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)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

магістр
(назва освітнього ступеня)

на тему: Розробка OSINT інструменту для пошуку профілів в соціальних мережах

Виконав: студент II курсу, групи СБмз-61
спеціальності 125 Кібербезпека
(шифр і назва спеціальності)

(підпис) Сіткар Т.В. (прізвище та ініціали)

Керівник (підпис) Максимчук О. О. (прізвище та ініціали)

Нормоконтроль (підпис) Лечаченко Т.А. (прізвище та ініціали)

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

Рецензент (підпис) (прізвище та ініціали)

Тернопіль
2023

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)
«____» _____ 2023 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня Магістр
(назва освітнього ступеня)

за спеціальністю 125 Кібербезпека
(шифр і назва спеціальності)

Студенту Сіткар. Тарасу Вікторовичуч
(прізвище, ім'я, по батькові)

1. Тема роботи Розробка OSINT інструменту для пошуку профілів в соціальних мережах

Керівник роботи Максимчук Олександр Олександрович, асистент кафедри КБ
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від «_16_» _листопада__ 2023 року № _4/7-1060_____

2. Термін подання студентом завершеної роботи 10 грудня 2023р.

3. Вихідні дані до роботи Пошук профілю людини в соціальних мережах

4. Зміст роботи (перелік питань, які потрібно розробити):

1. Аналіз сучасного стану та особливостей використання технології OSINT в розвідувальних операціях у соціальних мережах
2. Розробка інструменту для автоматизованого збору інформації про користувачів соціальних мереж.
3. Визначення методології та алгоритмів ефективного пошуку профілів з використанням розробленого інструменту.
4. Аналіз сучасного стану та особливостей використання технології OSINT в розвідувальних операціях у соціальних мережах.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)

1 Титульна сторінка. 2 Об'єкт, предмет. 3. Мета. 4. Завдання. 5. Наукова новизна. 6. Приклади практичного застосування OSINT. 7. Популярні інструменти OSINT. 8. Найпопулярніші соціальні медіа-платформи та їхні специфічні OSINT-можливості. 9. Застосування API у розвідці за допомогою OSINT. 10. Плану пошуку з використанням OSINT. 11. Код для отримання доступу до списку фотографій за допомогою API. 12. Висновки

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Охорона праці	Осухівська Г.М., к.т.н., доцент		
Безпека в надзвичайних ситуаціях	Клепчик В.М., проректор з адміністративно-господарської роботи та будівництва		

7. Дата видачі завдання 16 листопада 2023 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1.	Ознайомлення з завданням до кваліфікаційної роботи	16.11.2023-17.11.2023	*Виконано*
2.	Підбір наукових джерел про OSINT	18.11.2023-20.11.2023	*Виконано*
3.	Переклад та опрацювання наукових джерел про		
	дослідження методів OSINT пошуку профілів в		
	соціальних мережах	21.11.2023-23.11.2023	*Виконано*
4.	Виконання дослідження щодо застосування методів		
	OSINT для пошуку профілів в соціальних мережах	24.11.2023-27.11.2023	*Виконано*
5.	Оформлення розділу «Технологія OSINT: аналіз та		
	застосування»	28.11.2023-30.11.2023	*Виконано*
6.	Оформлення розділу «Засоби реалізації технології		
	OSINT»	01.12.2023-04.12.2023	*Виконано*
7.	Оформлення розділу «Розробка інструменту на основі		
	OSINT для соціальних мереж»	05.12.2023-07.12.2023	*Виконано*
8.	Виконання завдання до підрозділу «Охорона праці»	08.12.2023-09.12.2023	*Виконано*
9.	Виконання завдання до підрозділу «Безпека в надзви-		
	чай них ситуаціях»	10.12.2023-11.12.2023	*Виконано*
10.	Оформлення кваліфікаційної роботи	12.12.2023-13.12.2023	*Виконано*
11.	Нормоконтроль	14.12.2023-15.12.2023	*Виконано*
12.	Перевірка на плагіат	09.12.2023	*Виконано*
13.	Попередній захист кваліфікаційної роботи	16.12.2023	*Виконано*
14.	Захист кваліфікаційної роботи	28.12.2023	

Студент _____ Сіткар Т.В.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Максимчук О. О.
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Розробка OSINT інструменту для пошуку профілів в соціальних мережах // Кваліфікаційна робота магістра // Сіткар Тарас Вікторович // ТНТУ, Кібербезпека та захист інформації, група СБмз-61 // Тернопіль, 2023 // с. - 63 , рис. - 6, табл. - 0, бібліографія - 39.

Ключові слова: OSINT, соціальні мережі, профілі, інструмент розвідки, технології інтернет-розвідки, API, Python.

Магістерська робота присвячена розробці інструменту на основі відкритих джерел інформації (OSINT) для пошуку профілів в соціальних мережах. У вступі роботи визначено актуальність теми та сформульовано основні завдання дослідження.

Проведено аналіз сучасного стану та застосування технології OSINT. Досліджено приклади практичного використання OSINT.

