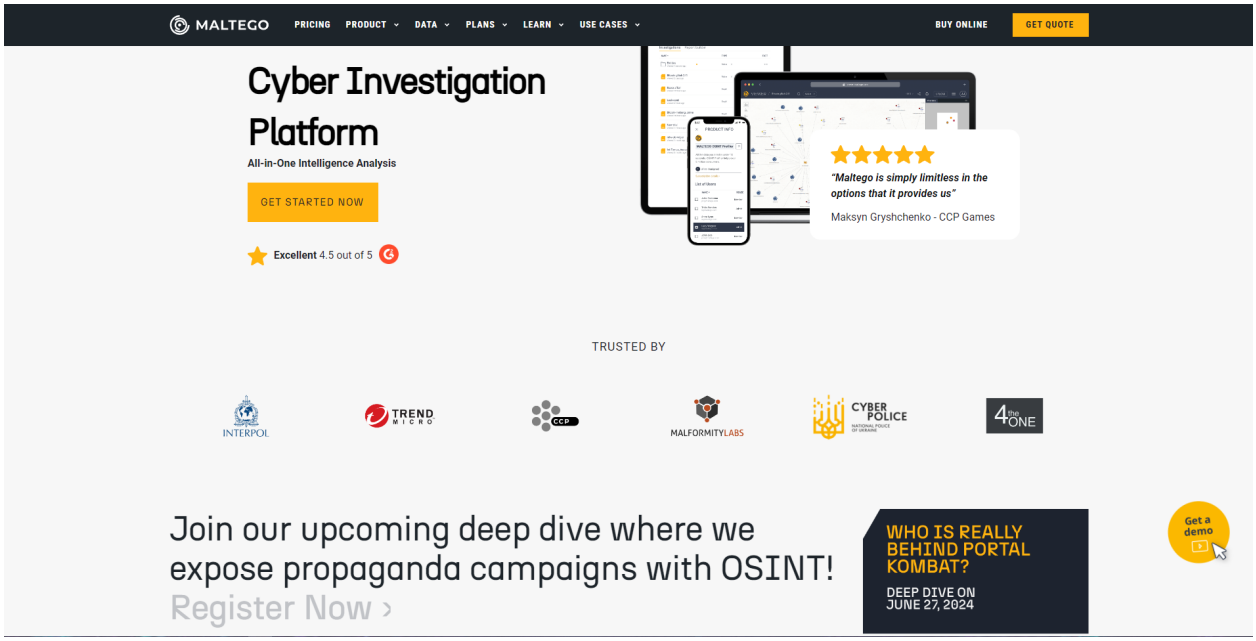

Рисунок 2.1 – Головна сторінка електоронного ресурсу Maltego

Shodan – це пошукова система для Інтернету речей (IoT), що дозволяє знаходити підключені до Інтернету пристрої. Вона використовується для виявлення вразливих пристроїв, відкритих портів та інших конфігурацій.

Можливості:

1) Сканування мережі: Shodan дозволяє сканувати мережі на наявність підключених пристроїв, таких як камери, маршрутизатори, сервери та інші IoT-пристрої [15].
2) Виявлення вразливостей: Інструмент допомагає ідентифікувати вразливі пристрої, що можуть бути потенційними цілями для атак.
3) Моніторинг мережі: Shodan забезпечує можливість моніторингу стану мережі та виявлення змін у конфігурації пристроїв.

Недоліки:

1) Обмеженість даних: Shodan збирає дані тільки з відкритих портів, тому він може не виявити всі потенційні загрози в мережі.
2) Необхідність технічних знань: Для ефективного використання Shodan користувачі повинні мати досить високий рівень технічних знань та розуміння мережевих технологій.

На рисунку 2.2 показано головну сторінку електоронного ресурсу Shodan.

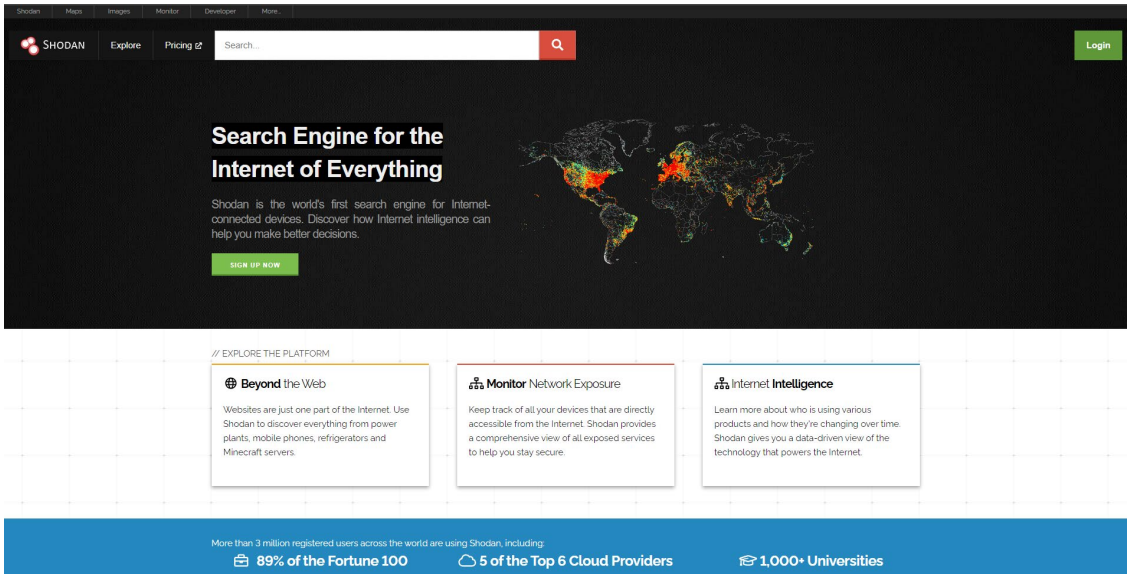

Рисунок 2.2 – Головна сторінка електоронного ресурсу Shodan

Censys – це платформа для моніторингу та аналізу стану Інтернету. Вона дозволяє проводити пошук та аналіз інформації про відкриті порти, сертифікати SSL/TLS, конфігурації пристроїв та інші технічні деталі.

Можливості:

1) Глобальний сканер Інтернету: Censys регулярно сканує Інтернет, збираючи дані про підключені пристрої та їх конфігурації [16].
2) Аналіз безпеки: Інструмент дозволяє проводити аналіз безпеки мережевих пристроїв, виявляти вразливості та слідкувати за їх усуненням.
3) Пошук даних: Censys надає можливість пошуку інформації за різними параметрами, що дозволяє знаходити конкретні пристрої чи конфігурації.

Недоліки:

1) Висока вартість преміум-версії: Як і Maltego, повна функціональність Censys доступна тільки у платній версії, що може бути дорогим для малих організацій.
2) Відсутність деяких даних: Censys може не охоплювати всі пристрої та мережі, оскільки його сканування залежить від багатьох факторів, включаючи географічне розташування та типи мереж.

На рисунку 2.3 показано головну сторінку електоронного ресурсу Censys.

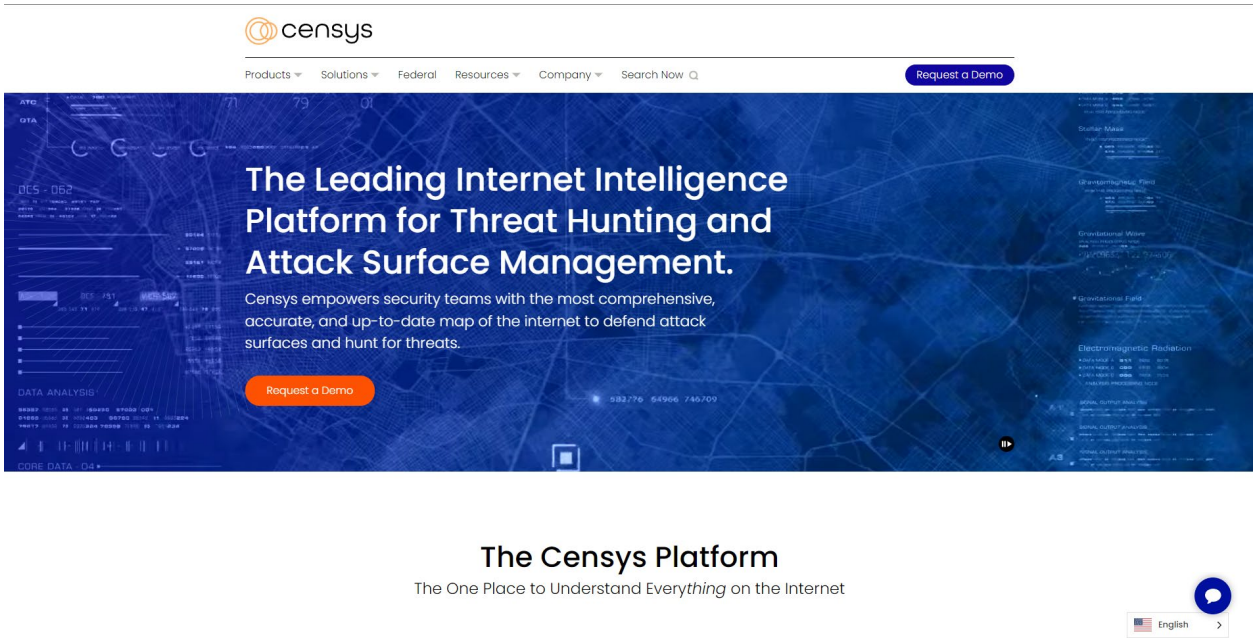

Рисунок. 2.3 – Головна сторінка електоронного ресурсу Censys

theHarvester – це інструмент для збору інформації про домени, електронні адреси, IP-адреси та інші мережеві ресурси. Він широко використовується для розвідки у сфері кібербезпеки та підготовки до тестування на проникнення.

Можливості:

1) Збір даних з різних джерел: theHarvester збирає дані з пошукових систем, соціальних мереж, DNS-серверів та інших джерел [17].
2) Інтеграція з іншими інструментами: Інструмент може інтегруватися з іншими інструментами та платформами для розширення своїх можливостей.
3) Автоматизація процесу збору даних: theHarvester автоматизує процес збору інформації, що дозволяє швидко отримувати необхідні дані.

Недоліки:

1) Обмеженість джерел: theHarvester обмежується тими джерелами, з яких він може збирати дані, тому деяка інформація може бути пропущена.

2) Відсутність аналізу: Інструмент в основному орієнтований на збір даних і не надає розширених можливостей для їх аналізу, тому отримані дані потребують додаткової обробки [17].

На рисунку 2.4 показано головну сторінку електоронного ресурсу theHarvester, а на рисунку 2.5 зображено графічний інтерфейс даного інструмента в операційній системі Kali Linux.

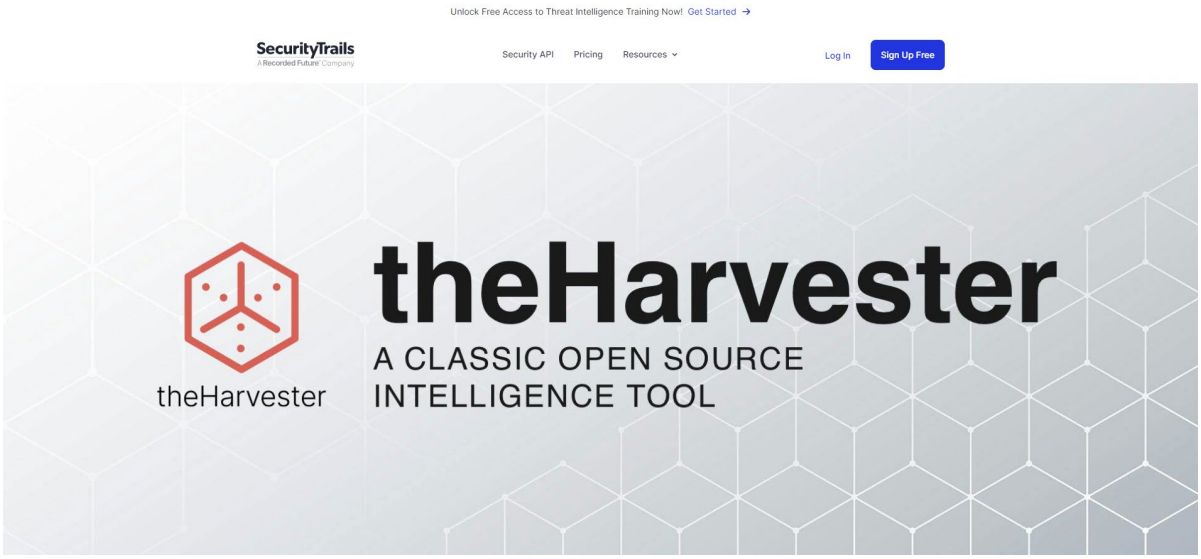

Рисунок 2.4 – Головна сторінка електоронного ресурсу theHarvester

Рисунок 2.5 – Графічний інтерфейс theHarvester

SpiderFoot – це інструмент для автоматизованого збору даних з різних джерел, що дозволяє проводити комплексний аналіз кіберзагроз.

Можливості:

1) Автоматизований збір даних: SpiderFoot дозволяє автоматизувати збір даних з багатьох джерел, що значно спрощує процес розвідки.
2) Модульна структура: Інструмент підтримує модулі для різних видів даних, що робить його дуже гнучким і настроюваним під конкретні потреби [18].

Недоліки:

1) Складність налаштування: Для ефективного використання SpiderFoot може вимагатися складне налаштування та конфігурація, що потребує технічних знань.
2) Проблеми з точністю: Деякі модулі можуть надавати неточні або неповні дані, що може впливати на результати розвідки [18].

На рисунку 2.6 показано головну сторінку електоронного ресурсу SpiderFoot, а на рисунку 2.7 зображено графічний інтерфейс даного інструмента.

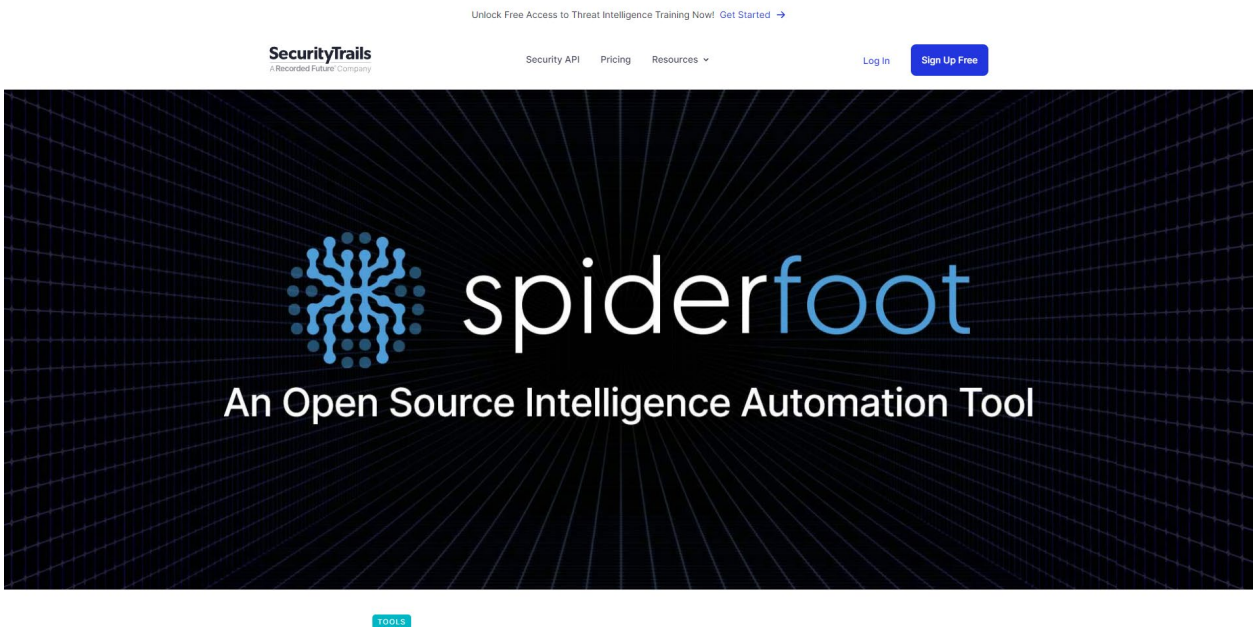

Рисунок 2.6 – Головна сторінка електоронного ресурсу SpiderFoot

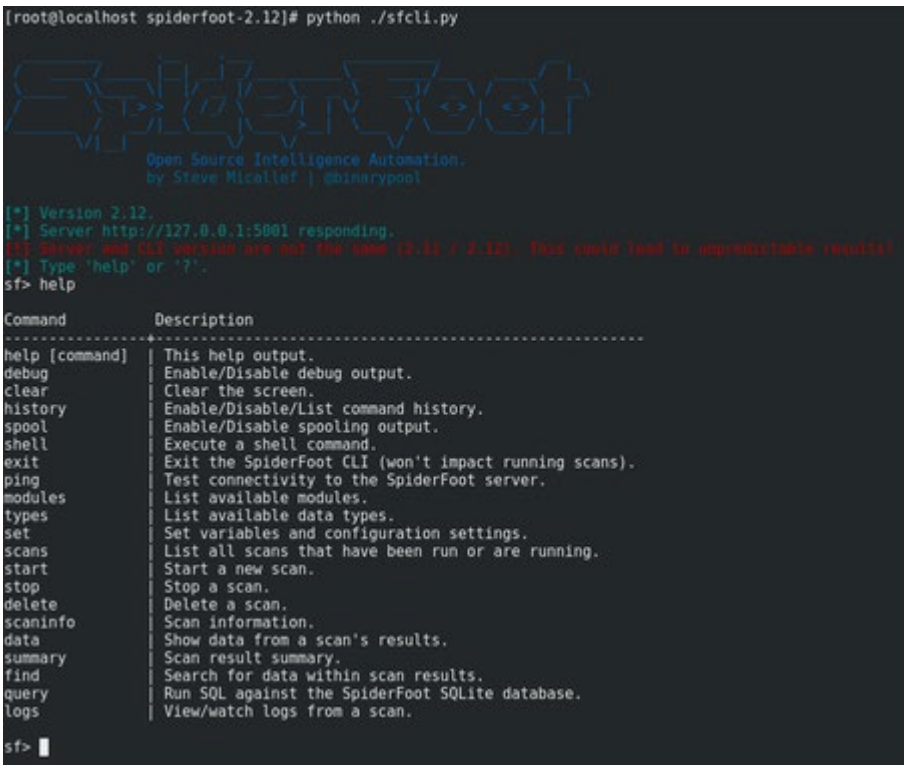

Рисунок 2.7 – Графічний інтерфейс SpiderFoot

FOCA – це інструмент для аналізу метаданих у документах, що дозволяє виявляти приховану інформацію.

Можливості:

1) Аналіз метаданих: FOCA дозволяє аналізувати метадані в документах, що допомагає виявляти приховану інформацію [19].
2) Збір даних з різних форматів: Інструмент підтримує роботу з багатьма форматами документів, включаючи PDF, DOC, XLS та інші.

Недоліки:

1) Обмежена функціональність: FOCA спеціалізується тільки на аналізі метаданих, тому його можливості обмежені в порівнянні з іншими інструментами OSINT.
2) Необхідність додаткової обробки даних: Отримані дані потребують додаткової обробки для використання у комплексних розслідуваннях [19].

На рисунку 2.8 зображено інтерфейс програми Fingerprinting Organizations with Collected Archives.

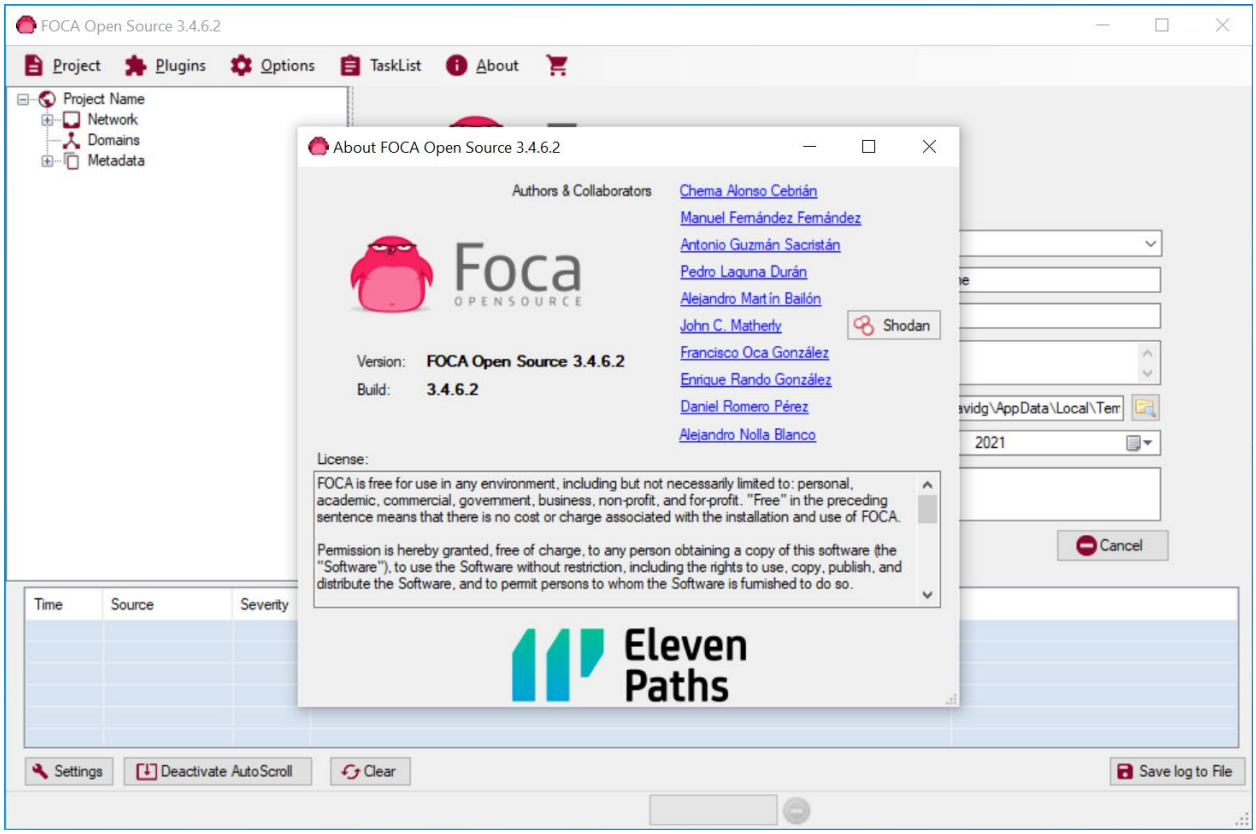

Рисунок 2.8 – Інтерфейс програми FOCA

Recon-ng – це платформа для розвідки, що підтримує модульну структуру та дозволяє інтегрувати різні методи збору та аналізу даних.

Можливості:

1) Модульна структура: Recon-ng має модульну архітектуру, що дозволяє користувачам додавати різні модулі для збору та аналізу даних, залежно від конкретних потреб. Ця гнучкість робить його дуже універсальним інструментом для розвідки.
2) Автоматизація збору даних: Інструмент автоматизує процес збору даних з різноманітних джерел, таких як пошукові системи, соціальні медіа, DNS-сервери та інші.
3) Звітність: Recon-ng дозволяє генерувати детальні звіти про зібрані дані, що є корисним для подальшого аналізу та прийняття рішень [20].

Недоліки:

1) Потреба в налаштуванні: Для максимальної ефективності інструменту потрібні початкові налаштування, що можуть вимагати певних технічних знань.
2) Обмежена база даних: Як і інші інструменти, Recon-ng залежить від доступності та якості даних у відкритих джерелах, що може обмежувати його можливості у певних випадках [20].

На рисунку 2.9 зображено інтерфейс програми Recon-ng.

Рисунок 2.9 – Інтерфейс програми Recon-ng

Кожен з цих інструментів має свої унікальні функції та підходи до збору та аналізу даних. Використання їх у комплексі дозволяє забезпечити ефективний процес виявлення та реагування на кіберзагрози, отримуючи детальну та актуальну інформацію з різноманітних відкритих джерел.

2.3 Висновки додругого розділу

У другому розділі дипломної роботи було розглянуто теоретичні основи та основні інструменти OSINT, їх можливості та недоліки. OSINT, як важливий компонент сучасної кібербезпеки, виявився надзвичайно потужним

інструментом для збору, аналізу та моніторингу інформації з відкритих джерел.

Теоретичні основи OSINT, включаючи його історію розвитку, концептуальні основи, основні принципи та методи, становлять основу для розуміння та ефективного використання цього інструменту. Розглянувши роль OSINT у виявленні кіберзагроз і його значення у цьому процесі, стає очевидним, що він дозволяє оперативно реагувати на потенційні небезпеки та мінімізувати їх наслідки.

Огляд основних інструментів та платформ OSINT показав їхні можливості і недоліки. Хоча ці інструменти дозволяють здійснювати різноманітний аналіз інформації з відкритих джерел, вони також мають обмеження, пов'язані з точністю та актуальністю даних, а також з етичними питаннями.

Отже, розділ підкреслив важливість і актуальність OSINT у сучасній кібербезпеці, визначивши його роль як критичного елементу в проактивному виявленні та моніторингу кіберзагроз. Для подальшого розвитку інформаційної безпеки важливо продовжувати дослідження та вдосконалювати інструменти OSINT з метою забезпечення максимально ефективного захисту інформаційних ресурсів.

3 ПРАКТИЧНЕ ЗАСТОСУВАННЯ OSINT: МЕТОДИКИ, ЕФЕКТИВНІСТЬ ТА ЕТИЧНІ АСПЕКТИ

3.1 Практичне застосування OSINT для виявлення кіберзагроз

3.1.1 Методика проведення OSINT-досліджень

OSINT-дослідження є систематичним процесом збору, аналізу та інтерпретації даних з відкритих джерел для виявлення та реагування на кіберзагрози. Методика проведення таких досліджень включає кілька основних етапів: планування, збір даних, обробка та аналіз даних, а також підготовка звітів і реагування на виявлені загрози.

На етапі планування визначаються цілі та завдання дослідження, а також обираються відповідні інструменти та джерела для збору даних. Важливими аспектами цього етапу є чітке формулювання мети дослідження, наприклад, виявлення конкретних типів кіберзагроз або моніторинг активності певних груп зловмисників. Вибір найбільш підходящих інструментів OSINT, таких як Maltego, Shodan, Censys, theHarvester, SpiderFoot, FOCA та Recon-ng, залежить від поставлених цілей. Також необхідно ідентифікувати відкриті джерела, які будуть використані для збору інформації, такі як соціальні медіа, форуми, новинні сайти, бази даних вразливостей та інші.

На етапі збору даних здійснюється безпосередній збір інформації з обраних джерел за допомогою інструментів OSINT. Основні кроки включають моніторинг соціальних медіа та форумів з використанням інструментів для автоматичного збору даних, де можуть обговорюватися кіберзагрози. Сканування мережевих пристроїв здійснюється за допомогою Shodan та Censys для виявлення підключених до Інтернету пристроїв і їх вразливостей. Збір інформації про домени та IP-адреси виконується за допомогою theHarvester, що дозволяє зібрати дані про домени, електронні адреси, IP-адреси та інші мережеві ресурси. Для аналізу метаданих у документах

використовується FOCA, що може містити важливу інформацію про потенційні загрози.