Розглядається популярні інструменти OSINT та їх використання у соціальних мережах та визначає ключові аспекти реалізації технології OSINT у вивченому контексті.

Описано застосування API для розвідки за допомогою OSINT, розроблено план пошуку та створено інструмент для використання в соціальних мережах. Висновки з цього розділу підкреслюють важливість розробки ефективних інструментів для використання OSINT.

Розглянуто поведінкові реакції населення в надзвичайних ситуаціях та запропоновані заходи для забезпечення безпеки праці в екстремальних умовах.

Магістерська робота пропонує вдосконалений інструмент для пошуку профілів в соціальних мережах, враховуючи актуальність та важливість технології OSINT у сучасному інформаційному середовищі.

ABSTRACT

Development of an OSINT tool for searching profiles in social networks // Master's thesis / Sitkar Taras V. // TNTU, Cybersecurity and Information Protection, group SBmz-61 // Ternopil, 2023 // p. - 63, fig. - 6, table - 0, bibliography - 39.

Keywords: OSINT, social networks, profiles, intelligence tool, Internet intelligence technologies, API, Python.

The master's thesis is devoted to the development of a tool based on open sources of information (OSINT) for searching profiles in social networks. In the introduction, the relevance of the topic is defined and the main research objectives are formulated.

The current state and application of OSINT technology is analysed. Examples of practical use of OSINT are studied.

Popular OSINT tools and their use in social media are considered and the key aspects of OSINT technology implementation in the context studied are identified.

The application of APIs for OSINT intelligence is described, a search plan is developed, and a tool for use in social media is created. The conclusions of this chapter emphasise the importance of developing effective tools for the use of OSINT.

The behavioural reactions of the population in emergency situations are considered and measures to ensure labour safety in extreme conditions are proposed.

The master's thesis proposes an improved tool for searching social media profiles, taking into account the relevance and importance of OSINT technology in the modern information environment.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

OSINT - Open source intelligence

ШІ – Штучний інтелект

API - application programming interface

URL - Uniform Resource Locator

ЗМІСТ

ВСТУП

Актуальність дослідження. В сучасному цифровому віці, де сучасні технології переплелися з усіма аспектами нашого життя, соціальні мережі стали нелише засобом спілкування, а й важливим ресурсом для отримання та обміну інформацією. Ростуча залежність від цифрового середовища покладає насамперед важливі завдання щодо забезпечення безпеки та захисту особистої інформації. У зв'язку з цим, розробка інструментів для пошуку профілів у соціальних мережах стає критичною вимогою в контексті кібербезпеки та розвідувальної діяльності.

Сучасні соціальні мережі, такі як Facebook, Instagram, X (Twitter) тощо, стали важливими платформами для обміну інформацією та побудови віртуальних спільнот. За допомогою цих платформ, мільйони користувачів з усього світу діляться своїми інтересами, здобутками та особистою інформацією. Однак в цьому океані особистих даних та віртуальних зв'язків існують потенційні загрози для безпеки та конфіденційності. Кіберзлочинці можуть використовувати ці дані для вчинення злочинів, шахрайства, чи інших небезпечних дій.

З урахуванням актуальності та важливості цієї теми, магістерська робота спрямована на розробку інструменту для ефективного та безпечного пошуку профілів у соціальних мережах з використанням технології OSINT (Open Source Intelligence). OSINT визначається як метод збору та аналізу відкритої інформації з відкритих джерел, і в контексті соціальних мереж може бути використана для створення повного та актуального зображення профілю користувача.

Об'єктом магістерської роботи є процеси та інструменти, пов'язані з вдосконаленням пошуку профілів у соціальних мережах за допомогою технології OSINT (Open Source Intelligence).

Предметом дослідження є розробка OSINT інструменту, спрямованого на ефективний та безпечний пошук профілів користувачів у різних соціальних мережах.

Метою (слайд 3) магістерської роботи є розробка та впровадження інструменту для систематизації та автоматизації пошуку профілів у соціальних мережах з використанням принципів OSINT.

Завдання (слайд 4) дослідження:

- Аналіз сучасного стану та особливостей використання технології OSINT в розвідувальних операціях у соціальних мережах.
- Розробка інструменту для автоматизованого збору інформації про користувачів соціальних мереж.
- Визначення методології та алгоритмів ефективного пошуку профілів з використанням розробленого інструменту.

Наукова новизна (слай 5) дослідження полягає в розробці OSINT інструменту для здійснення ефективного та безпечного пошуку профілів у соціальних мережах, що відповідає сучасним викликам кібербезпеки та розвідувальної діяльності.

Практичне значення. Результати даного дослідження можуть бути використані в сферах кібербезпеки, кримінального розслідування, а також в інших областях, де важлива розвідка в соціальних мережах для забезпечення безпеки та виявлення загроз.

Дана робота спрямована на підвищення ефективності та точності розвідки в соціальних мережах, що може внести значний вклад у сферу кібербезпеки та забезпечити кращий рівень захисту особистої інформації користувачів.