Зібрані дані повинні бути оброблені та проаналізовані для виявлення актуальних загроз і тенденцій. Цей етап включає валідацію даних для перевірки їх точності та достовірності з метою уникнення помилкових висновків. Аналіз патернів та тенденцій здійснюється за допомогою інструментів, таких як Maltego, для візуалізації зв'язків між об'єктами та аналізу патернів поведінки зловмисників. Ідентифікація вразливостей проводиться через аналіз даних, зібраних за допомогою Shodan і Censys, що дозволяє виявити вразливі пристрої та системи.

Останнім етапом є підготовка звітів на основі проведеного аналізу та вживання заходів для реагування на виявлені загрози. Підготовка звітів включає створення детальних документів, що містять результати аналізу, виявлені загрози, рекомендації щодо їх усунення та попередження майбутніх атак. Реагування на загрози передбачає вживання заходів для усунення вразливостей, зміцнення безпеки систем та попередження можливих атак у майбутньому. Постійний моніторинг стану безпеки та оновлення захисних заходів на основі нових даних і тенденцій є важливими для підтримання високого рівня захисту інформаційних систем.

Методика проведення OSINT-досліджень є комплексним процесом, що включає планування, збір, обробку та аналіз даних, а також підготовку звітів та реагування на загрози. Використання сучасних інструментів OSINT, таких як Maltego, Shodan, Censys, theHarvester, SpiderFoot, FOCA та Recon-ng, дозволяє ефективно виявляти та реагувати на кіберзагрози, забезпечуючи надійний захист інформаційних систем.

3.1.2 Реальні приклади виявлення кіберзагроз за допомогою OSINT

OSINT (Open Source Intelligence) довів свою ефективність у виявленні та нейтралізації кіберзагроз у багатьох реальних випадках. Завдяки своїм можливостям зі збору та аналізу даних з відкритих джерел, OSINT допомагає організаціям своєчасно реагувати на загрози та запобігати інцидентам.

Одним із найпоширеніших прикладів використання OSINT є виявлення витоку конфіденційних даних через соціальні медіа. Наприклад, компанія могла виявити інформацію про продаж бази даних користувачів на одному з форумів або в соціальній мережі. За допомогою інструментів OSINT, таких як SpiderFoot або theHarvester, можна було швидко зібрати інформацію про джерело витоку та ідентифікувати користувачів, які могли отримати доступ до цих даних. [17].

Інший приклад – виявлення вразливих пристроїв у мережі організації за допомогою Shodan. У 2021 році велика фінансова установа використовувала Shodan для моніторингу своєї мережі і виявила кілька пристроїв з відкритими портами, які не відповідали стандартам безпеки. Це дозволило своєчасно усунути вразливі місця та запобігти потенційним атакам [15].

Ось приклад як за допомогою OSINT та інструмента Shodan можна виявити вражливість вашого пристрою. Пристроєм буде слугувати камера відеоспостереження. Співробітники компанії які встановлюють камери затверджують вас, що до камери ніхто крім вас не зможе отримати доступ, а потім самі ж ставлять паролі «12345» або «admin» чи припускаються помилок конфігурації. Зловмисники запросто можуть підібрати такий пароль. Щоб перевірити чи справді захищена ваша камера потрібно виконати тільки пару простих кроків.

Заходимо на сайт Shodan який проводить пошук по всіх пристроях що підключені до мережі. Шукаєм на ньому свій IP адрес камери, також на сайті вказана основна інформація про сам пристрій, (див. рисунок 3.1)

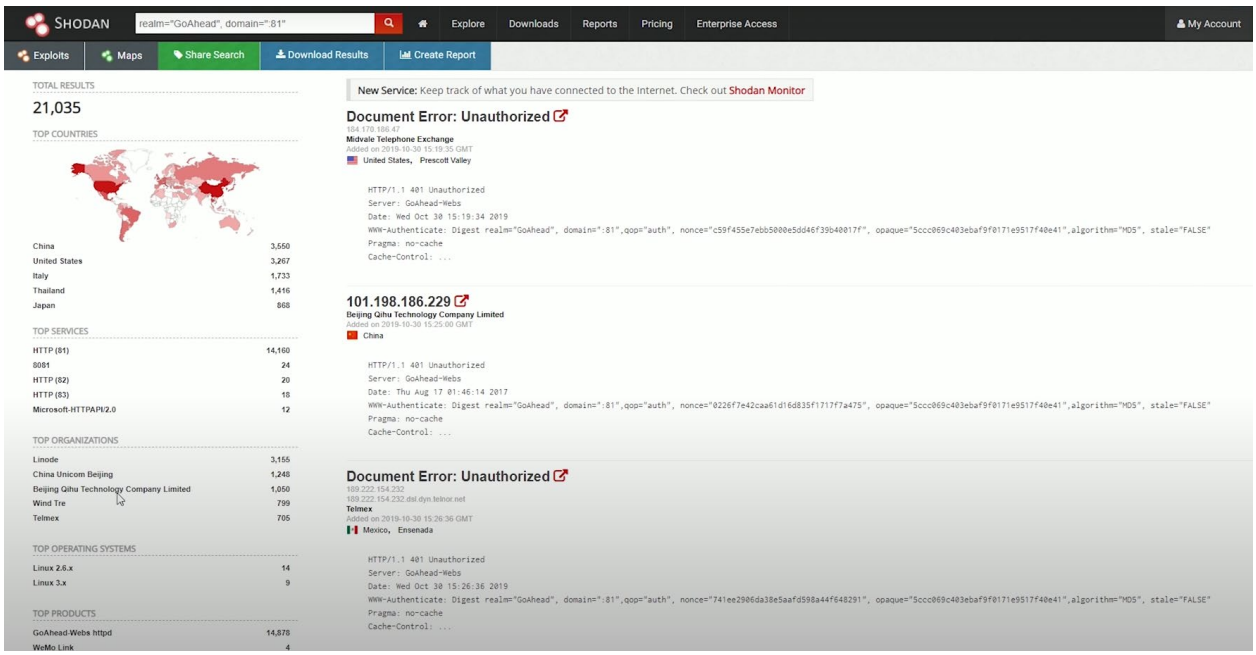

Рисунок 3.1 – Пошук камери

Берем цей адрес і відкриваєм його через бравзер, вказавши порт через двохкрапку, після виконання пошуку появиться вікно авторизації, (див.рисунок 3.2)

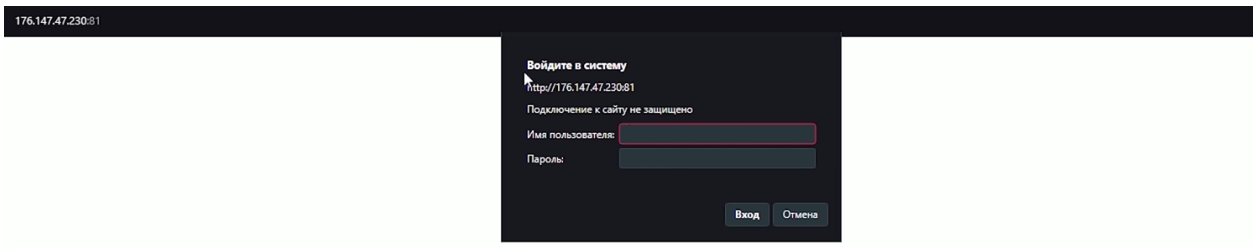

Рисунок 3.2 – Вікно авторизації

Щоб зловмиснику отримати доступ до даної камери прийдеться підбирати пароль і на перший погляд здається що камера захищена, но це не так. В камерах всі логіни і паролі зберігаються в файлах конфігурацій, які зашифровані. Але деякі компанії допускаються помилок і не шифрують даний файл і з допомогою спеціального запиту зловмисник може його злегкістю

отримати. Цей запит виглядає ось так: 176.147.47.230:81/system.ini?loginuse&loginpas. Вставивши цю команду в бравзер і виконавши пошук скачається файл конфігурації, (див. рисунок 3.3), де буде зберігатися в незашифрованому виді інформація, така як: ваш логін та пароль, (див. рисунок 3.4)

Рисунок 3.3 – Файл конфігурації

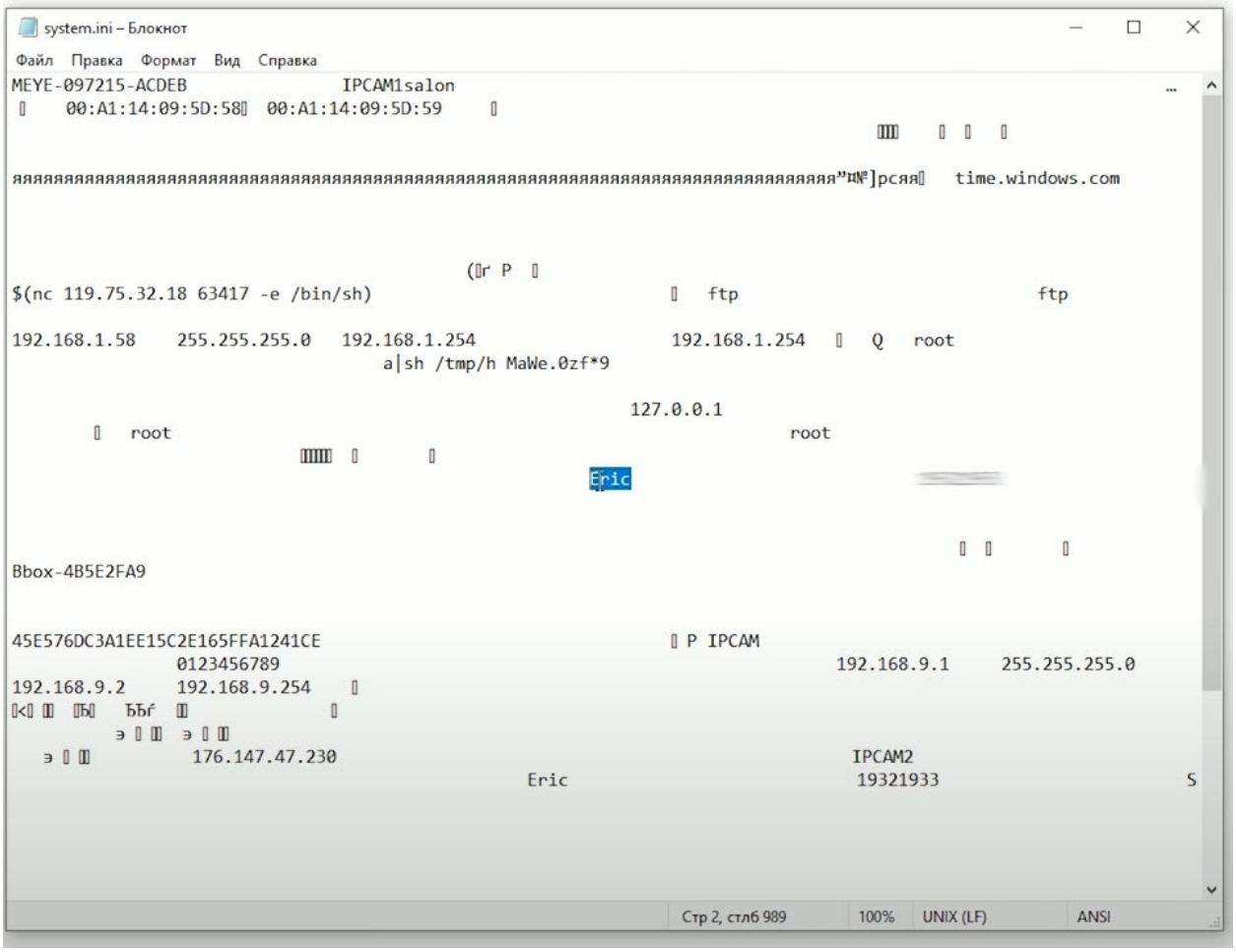

Рисунок 3.4 – Логін і пароль для авторизації

Після чого потрібно ще раз ввести в пошоковій стрічці IP та порт, з’явиться знову вікно авторизації, куди потрібно ввести дані, (див. рисунок 3.5)

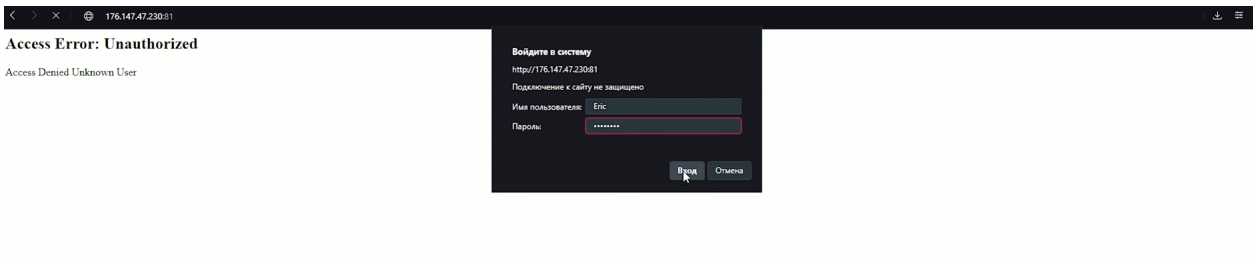

Рисунок 3.5 – Авторизація

Далі вибравши тип трансляції, отримуємо доступ до камери, а також контроль над нею, це показано на рисунку 3.6, а також зайти в налаштування і повністю змінити її налаштування або вимкнути її, (див. рисунок 3.7)

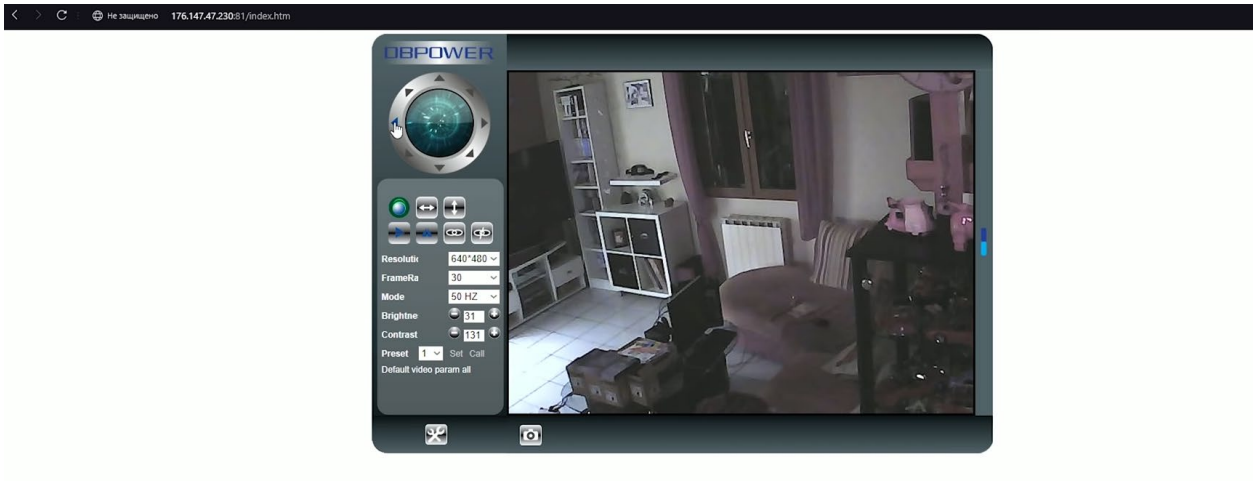

Рисунок 3.6 – Успішний доступ до камери

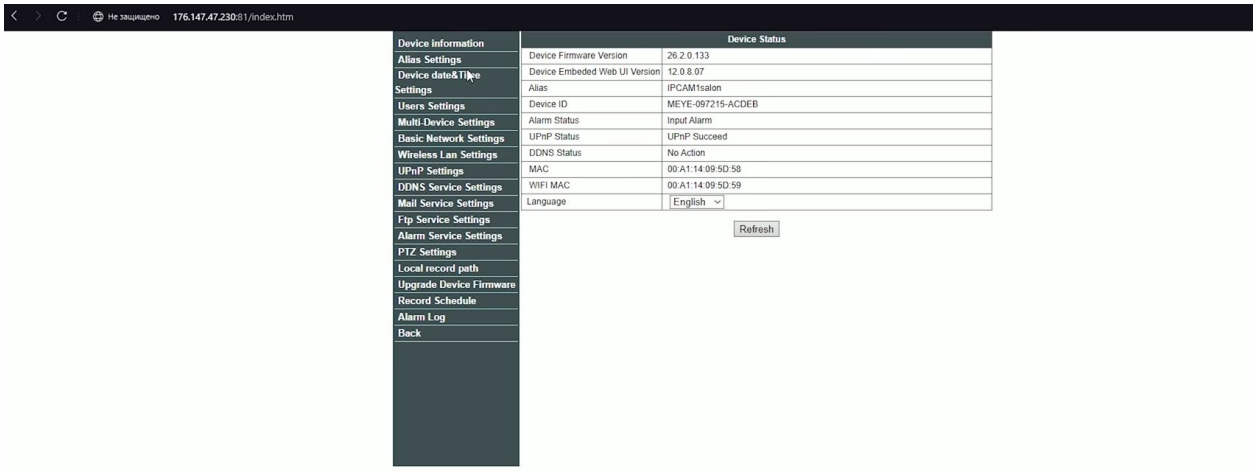

Рисунок 3.7 – Налаштування камери

В даному випадку можна побачити яскравий приклад як з допомогою OSINT можна виявити кіберзагрозу.

Maltego широко використовується для розслідування фішингових атак. Наприклад, в одній із компаній співробітники отримали підозрілі електронні листи, які намагалися викрасти їхні облікові дані. За допомогою Maltego аналітики змогли виявити зв'язки між цими листами та раніше відомими фішинговими кампаніями. Інструмент дозволив створити схеми, що показали джерела цих атак і допомогли ідентифікувати зловмисників. [14].

Також цей інструмент можна використовувати і для пошуку вразливостей електронних ресурсів. Візмемо наприклад домен gazeta.uz і застосуєм фільтр DNS from Domains, результат можна побачити на рисунку 3.8

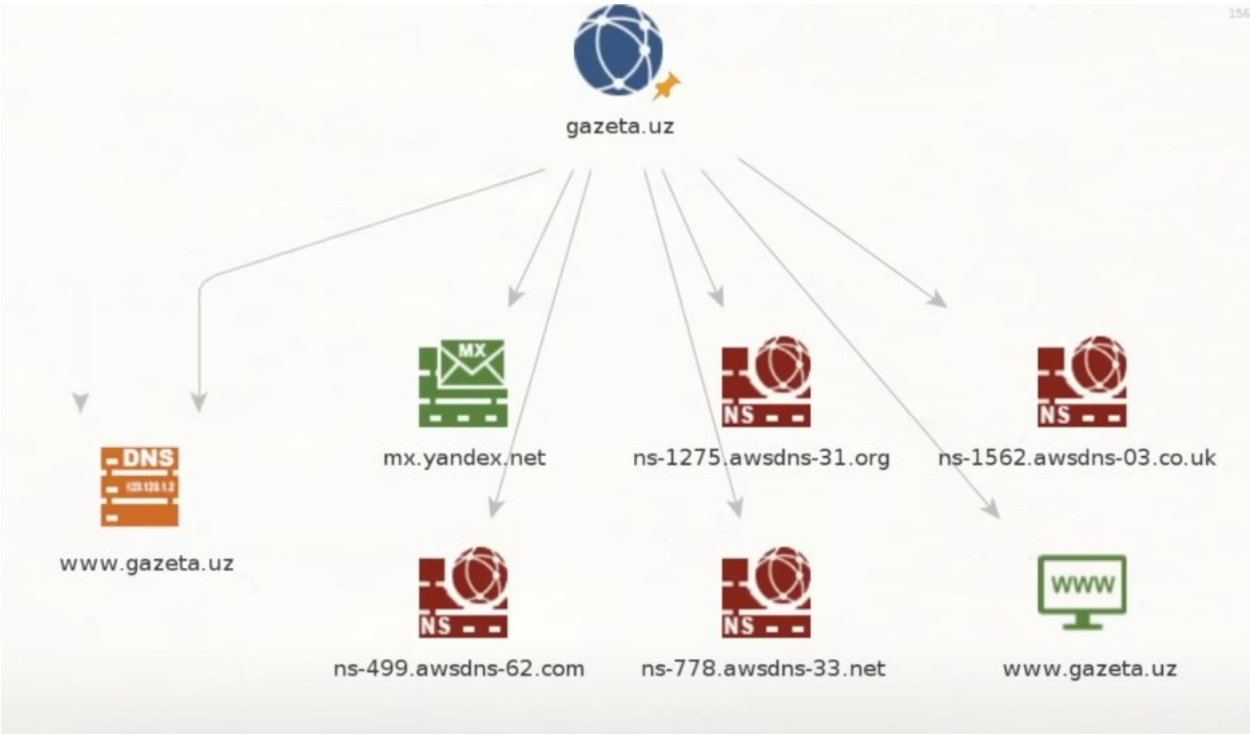

Рисунок 3.8 – Результат застосування фільтра DNS

Спробуємо отримати IP адрес даного сайта, нажавши Resolve to IP, результат можна побачити на рисунку 3.9

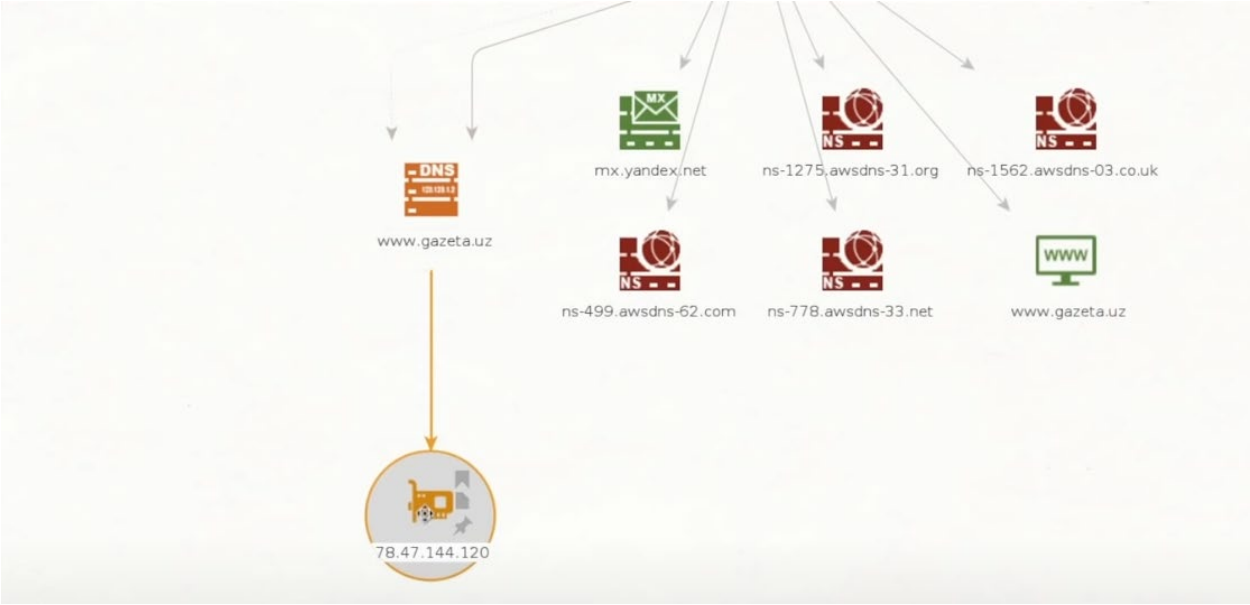

Рисунок 3.9 – IP сайту www.gazeta.uz

Копіюємо даний IP вставляєм у пошукову стрічку бравзера і переходимо на сайт, як можна побачити на рисунку 3.10 нам відкривається сайт gazeta.uz, а це офіційний сайт газети Узбекистана.

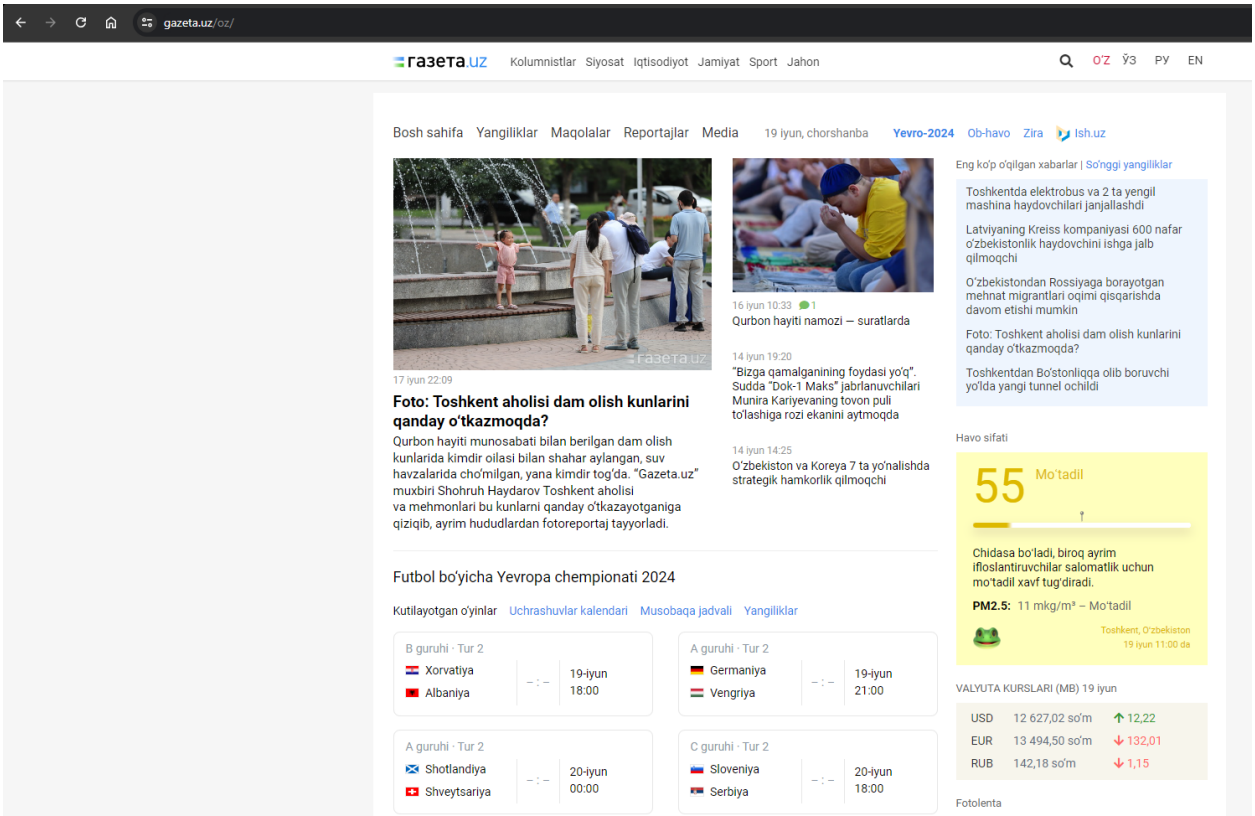

Рисунок 3.10 – Офіційний сайт газети Узбекистана

Ми дізналися справжній адрес цього сайту, а це вказує на наявністькіберзагрози,а саме можливості здійснити DoS чи DDoS атаку, тим самим зробити сервіс не доступний для користувачів.

Censys допоміг одній із IT-компаній виявити шкідливе програмне забезпечення на своїх серверах. Регулярне сканування мережі виявило підозрілі з'єднання з зовнішніми IP-адресами, які не повинні були мати доступу до внутрішніх серверів. Це дозволило аналітикам провести глибокий аналіз і знайти шкідливе ПЗ, яке вже встигло завдати шкоди. [16].

Інструмент Recon-ng використовувався для виявлення кіберзагроз в одній з організацій, яка зазнала численних спроб несанкціонованого доступу до своїх систем. Завдяки модулям для збору даних з відкритих джерел вдалося зібрати інформацію про IP-адреси зловмисників, виявити зв'язки між ними та іншими подібними атаками. Це дозволило організації зміцнити свою систему безпеки та запобігти майбутнім атакам. [20].

FOCA допоміг одній юридичній фірмі виявити вразливості у своїй документній системі. Використовуючи цей інструмент для аналізу метаданих у файлах, що надсилалися клієнтам, фірма виявила, що деякі документи містили конфіденційну інформацію, яка не повинна була бути доступною. Це дозволило їм вжити заходів для захисту цієї інформації та запобігти витоку даних. [19].

Реальні приклади використання OSINT показують, наскільки важливим є цей підхід для сучасної кібербезпеки. Від виявлення витоків даних у соціальних медіа до ідентифікації вразливих пристроїв та розслідування фішингових атак – OSINT є незамінним інструментом для своєчасного реагування на кіберзагрози та запобігання інцидентам.

3.1.3 Аналіз ефективності використання OSINT у конкретних випадках

Використання OSINT для виявлення та реагування на кіберзагрози демонструє високу ефективність у різних сценаріях. У цьому розділі ми розглянемо конкретні випадки використання OSINT і проаналізуємо його ефективність на основі реальних прикладів.

У випадку з компанією, яка виявила витік конфіденційних даних у соціальних медіа, OSINT-інструменти, такі як SpiderFoot та theHarvester, дозволили швидко ідентифікувати джерело витоку та потенційних зловмисників. Швидке реагування та знешкодження загрози допомогло компанії мінімізувати шкоду та вжити заходів для запобігання подібним інцидентам у майбутньому. Цей приклад демонструє ефективність OSINT у швидкому виявленні та реагуванні на витоки даних.

Фінансова установа, яка використовувала Shodan для моніторингу своєї мережі, змогла виявити кілька вразливих пристроїв з відкритими портами. Це дозволило закрити вразливі місця та запобігти потенційним атакам. Ефективність Shodan у цьому випадку полягала у здатності швидко сканувати мережу та надавати точну інформацію про конфігурацію пристроїв.

При розслідуванні фішингових атак Maltego показав себе як потужний інструмент для виявлення зв'язків між підозрілими електронними листами та відомими фішинговими кампаніями. Візуалізація зв'язків допомогла аналітикам швидко зрозуміти структуру атаки та ідентифікувати зловмисників. Цей приклад підкреслює ефективність Maltego у складних розслідуваннях, де необхідно швидко ідентифікувати та аналізувати зв'язки між різними об'єктами.

ІТ-компанія, яка використовувала Censys для моніторингу своїх серверів, виявила шкідливе програмне забезпечення, що вже встигло завдати шкоди. Censys допоміг ідентифікувати підозрілі з'єднання з зовнішніми IP-адресами, що дозволило аналітикам провести глибший аналіз і знайти

шкідливе ПЗ. Це демонструє ефективність Censys у виявленні аномалій та шкідливого програмного забезпечення.

Організація, яка зазнала численних спроб несанкціонованого доступу, використовувала Recon-ng для збору даних про IP-адреси зловмисників. Використання модулів для збору даних з відкритих джерел дозволило зібрати інформацію про зловмисників та їхні зв'язки з іншими подібними атаками. Це дозволило організації зміцнити свою систему безпеки та запобігти майбутнім атакам, підкреслюючи ефективність Recon-ng у проактивному моніторингу та аналізі загроз.

Юридична фірма, яка використовувала FOCA для аналізу метаданих у своїх документах, змогла виявити конфіденційну інформацію, яка не повинна була бути доступною. Використання FOCA дозволило виявити ці вразливості та вжити заходів для їх усунення, що допомогло запобігти потенційним витокам даних. Це приклад ефективності FOCA у виявленні прихованих вразливостей у документах.

Аналіз ефективності використання OSINT у конкретних випадках показує, що цей підхід є важливим інструментом у боротьбі з кіберзагрозами. Від виявлення витоків даних і вразливих пристроїв до розслідування фішингових атак та аналізу метаданих – OSINT демонструє високу ефективність у різних сценаріях. Використання інструментів OSINT дозволяє організаціям своєчасно реагувати на загрози та запобігати інцидентам, забезпечуючи надійний захист своїх інформаційних систем.

3.2 Реагування на кіберзагрози за допомогою OSINT

3.2.1 Стратегії реагування на кіберзагрози, виявлені за допомогою OSINT

Ефективне реагування на кіберзагрози, виявлені за допомогою OSINT, включає комплекс заходів, спрямованих на швидке усунення вразливостей, нейтралізацію загроз та мінімізацію потенційної шкоди. У цьому розділі розглянемо ключові стратегії реагування, які включають оцінку загроз, планування дій, впровадження заходів безпеки, моніторинг і вдосконалення.

Першим кроком у реагуванні на кіберзагрози є їх оцінка. Необхідно визначити рівень загрози, потенційний вплив та пріоритетність дій. Для цього використовуються методи класифікації загроз, де визначається тип загрози, як фішинг, шкідливе ПЗ, атаки на мережу тощо, та її джерело [20]. Оцінка ризиків включає аналіз потенційного впливу загрози на організацію, що враховує фінансові втрати, репутаційні ризики та вплив на операційну діяльність. Пріоритезація допомагає визначити пріоритет реагування на загрози на основі їх критичності та ймовірності реалізації.

На основі оцінки загроз розробляється план дій, який включає конкретні заходи для нейтралізації загроз та усунення вразливостей. Це включає розробку стратегії реагування, що визначає основні кроки для реагування на загрозу, включаючи технічні заходи, комунікаційні стратегії та планування ресурсів. Важливим елементом є формування команд реагування, які будуть відповідати за різні аспекти реагування, включаючи технічну підтримку, юридичні питання та зв'язки з громадськістю [15].

Після розробки плану дій необхідно впровадити конкретні заходи для нейтралізації загроз та підвищення рівня безпеки. Це включає видалення шкідливого ПЗ за допомогою антивірусного програмного забезпечення та інструментів для виявлення і видалення шкідливих програм [16], закриття вразливих портів та сервісів за допомогою інструментів для ідентифікації та

закриття вразливих портів і сервісів [15], а також оновлення програмного забезпечення шляхом встановлення останніх оновлень та патчів для усунення відомих вразливостей [17].

Після впровадження заходів безпеки необхідно забезпечити постійний моніторинг стану системи та вдосконалення заходів безпеки. Постійний моніторинг включає використання інструментів OSINT для виявлення нових загроз. Регулярне проведення аудитів безпеки дозволяє оцінити ефективність впроваджених заходів та виявити нові вразливості. Навчання персоналу через тренінги з питань кібербезпеки та реагування на інциденти є важливим елементом підвищення рівня безпеки.

Ефективне реагування на кіберзагрози також включає чітку комунікацію та звітність як всередині організації, так і з зовнішніми стейкхолдерами. Регулярне інформування керівництва про стан безпеки, виявлені загрози та вжиті заходи є критично важливим. Звітність перед регуляторами передбачає підготовку звітів для регуляторних органів, якщо це вимагається законодавством. Комунікація з клієнтами та партнерами передбачає інформування їх про заходи, вжиті для захисту їхніх даних та запобігання кіберзагрозам.

Стратегії реагування на кіберзагрози, виявлені за допомогою OSINT, включають комплекс заходів, спрямованих на оцінку загроз, планування дій, впровадження заходів безпеки, постійний моніторинг та вдосконалення, а також ефективну комунікацію та звітність. Використання сучасних інструментів OSINT дозволяє організаціям своєчасно виявляти та реагувати на загрози, забезпечуючи надійний захист своїх інформаційних систем.

3.2.2 Використання OSINT для запобігання кіберзагрозам

Open Source Intelligence (OSINT) є потужним інструментом для запобігання кіберзагрозам завдяки своїй здатності збирати, аналізувати та інтерпретувати інформацію з відкритих джерел. Використання OSINT

дозволяє організаціям проактивно виявляти потенційні загрози та вживати заходів для запобігання інцидентам до їхнього виникнення.

Одним із ключових методів запобігання кіберзагрозам за допомогою OSINT є постійний моніторинг та аналіз даних з відкритих джерел. Це включає використання інструментів, таких як SpiderFoot і theHarvester, для моніторингу соціальних медіа та форумів, де зловмисники можуть обговорювати плани атак або розповсюджувати шкідливе програмне забезпечення. Також використовуються інструменти, такі як Shodan і Censys, для сканування Інтернету з метою виявлення підключених пристроїв, їх конфігурацій та потенційних вразливостей.

Використання OSINT дозволяє виявляти вразливості в інформаційних системах до того, як зловмисники зможуть їх використати. Інструменти, такі як Maltego, застосовуються для аналізу зв'язків між різними компонентами системи та виявлення потенційних вразливостей. За допомогою Shodan можна виявити відкриті порти та сервіси, які можуть бути використані зловмисниками для атак, що дозволяє своєчасно закрити або захистити ці вразливі місця.

OSINT може бути використаний для виявлення підозрілої активності, що може свідчити про підготовку до кіберзагрози. Це включає моніторинг поведінки користувачів у соціальних медіа та на форумах для виявлення аномалій або підозрілих дій, що можуть вказувати на підготовку до атаки. Інструмент Censys використовується для виявлення підозрілих з'єднань з зовнішніми IP-адресами, що можуть свідчити про зловмисні дії.

OSINT дозволяє організаціям своєчасно отримувати попередження про нові загрози та тренди в кіберзлочинності. Дані з відкритих джерел використовуються для створення регулярних інформаційних бюлетенів та звітів про нові загрози та тенденції в кіберзлочинності, що допомагає організаціям бути в курсі останніх подій і вживати необхідних заходів для захисту. Важливою є також співпраця з іншими організаціями та обмін інформацією для виявлення та запобігання кіберзагрозам.

Освічений і підготовлений персонал є важливим елементом у запобіганні кіберзагрозам. Проведення регулярних тренінгів для співробітників з питань кібербезпеки та використання OSINT для виявлення та запобігання загрозам значно підвищує рівень безпеки. Організація внутрішніх інформаційних кампаній сприяє підвищенню обізнаності співробітників про актуальні кіберзагрози та методи їхнього запобігання.

Використання OSINT для запобігання кіберзагрозам є ефективним та важливим інструментом у сучасних стратегіях кібербезпеки. Постійний моніторинг, виявлення вразливостей, ідентифікація підозрілої активності, своєчасне попередження про нові загрози та навчання персоналу дозволяють організаціям проактивно захищати свої інформаційні системи та мінімізувати ризики кіберінцидентів.

3.2.3 Приклади успішного реагування на кіберзагрози з використанням OSINT

Використання OSINT (Open Source Intelligence) для реагування на кіберзагрози демонструє високу ефективність у багатьох реальних сценаріях. Нижче наведено декілька прикладів успішного реагування на кіберзагрози, де OSINT відіграв ключову роль.

Виявлення та нейтралізація фішингових кампаній стали успішним завданням для компанії, яка спеціалізується на кібербезпеці. Використовуючи Maltego, аналітики змогли виявити фішингову кампанію, яка цілилася на їхніх співробітників. Інструмент дозволив відстежити зв'язки між підозрілими електронними листами та доменами, що використовувалися для фішингу. Отримана інформація була передана відповідним службам, що призвело до блокування фішингових сайтів та затримання зловмисників. [14].

Захист фінансової установи від DDoS-атак був успішно забезпечений за допомогою використання OSINT. Вона використала інструменти Shodan і Censys для виявлення вразливих IoT-пристроїв у своїй мережі, які могли

потенційно бути використані для проведення DDoS-атак. Виявлені пристрої були належним чином налаштовані, що дозволило забезпечити їхню захищеність та запобігти їх використанню у майбутніх атаках [15].

Розслідування витоків даних у великій корпорації було успішно проведено за допомогою OSINT-інструменту theHarvester. Корпорація використала цей інструмент для збору інформації про можливі витоки через соціальні медіа та інші відкриті джерела. Це дозволило компанії швидко ідентифікувати джерело витоку, вжити необхідних заходів для його усунення та мінімізації шкоди. Крім того, були впроваджені додаткові заходи безпеки з метою попередження подібних інцидентів у майбутньому [17].

ІТ-компанія виявила шкідливе програмне забезпечення на своїх серверах завдяки використанню інструмента Censys. Цей інструмент дозволив ідентифікувати підозрілі з'єднання з зовнішніми IP-адресами. Після глибокого аналізу було виявлено шкідливе програмне забезпечення, яке було успішно видалено з системи компанією. Додатково, були впроваджені додаткові заходи для посилення моніторингу та захисту їхніх серверів [16].

Державна установа скористалася інструментом SpiderFoot для виявлення потенційних вразливостей у своїй інформаційній мережі. Інструмент автоматично збирав дані з різних джерел, включаючи пошукові системи та бази даних з вразливостями. Цей процес дозволив ідентифікувати кілька критичних вразливостей, які були оперативно усунені. Як результат, безпека установи значно зросла. [18].

Юридична фірма стикнулася з інцидентом витоку конфіденційних документів. Використовуючи інструмент FOCA, вони провели аналіз метаданих викрадених файлів, що дозволило встановити, як саме стався цей витік. Цей аналіз сприяв ідентифікації внутрішнього зловмисника, а також упровадженню необхідних заходів для захисту інших документів. Додатково, в організації були введені нові політики безпеки з метою попередження подібних інцидентів у майбутньому. [19].

Також OSINT можна використовувати і у більш простих задачах, наприкад вам зателефонували з незнайомого номера, (див. рисунок 3.11) і ви вагаєтесь хто це, чи це зловмисники, чи ні. Потрібно просто пошукати цей номер у просторах інтернету та соціальних мережах, (див. рисунок 3.12)

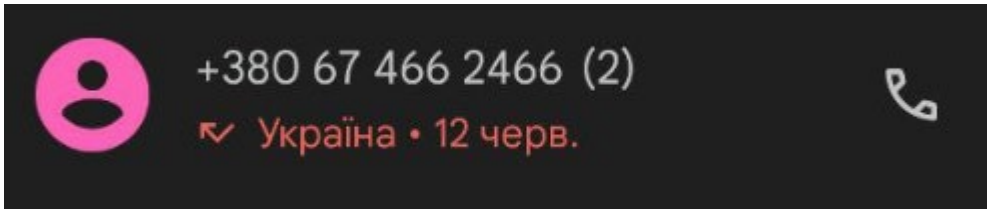

Рисунок 3.11 – Невідомий номер

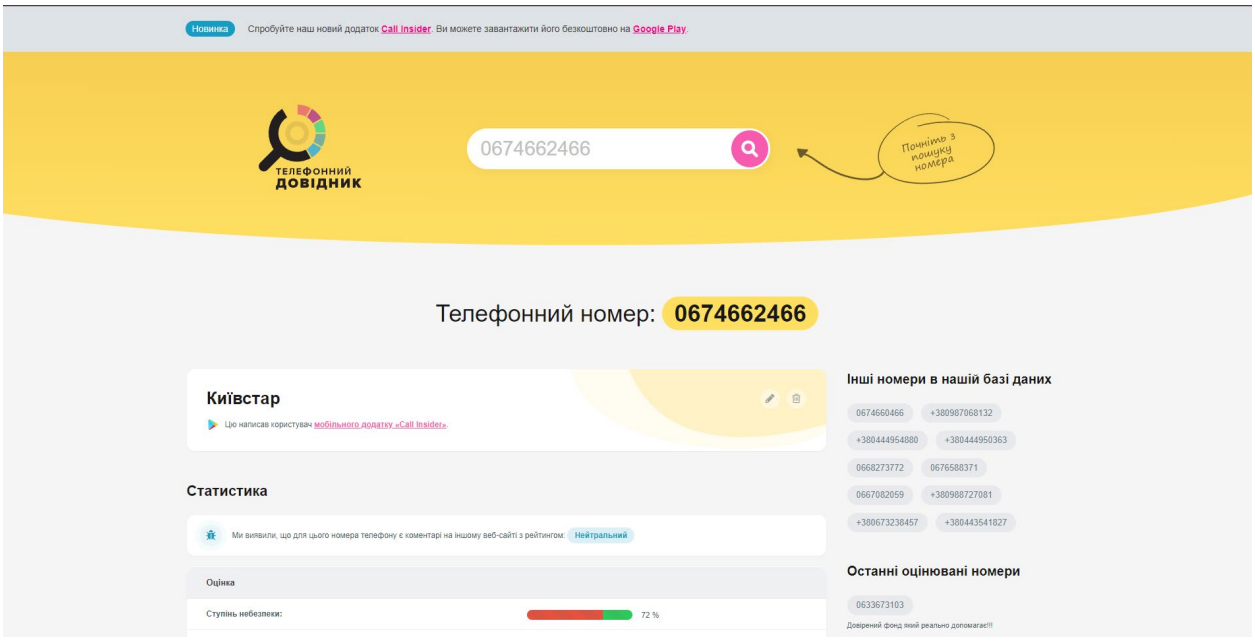

Рисунок 3.12 – Результати пошуку

Як можна побачити цей номер належить Київстар, почитавши відгуки інших користувачів можна зрозуміти чи варто вам передзвонювати, в даному випадку ні, оскільки у відгуках йдеться що це бот, (див. рисунок 3.13)

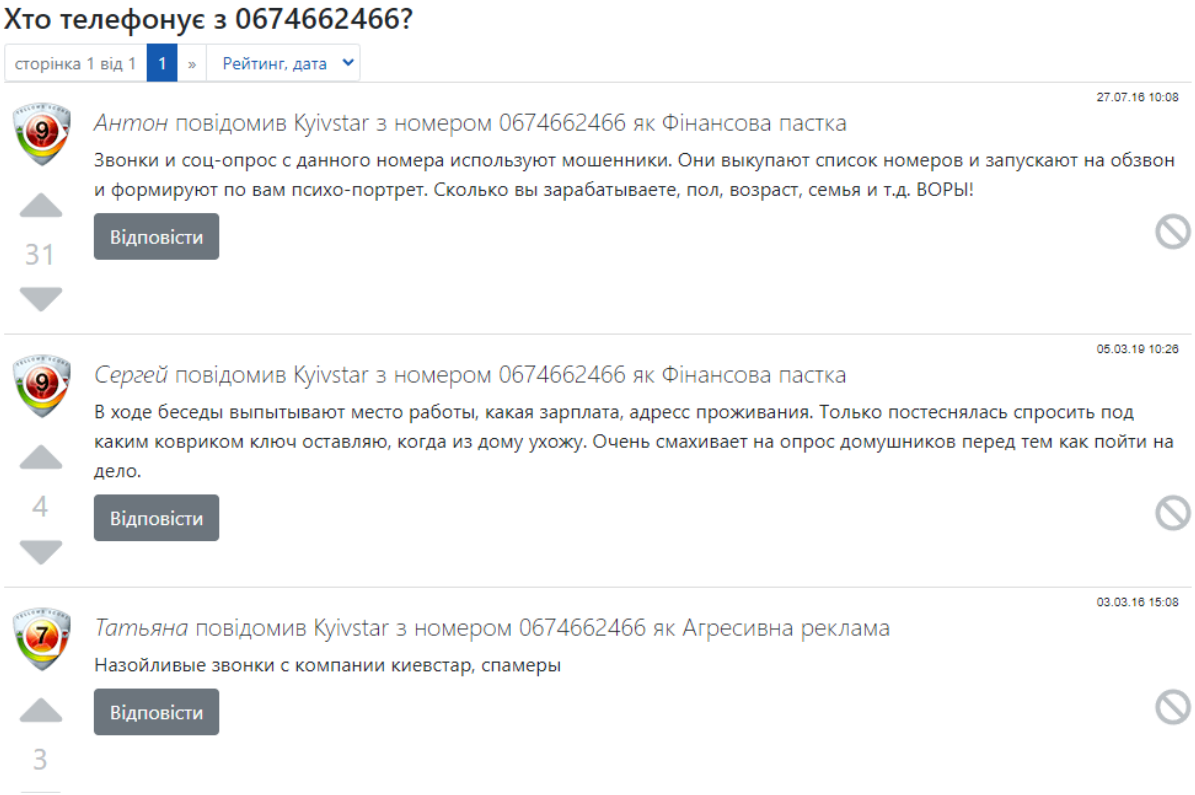

Рисунок 3.13 – Відгуки користувачів

Давайте розглянемо ще один приклад, спам листів на електронну пошту. Початок розслідування інциденту цього типу слід здійснювати з адреси електронної пошти відправника та його IP-адреси. Завантаживши лист на персональний комп'ютер та відкривши його в текстовому редакторі, можна виявити IP-адресу відправника або сервісу, через який здійснювалась відправка. Приклад відкритого листа показано на рисунку 3.14

```
        7gjVanyw2UdtlQgDIMB9/ZF8va48MxRw8nnYObilxkIwd0TCBCZasLzFGI7TPj2i9MtN
        umSw==
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20160816;
        h=date:message-id:list-unsubscribe:feedback-id:list-id:precedence
        :reply-to:mime-version:to:subject:from:dkim-signature;
        bh=Vbqpy6Dphevz6yS2gxqsEUYAGR5qF+tKt2kxgsr1r3o=;
        fh=WPPaW5E0OZUteDWN0PHExMxr3keXUQZv8Ne3QjLLEP0=;
        b=TeFX6CZBN57bYZaf/0kyu60b1IspYaBkiDA3NnKDuPoiE5FZzr92UGhEXLKLu8g6ge
        LmZzmMMpRl/unKqQjAgpw4M76yC7oVkNphiq67/VSciWLxjmYYk/ttp7GDlKSNDzG8A7
        lMQGIx4xDNGQc6MCXwjJk4e9bAkJ9r5pa26NpL6A1HgJ2CR8AzXerKNb2hV/oMe+eEf3
        eV7djcPVjhC64eacz+Im6TmqgdR10I+EvNlCDH091Zw3hn+ORI0bmLbMcN0uSSZz/j0J
        r0lxg0hGgK6LwnjHGsTs18p1h7yIXz88v7GaDR29tMCMEzRqyDCpgjTNn8Gxq1T8K2M8
        zPlA==;
        dara=google.com
ARC-Authentication-Results: i=1; mx.google.com;
       dkim=pass header.i=@dkim-vs01.justclick.ru header.s=default2 header.b=enHmp24y;
       spf=pass (google.com: domain of mta@mta0117.justclick.ru designates 148.251.149.17 as per
Return-Path: <mta@mta0117.justclick.ru>
Received: from mta0117.justclick.ru (mta0117.justclick.ru. [148.251.149.17])
        by mx.google.com with ESMTPS id ffacd0b85a97d-3607511e08bsi1874702f8f.383.2024.06.14.01.
        for <ivanmisterman@gmail.com>
        (version=TLS1_2 cipher=ECDHE-ECDSA-AES128-GCM-SHA256 bits=128/128);
        Fri, 14 Jun 2024 01:01:55 -0700 (PDT)
Received-SPF: pass (google.com: domain of mta@mta0117.justclick.ru designates 148.251.149.17 as
Authentication-Results: mx.google.com;
       dkim=pass header.i=@dkim-vs01.justclick.ru header.s=default2 header.b=enHmp24y;
       spf=pass (google.com: domain of mta@mta0117.justclick.ru designates 148.251.149.17 as per
Received: from justclick.ru (backend-02.justru.justclick.net.ru [94.26.231.225])
        by mta0117.justclick.ru (Postfix) with ESMTPA id 4W0sDy6p8cz1kNW8
        for <ivanmisterman@gmail.com>; Fri, 14 Jun 2024 11:01:54 +0300 (MSK)
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
        d=dkim-vs01.justclick.ru; s=default2; t=1718352115;
```

Рисунок 3.14 – Відкритий лист через блокнот

В листі можна побачити IP адресу відправника: 94.26.231.225. Застосовуючи інструмент “whois”, можна отримати інформацію про хостинг-провайдера, який обслуговує цей IP-адрес. Як можна побачити на рисунку 3.15 інформація про відправника зберігається в компанії «OOO Network of data-centers Selectel», а її сервери знаходять на території країни-агресора, а саме в місті Санкт-Петербург, індекс міста: 191015.

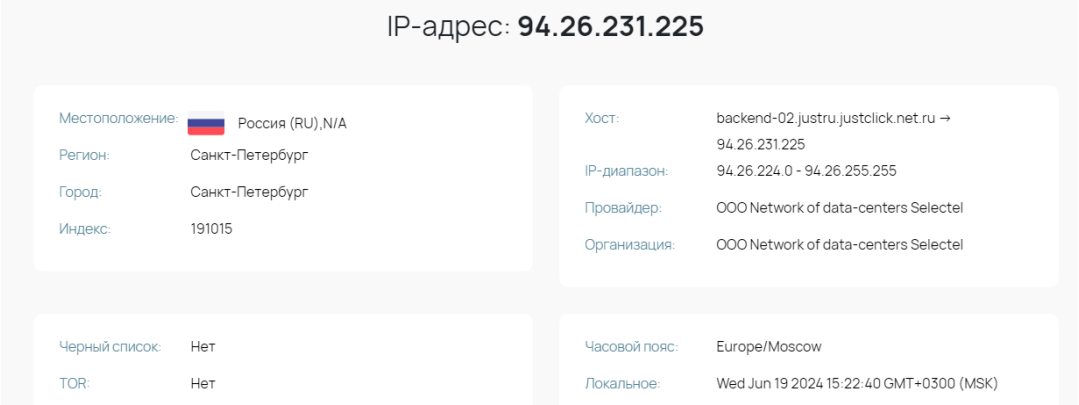

Рисунок 3.15 – Інформація про IP адрес відправника

Отже, завдяки використанню лише методів та інструментів OSINT, ми змогли встановити, через який сервіс було надіслано повідомлення та де зберігаються дані про відправника. Зібрана інформація, у разі звернення до правоохоронних органів, сприятиме швидшому розслідуванню справи та дозволить оперативно реагувати на подібні інциденти.

Ці приклади демонструють, як використання OSINT дозволяє ефективно реагувати на різноманітні кіберзагрози, від фішингових атак до виявлення вразливих пристроїв і розслідування витоків даних. Завдяки своїм можливостям зі збору та аналізу даних з відкритих джерел, OSINT допомагає організаціям своєчасно виявляти загрози та вживати необхідних заходів для їх нейтралізації.

3.3 Правові та етичні аспекти використання OSINT

3.3.1 Законодавчі обмеження та регулювання використання OSINT

Законодавчі обмеження та регулювання використання OSINT (Open Source Intelligence) є важливим аспектом для організацій, які використовують цей метод для виявлення та реагування на кіберзагрози. Використання інформації з відкритих джерел повинно здійснюватися у відповідності до правових норм і етичних стандартів, щоб уникнути порушення законодавства та прав осіб. У цьому розділі розглянемо основні законодавчі обмеження та регулювання, які стосуються використання OSINT у різних юрисдикціях.

Захист персональних даних є однією з ключових сфер регулювання використання OSINT. Закони, такі як GDPR (General Data Protection Regulation) в Європейському Союзі та CCPA (California Consumer Privacy Act) у Каліфорнії, встановлюють суворі вимоги щодо збору, обробки та зберігання персональних даних.

GDPR: Відповідно до GDPR, організації повинні забезпечити законність збору персональних даних, отримувати згоду від суб'єктів даних, а також надавати їм право на доступ, виправлення та видалення їхніх даних. Використання OSINT для збору персональних даних без належної згоди або без забезпечення захисту цих даних може призвести до значних штрафів [21].

CCPA: Згідно з CCPA, споживачі мають право знати, які їхні дані збираються, і вимагати видалення своїх даних. Організації повинні забезпечити можливість реалізації цих прав споживачів при використанні OSINT [22].

При використанні OSINT важливо враховувати закони про авторське право та інтелектуальну власність. Збір та використання інформації, захищеної авторським правом, повинні здійснюватися у відповідності до законодавства.

Закон про авторське право США: Використання матеріалів, захищених авторським правом, у дослідницьких цілях може підпадати під поняття "чесного використання" (fair use). Однак, організації повинні бути обережними, щоб не порушувати авторські права, особливо при публікації або поширенні зібраної інформації [23].

Окрім правових норм, використання OSINT повинно відповідати етичним стандартам. Це включає забезпечення конфіденційності та захисту прав суб'єктів даних, а також уникнення використання отриманої інформації для шкідливих цілей.

Багато організацій розробляють власні кодекси етики, які регламентують використання OSINT. Ці кодекси можуть включати правила щодо забезпечення конфіденційності, уникнення конфлікту інтересів та дотримання прав людини [11].

Багато країн мають специфічне законодавство, що регулює діяльність у сфері кібербезпеки, включаючи використання OSINT. Ці закони можуть включати вимоги щодо звітності, захисту даних та координації дій з державними органами.

Закон про кібербезпеку в США: Відповідно до Закону про кібербезпеку, компанії повинні звітувати про значні кіберінциденти до відповідних органів, а також дотримуватися стандартів захисту даних [24].

Директива NIS в ЄС: Директива NIS (Network and Information Systems Directive) встановлює вимоги до забезпечення кібербезпеки критичних інфраструктур та служб в Європейському Союзі. Це включає вимоги щодо звітності та співпраці з національними органами кібербезпеки [25].

Деякі види інформації можуть бути обмежені для доступу або використання через національну безпеку або інші законодавчі обмеження.

Закон про національну безпеку в США: Деякі види інформації можуть бути класифіковані як секретні, і їх збір або використання без належного дозволу є незаконним [26].

Законодавчі обмеження та регулювання використання OSINT є важливими для забезпечення законності та етичності цих дій. Організації, які використовують OSINT, повинні дотримуватися законів про захист персональних даних, авторське право, етичні стандарти, а також специфічних вимог у сфері кібербезпеки. Це допоможе уникнути правових проблем та забезпечити ефективний захист інформації.

3.3.2 Етичні питання у зборі та аналізі відкритих даних

Використання відкритих даних (Open Source Intelligence, OSINT) є цінним інструментом для організацій, але разом із цим виникають важливі етичні питання. Важливо дотримуватися певних етичних принципів, щоб забезпечити законність і моральність збору та аналізу інформації.

Організації повинні поважати конфіденційність і приватність осіб, чиї дані збираються. Це включає забезпечення захисту особистої інформації та отримання згоди на її обробку. Наприклад, згідно з GDPR, необхідно отримувати згоду від суб'єктів даних і надавати їм право на доступ, виправлення та видалення їхніх даних [21].

Збір та використання інформації не повинні завдавати шкоди особам або організаціям. Це означає, що отримані дані не можна використовувати для шантажу, дискримінації або будь-яких інших шкідливих цілей. Організації повинні розробляти політики, які регулюють етичне використання OSINT, щоб уникнути конфліктів інтересів та захистити права людини [11].

Організації, що займаються збором та аналізом відкритих даних, повинні діяти прозоро та нести відповідальність за свої дії. Це включає документування джерел інформації та забезпечення можливості перевірки зібраних даних. Також важливо повідомляти суб'єктів даних про те, як використовуються їхні дані, і забезпечувати дотримання їхніх прав на конфіденційність та захист інформації [22].

Дотримання правових норм є ключовим аспектом етичного використання OSINT. Наприклад, закони про авторське право, такі як Закон про авторське право США, регулюють використання захищених матеріалів і вимагають дотримання принципу "чесного використання" (fair use) при зборі даних для дослідницьких цілей [23]. . Також важливо дотримуватися законів про кібербезпеку, які регламентують звітність та захист даних при використанні OSINT [24].

3.3.3 Випадки порушення прав та конфіденційності при використанні OSINT

Використання відкритих даних (OSINT) може призвести до порушення прав та конфіденційності осіб, якщо не дотримуватися етичних та правових норм. Розглянемо деякі випадки таких порушень.

Одним із найпоширеніших порушень є незаконний збір та використання персональних даних без згоди суб'єктів даних. Згідно з GDPR, організації повинні забезпечити законність збору персональних даних та отримувати згоду від суб'єктів даних. Наприклад, компанія Cambridge Analytica незаконно

збирала дані з профілів користувачів Facebook без їхнього відома та згоди, що призвело до великого скандалу та правових наслідків.

Ще одним серйозним порушенням є використання зібраної інформації для шантажу або дискримінації. Така практика суперечить етичним стандартам і може призвести до значної шкоди для суб'єктів даних. Наприклад, витік персональних даних, зібраних з відкритих джерел, може використовуватися для шантажу або дискримінації окремих осіб, що порушує їхні права та конфіденційність.

Організації часто не забезпечують реалізацію прав суб'єктів даних на доступ, виправлення та видалення їхніх даних. Згідно з CCPA, споживачі мають право знати, які їхні дані збираються, і вимагати видалення своїх даних. У багатьох випадках компанії ігнорують ці вимоги, що призводить до порушення прав на конфіденційність.

Використання матеріалів, захищених авторським правом, без належного дозволу є порушенням закону. Згідно з Законом про авторське право США, використання таких матеріалів повинно відповідати принципу "чесного використання" (fair use). Однак, часто організації ігнорують ці вимоги, що призводить до порушення авторських прав та конфіденційності інформації.

3.4 Висновки до третього розділу

У цьому розділі було розглянуто різні аспекти застосування OSINT у контексті кібербезпеки. Методика проведення OSINT-досліджень включає чіткі кроки, які забезпечують ефективний збір та аналіз відкритих даних. Реальні приклади виявлення кіберзагроз за допомогою OSINT демонструють практичну цінність цього підходу та його здатність своєчасно ідентифікувати загрози.

Аналіз ефективності використання OSINT у конкретних випадках підтверджує, що цей інструмент є надзвичайно корисним для різних організацій. OSINT дозволяє не лише виявляти загрози, але й формувати

стратегії реагування на них. Використання OSINT для запобігання кіберзагрозам показує, що проактивний моніторинг і аналіз можуть значно знизити ризики та запобігти атакам. Приклади успішного реагування на кіберзагрози з використанням OSINT підкреслюють його ефективність у реальних умовах.

Однак, важливо також враховувати законодавчі обмеження та регулювання використання OSINT. Відповідність правовим нормам є критичним аспектом для забезпечення законності та етичності проведених досліджень. Етичні питання у зборі та аналізі відкритих даних також відіграють важливу роль, оскільки порушення прав та конфіденційності може мати серйозні наслідки. Випадки порушення прав та конфіденційності при використанні OSINT наголошують на необхідності дотримання етичних стандартів і правових норм.

4 БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ, ОСНОВИ ОХОРОНИ ПРАЦІ

4.1 Фактори, що впливають на функціональний стан користувачів комп'ютерів

Сьогодні намітилася тенденція неухильного росту кількості користувачів. Водночас все більш очевидною стає ймовірна небезпека для здоров'я людей, які працюють на ПЕОМ.

Дисплей становить основне джерело небезпеки, оскільки генерує випромінювання декількох типів: рентгенівське, інфрачервоне, ультрафіолетове, електромагнітне. Для кожного із зазначених типів випромінювання розробниками напрацьовані гранично допустимі норми, хоча вони є досить умовними й у кожній країні мають свої показники . відповідно до встановлених норм, особливу небезпеку становлять електромагнітне випромінення, від якого опромінюється не весь організм людини, а лише верхня частина людського тулуба. Зазначимо, що норми встановлені окремо з розрахунку на кожен вид опромінення, хоча по факту всі поля одночасно діють, а їх комплексний вплив на сьогодні остаточно науковцями не досліджено [27, С.115].

Також важливо згадати, що відеодисплейний термінал порушує рівновагу між позитивно і негативно зарядженими іонами повітря. Дисплей комп’ютера створює електростатичне поле, яке притягує до себе негативні іони, у такий спосіб порушуючи загальний баланс навколишнього середовища. Така дія є згубною людському здоров’ю. Вже через годину роботи біля монітора комп’ютера майже повністю зникають негативні іони. Через подібний вплив на організм потрібно, щоб у кабінет, де розміщений комп’ютер, проникало свіже повітря. Через дію згаданої дії та небезпеки при роботі за монітором комп’ютера чітко регламентуються розміри столу і стільця для фахівців, які постійно працюють з комп’ютером. Сидяча робота призводить до формування "закам’янілої" постави, яка шкідливо впливає на

скелетно-м’язову систему людини. Комп’ютерний стіл має бути просторим, із спеціальною підставкою для ніг, а робочий стілець повинен бути облаштований твердою спинкою, мати певний кут нахилу сидіння і спинки, а також відрегульовану висоту [28, С.86].

За передбаченими правилами, світло при роботі за монітором комп’ютера має падати зліва, а відстань від очей до екрана має становити приблизно 50 см. Крім того, крісло слід відрегулювати таким чином, щоб очі людини, яка сидить за комп’ютером, знаходилися на одному рівні з центром монітора пристрою. Медики зауважують, що при роботі з комп’ютером саме очі страждають найбільше.

Монітор комп’ютера створює бета-випромінювання, генероване потоком електронів, що спричинює іонізацію повітря в приміщенні [29, С.34]. Бета-випромінювання від монітора поширюється у двох основних напрямках - вперед і назад. На своєму шляху таке випромінювання вибиває електрони з молекул повітря, перетворюючи їх у позитивні іони, і у такий спосіб створює шкідливий для людини вплив. Сучасні монітори комп’ютерів мають незначний рівень бета-випромінювання, іншими словами, електрони поширюються за межі екрану лише на кілька сантиметрів.

При тривалій фіксації постави людини, будь-яка поза шкідлива для опорно-рухового апарату, призводить до застою крові в органах. Це особливо негативно проявляється при фізіологічному положенні різних частин тіла людини, яка працює за комп’ютером, і тривало, і систематично повторюваних одноманітних рухах. У процесі роботи за комп’ютером людина кілька годин поспіль сидить в незручному положенні. Це не лише загрожує втомою м’язів і загальною втомою, а й може спричинити розвиток остеохондрозу різних ділянок хребта: шийного, грудного, попереково-крижового [30, С.89].

У цьому контексті медики великого значення надають підтримці правильної пози під час роботи за комп’ютером. Важливим елементом профілактики захворювань є дотримання зазначеного правила. Щоб робота за

комп’ютером шкідливо не впливало на здоров’я людини, потрібно постійно стежити за власною поставою.

Прийнято вважати, що при правильній поставі людини, її вуха мають точно розташовуватися в площині плечей, а плечі - просто над стегнами. Голову потрібно рівно тримати щодо плечового поясу. При спрямуванні погляду вниз, голова не може нахилятися вперед.

При роботі в згорбленому положенні, навантаження на хребетний стовп людини суттєво зростає, що приводить до надмірного розтягування м’язів. Згорблене положення може стати причиною синдрому зап’ястного каналу, грижі міжхребцевих дисків поперекового і шийного відділів хребта.

Працюючи за екраном монітора, багато людей витягують вперед шию. Нерідко це пов’язано з тим, що монітор комп’ютера відсунутий занадто далеко. Через навантаження на м’язи голови і шиї утричі збільшується тиск, стискуються судини шиї, що веде до погіршення кровопостачання головного мозку. [31, С.156].

Надмірне навантаження на плечові сухожилки і м’язи плечового поясу викликає сутулість постави. Тривала робота в скутій і нахиленій позі може також призвести до розвитку защемлення плеча і виникнення синдрому зап’ястного каналу.

Встаючи із стільця чи крісла, на яких вимушено проводять значну частину часу на роботі і вдома, хребетний стовбур, суглоби разом з прикріпленими до них зв’язками і м’язами "звикають" до статичної пози, тому перехід у вертикальне положення потребує від людина, яка встає з місця, плавних і точних рухів, щоб структури опорно-рухового апарату, які встигли "застоятися" за довгий час, оперативно включилися в новий повноцінний режим роботи. [32, с.413].

З метою піднесення вологості повітря у приміщенні, де працюють комп’ютери, необхідно використовувати зволожувальні прилади. У кабінеті повинно бути природне і штучне освітлення. Основний потік природного світла має надходити зліва. На вікнах мають висіти завіси в два рази більші за

ширину віконного отвору. Не рекомендується використовувати чорні завіси для вікон [33, С.93].

Тривалість безперервної роботи за монітором комп’ютера без регламентованої перерви не має перевищувати понад 2 години.

Під час регламентної перерви з метою зниження нервово-емоційного напруження, стомлення зорового аналізатора, усунення впливу гіподинамії та гіпокінезії, запобігання розвитку познотопічної втоми доцільно виконувати комплекси вправ. Рівень шуму в приміщенні під час роботи комп’ютерів не повинен перевищувати 50 дБА [34, с.178].

Конструкція відеомонітора має враховувати необхідні заходи, які б забезпечували високу розбірливість зображення, що не залежить від зовнішнього освітлення приміщення.

Недотримання встановлених вимог щодо мікроклімату у приміщенні може не лише різко знижувати продуктивність праці зайнятих на виробництві, призвести до втрати робочого часу через збільшеного кількості помилок при виконанні процесів, але і приводити до функціональних розладів або хронічних захворювань нервової системи, органів дихання, імунної системи людини.

4.2 Охорона праці при надзвичайних ситуаціях

Охорона праці при надзвичайних ситуаціях — це система заходів, спрямованих на забезпечення безпеки та здоров'я працівників під час роботи в умовах надзвичайних ситуацій (НС). Надзвичайні ситуації можуть включати природні катастрофи, техногенні аварії, терористичні акти, епідемії тощо.

В Україні прийнята і діє Єдина державна система запобігання і реагування на надзвичайні ситуації природного і техногенного характеру та захист інформації.

У сучасному інформаційному суспільстві діюча Єдина державна система запобігання і реагування на надзвичайні ситуації техногенного та

природного характеру, центральні та місцеві органи виконавчої влади, виконавчі органи рад, державні підприємства, установи та організації з відповідними силами і засобами, які здійснюють нагляд за забезпеченням техногенної та природної безпеки, організовують проведення роботи із запобігання надзвичайним ситуаціям (НС) техногенного та природного походження і у разі їх виникнення негайного реагують з метою захисту населення і довкілля, зменшення матеріальних втрат.

ЄДС НС складається з постійно діючих функціональних і територіальних підсистем і має чотири рівні – загальнодержавний, регіональний, місцевий та об'єктовий. Функціональні підсистеми (ФП) створюються міністерствами та іншими центральними органами виконавчої влади для організації роботи пов'язаної із запобіганням надзвичайним ситуаціям та захистом територій і населення, що їх населяє, від негативних наслідків. У надзвичайних ситуаціях сили і засоби функціональних підсистем регіонального, місцевого та об'єктового рівня підпорядковуються в межах, що не суперечать законодавству, органам управління відповідних територіальних підсистем ЄДС НС [34, С.170].

Кожен рівень ЄДС надзвичайних ситуацій має координуючі та постійні органи управління, систему повсякденного управління, сили і засоби, резерви матеріальних та фінансових ресурсів, системи зв'язку та інформаційного забезпечення.

Основні аспекти охорони праці при надзвичайних ситуаціях:

Планування та підготовка включає розробку планів дій для надзвичайних ситуацій, таких як евакуація та надання першої допомоги. Працівники повинні бути професійно підготовлені до виконання визначених процедур у випадку надзвичайних обставин, включаючи використання засобів індивідуального захисту та орієнтацію на евакуаційних маршрутах. Регулярні тренування і навчання є необхідними для збереження високого рівня готовності працівників до дій в критичних ситуаціях.

Забезпечення засобами індивідуального захисту (ЗІЗ) передбачає виділення працівникам необхідних засобів захисту, таких як маски, рукавички та спецодяг, залежно від конкретної надзвичайної ситуації. Навчання персоналу використанню цих засобів є важливою частиною підготовки, щоб забезпечити їх ефективне застосування в умовах кризових ситуацій.

Інформаційне забезпечення включає встановлення систем оповіщення, які швидко інформують персонал про початок надзвичайних ситуацій. Наявність інформаційних матеріалів, таких як плакати і інструкції, з інформацією про дії під час надзвичайних подій, також грає важливу роль у підвищенні свідомості та готовності персоналу.

Організація медичної допомоги передбачає наявність аптечок першої допомоги та навчання працівників їх використанню. Регулярні медичні огляди працівників, зокрема тих, хто працює в умовах підвищеної небезпеки, також є частиною організаційних заходів для забезпечення безпеки та здоров'я персоналу.

Технічні заходи включають встановлення систем безпеки, таких як аварійне освітлення, вентиляція та пожежні сигналізації, щоб забезпечити безпеку працівників та обладнання. Регулярний технічний огляд та обслуговування обладнання є необхідним для запобігання аварійним ситуаціям та забезпечення надійності систем.

Психологічна підтримка включає забезпечення доступу до психологічної допомоги для працівників після надзвичайних ситуацій для зменшення стресу та психологічних наслідків подій.

Ефективна охорона праці при надзвичайних ситуаціях вимагає системного підходу, включаючи планування, навчання, забезпечення засобами захисту, інформаційне та медичне забезпечення. Це допомагає знизити ризики та мінімізувати наслідки надзвичайних ситуацій для здоров'я та життя працівників.

ВИСНОВКИ

У процесі виконання кваліфікаційної роботи було проведено комплексне дослідження значущості та методології використання OSINT (Open Source Intelligence) у сфері кібербезпеки. Було встановлено, що актуальність застосування OSINT зростає в умовах підвищеної кіберзагрози, оскільки цей інструмент дозволяє своєчасно виявляти та реагувати на потенційні загрози завдяки використанню відкритих джерел інформації.

Мета та завдання дослідження полягали у вивченні можливостей OSINT для виявлення та реагування на кіберзагрози, аналізі його інтеграції з іншими системами кібербезпеки, а також розробці методології ефективного застосування цього інструменту. Було детально описано об'єкт дослідження, яким є кіберзагрози та методи їх виявлення, а також предмет дослідження – можливості OSINT для забезпечення кібербезпеки.

У другому розділі розглянуто теоретичні основи OSINT, включаючи його історію, концептуальні основи, принципи та методи. Особлива увага була приділена ролі OSINT у виявленні кіберзагроз та його значенню в цьому процесі. Проведено огляд основних інструментів та платформ OSINT, їх можливостей та недоліків, що дозволило зробити висновки про ефективність та обмеження використання цих інструментів у реальних умовах.

Третій розділ присвячений практичному застосуванню OSINT, де було розглянуто методику проведення OSINT-досліджень, реальні приклади виявлення кіберзагроз та аналіз ефективності використання OSINT у конкретних випадках. Було визначено стратегії реагування на кіберзагрози, виявлені за допомогою OSINT, та розглянуто приклади успішного реагування на ці загрози. Окремо розглянуто правові та етичні аспекти використання OSINT, включаючи законодавчі обмеження, етичні питання та випадки порушення прав і конфіденційності.

Крім того, були змодельовані кілька ситуацій, у яких на практичних прикладах продемонстровано методи використання технологій OSINT. Це

дозволило наочно показати, як саме ці інструменти можуть застосовуватися для виявлення та нейтралізації кіберзагроз у реальних умовах, що підкреслює їхню ефективність і практичну цінність.

В результаті дослідження було підтверджено, що OSINT є ефективним інструментом для забезпечення кібербезпеки, який дозволяє виявляти та реагувати на кіберзагрози на ранніх стадіях. Однак, для максимального ефекту його застосування необхідно враховувати правові та етичні вимоги, а також забезпечувати постійний моніторинг та вдосконалення методів збору і аналізу даних. Зібрані результати та висновки можуть бути корисними для подальшого розвитку методології використання OSINT у кібербезпеці та підвищення загального рівня захисту інформаційних систем.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Conry-Murray A., Weafer V. The Symantec *Internet Security Threat Report*. Addison-Wesley Professional, 2023. 240 p.

2. Bazzell M. Open source intelligence techniques: Resources for searching and analyzing online information. 2018. 461 p.

3. Global Cybersecurity Index. *ITU*. URL: https://www.itu.int/gci (date of access: 23.06.2024).

4. OWASP Top Ten | OWASP Foundation. *OWASP Foundation, the Open Source Foundation for Application Security | OWASP Foundation*. URL: https://owasp.org/www-project-top-ten/ (date of access: 23.06.2024).

5. Tymoshchuk, V., Dolinskyi, A., & Tymoshchuk, D. (2024). MESSENGER BOTS IN SMART HOMES: COGNITIVE AGENTS AT THE FOREFRONT OF THE INTEGRATION OF CYBER-PHYSICAL SYSTEMS AND THE INTERNET OF THINGS. Матеріали конференцій МЦНД, (07.06. 2024; Луцьк, Україна), 266-267. https://doi.org/10.62731/mcnd-07.06.2024.004

6. Cost of a data breach 2023 | IBM. *IBM - United States*. URL: https://www.ibm.com/security/data-breach (date of access: 23.06.2024).

7. Snort. *Snort Intrusion Detection System*. URL: https://www.snort.org/ (date of access: 23.06.2024).

8. Демчук, В., Тимощук, В., & Тимощук, Д. (2023). ЗАСОБИ МІНІМІЗАЦІЇ ВПЛИВУ SYN FLOOD АТАК. Collection of scientific papers «SCIENTIA», (November 24, 2023; Kraków, Poland), 130-130.

9. Splunk | *Log Management and Analysis*. *Splunk*. URL: https://www.splunk.com/ (date of access: 23.06.2024).

10. What Is SIEM? - Security Information and Event Management. *Cisco*. URL: https://www.cisco.com/c/en/us/products/security/what-is-siem.html (date of access: 23.06.2024).

11. Іваночко, Н., Тимощук, В., Букатка, С., & Тимощук, Д. (2023). РОЗРОБКА ТА ВПРОВАДЖЕННЯ ЗАХОДІВ ЗАХИСТУ ВІД UDP FLOOD

АТАК НА DNS СЕРВЕР. Матеріали конференцій МНЛ, (3 листопада 2023 р., м. Вінниця), 177-178.

12. Ванца, В., Тимощук, В., Стебельський, М., & Тимощук, Д. (2023). МЕТОДИ МІНІМІЗАЦІЇ ВПЛИВУ SLOWLORIS АТАК НА ВЕБСЕРВЕР. Матеріали конференцій МЦНД, (03.11. 2023; Суми, Україна), 119-120.

13. Бекер, І., Тимощук, В., Маслянка, Т., & Тимощук, Д. (2023). МЕТОДИКА ЗАХИСТУ ВІД ПОВІЛЬНИХ ТА ШВИДКИХ BRUTE-FORCE АТАК НА IMAP СЕРВЕР. Матеріали конференцій МНЛ, (17 листопада 2023 р., м. Львів), 275-276.Homepage. Homepage. URL: https://www.paterva.com (date of access: 23.06.2024).

14. Homepage. *Homepage*. URL: https://www.paterva.com (date of access: 23.06.2024).

15. Ko Y. S., Ra I.-K., Kim C.-S. A Study on IP Exposure Notification System for IoT Devices Using IP Search Engine Shodan. *International Journal of Multimedia and Ubiquitous Engineering*. 2015. Vol. 10, no. 12. P. 61–66. URL: https://doi.org/10.14257/ijmue.2015.10.12.07 (date of access: 23.06.2024).

16. Exposure Management and Threat Hunting Solutions | Censys. *Censys*. URL: https://censys.io (date of access: 23.06.2024).

17. GitHub - laramies/theHarvester: E-mails, subdomains and names Harvester - OSINT. *GitHub*. URL: https://github.com/laramies/theHarvester (date of access: 23.06.2024).

18. Combat Cybercrime with Attack Surface Management. *Intel471*. URL: https://www.spiderfoot.net (date of access: 23.06.2024).

19. FOCA - Metadata and Information Gathering Tool [Електронний ресурс] // . ElevenPaths. – 2023. – Режим доступу до ресурсу: https://www.elevenpaths.com/technology/foca.

20. Recon-ng - Web Reconnaissance Framework [Електронний ресурс]. – 2023. – Режим доступу до ресурсу: https://github.com/lanmaster53/recon-ng.

21. European Parliament and Council. General Data Protection Regulation (GDPR).

22. California State Legislature. California Consumer Privacy Act (CCPA).

23. U.S. Copyright Office. Закон про авторське право США.

24. U.S. Congress. Закон про кібербезпеку в США.

25. European Parliament and Council. Директива NIS (Network and Information Systems Directive).

26. U.S. Congress. Закон про національну бзпеку в США.

27. Жидецький, В. І. Основи охорони праці / В. І. Жидецький – Л. : Афіша, 2005. – 349 с

28. Гандзюк, М. П. Основи охорони праці: підруч. / М. П. Гандзюк, Е. П. Желібо, М. О. Халимовський – К. : Каравела, 2005. – 393 с.

29. Григорьев, М. Кто выигрывает в масс-медиа войнах / М. Григорьев // Открытая политика. – 1999. – №3-4 (34). – С. 2-7.

30. Бедрій, Я. І. Охорона праці : навч. посіб. / Я. І. Бедрій. – Львів : Афіша, 1997. – 258 с.

31. Дурдинця, В. В. Збірник нормативно-правових актів з питань надзвичайних ситуацій техногенного та природного характеру / В. В. Дурдинця. – К. : Чорнобиль інтерінформ, 2001. – 532 с.

32. Ткачук, К. Н. Охорона праці та промислова безпека / Ткачук К. Н., Зацарний В. В., Сабарно Р. В. – К. : Лібра, 2010. – 560 с.

33. Рожков, А. П. Пожежна безпека : навч. довід. / А. П. Рожков. – К., 1999. – 256 с.

34. Теличко, Е. М. Міжнародне законодавство про охорону праці. Конвенції та рекомендації МОП у 3-х томах. Том 1 / Е. М. Теличко. – К. : «Основа», 1997. – 672 с.

35. Karpinski, M., Korchenko, A., Vikulov, P., Kochan, R., Balyk, A., & Kozak, R. (2017, September). The etalon models of linguistic variables for sniffing-attack detection. In 2017 9th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems : Technology and Applications (IDAACS) (Vol. 1, pp. 258-264). IEEE.

36. ZAGORODNA, N., STADNYK, M., LYPA, B., GAVRYLOV, M., & KOZAK, R. (2022). Network Attack Detection Using Machine Learning Methods. Challenges to national defence in contemporary geopolitical situation, 2022(1), 55-61.

37. Skarga-Bandurova, I., Biloborodova, T., Skarha-Bandurov, I., Boltov, Y., & Derkach, M. (2021). A Multilayer LSTM Auto-Encoder for Fetal ECG Anomaly Detection. Studies in health technology and informatics, 285, 147-152.