РОЗДІЛ І. ТЕХНОЛОГІЯ OSINT: АНАЛІЗ ТА ЗАСТОСУВАННЯ

1.1 Сучасний стан і застосування технології OSINT

В сучасному інформаційному суспільстві, де величезний обсяг даних неперервно формується та обмінюється в цифровому вигляді, технологія OSINT виявляється ключовою у забезпеченні доступу до відкритої інформації. Особливо це стосується сфери розвідки, кібербезпеки та аналізу великих обсягів даних. Розділ 1.1 присвячений детальному аналізу сучасного стану та різноманітних застосувань технології OSINT у цих контекстах.

Перед введенням в деталі аналізу сучасного стану технології OSINT, важливо розглянути та уточнити термінологічний аспект цієї технології. OSINT - це збір, аналіз та інтерпретація відкритої інформації з вільних джерел, доступних для будь-якого користувача. Це може включати в себе дані з відкритих джерел в Інтернеті, такі як соціальні мережі, публічні бази даних, новинні статті, та інші відкриті ресурси.

Технологія OSINT має широкий спектр застосувань у сфері розвідки та забезпечення безпеки. У розвідувальних операціях, вона використовується для збору великої кількості відкритої інформації про осіб, організації, або навіть держави. Аналіз соціальних мереж, форумів та інших відкритих платформ надає розвідникам можливість відстежувати зміни в громадському настрої, виявляти потенційні загрози та проводити аналіз публічних думок.

Важливим напрямком застосування технології OSINT є кібербезпека. Здатність аналізувати великі обсяги даних з відкритих джерел дозволяє ідентифікувати потенційні кіберзагрози, виявляти слабкі місця в інфраструктурі та вчасно реагувати на інциденти безпеки.

Однією з головних характеристик сучасного застосування технології OSINT є її вплив на глобальний інформаційний ландшафт. За допомогою цієї технології, будь-який користувач може отримати доступ до великої кількості інформації, що раніше може бути була недоступна або важкодоступна.

Однак, використання технології OSINT необхідно ретельно узгоджувати з етичними та правовими вимогами. Збір та аналіз відкритої інформації може порушити приватність осіб та породжувати етичні питання. Тому, розвиток та застосування цієї технології повинні бути здійснені в рамках визначених етичних та законних норм.

На тлі швидкого технологічного розвитку, технологія OSINT постійно трансформується та вдосконалюється. Динамічність цього напрямку дозволяє прогнозувати появу нових методів та інструментів для ще більш точного та комплексного аналізу відкритої інформації.

Результати аналізу свідчать про те, що технологія OSINT є невід'ємною частиною сучасного інформаційного простору. Вона не тільки забезпечує доступ до великого обсягу інформації, але й використовується у багатьох галузях, включаючи розвідку, кібербезпеку та аналіз глобальних тенденцій. Однак, важливо враховувати етичні та правові аспекти використання цієї технології для збереження балансу між можливостями та загрозами, які вона може нести.

Однією з ключових особливостей технології OSINT є здатність збору та аналізу великого обсягу даних з відкритих джерел. Серед таких джерел входять соціальні мережі, форуми, блоги, публічні бази даних, новинні портали, геопросторові сервіси та інші. Основною метою OSINT є використання цих даних для створення повного та об'єктивного зображення об'єкта розвідки.

Процес збору відкритої інформації може включати автоматизовані методи, такі як сканування веб-сайтів, використання API-інтерфейсів та

спеціалізованих інструментів. Збір даних здійснюється відкритими методами, доступними для будь-якого користувача, що дозволяє використовувати цю інформацію в різних контекстах, включаючи розвідку та кібераналітику.

У контексті розвідки, технологія OSINT виявляється дуже корисною для аналізу ситуаційної обстановки. Аналіз відкритої інформації з різних джерел, включаючи соціальні мережі, форуми та новинні портали, дозволяє виявляти зміни в громадському настрої, виявляти потенційні загрози та прогнозувати можливі події.

Особливу роль технологія OSINT відіграє у кризовому менеджменті та прогнозуванні кризових ситуацій. Здатність оперативно аналізувати дані з відкритих джерел дозволяє оперативним службам та розвідувальним організаціям отримувати інформацію про потенційні небезпеки та приймати швидкі та обґрунтовані рішення.

Ще одним важливим напрямком застосування технології OSINT є сфера кібербезпеки. Аналіз відкритої інформації може бути використаний для виявлення потенційних кіберзагроз, ідентифікації вразливостей у системах та аналізу методів кібератак.

Системи моніторингу соціальних мереж дозволяють виявляти вказівники можливих атак або злочинних дій. Використання технік OSINT у цій сфері дозволяє забезпечити вчасну реакцію на потенційні загрози та підвищити рівень безпеки кіберпростору.

OSINT також відіграє значущу роль у вивченні громадської думки та впливу на глобальний інформаційний ландшафт. Широкий доступ до відкритої інформації дозволяє виявляти тенденції у громадській думці, визначати реакції на події та аналізувати інші аспекти соціокультурного та політичного життя.

Аналіз громадської думки здійснюється через моніторинг соціальних мереж, дискусійних форумів та інших публічних платформ. Здатність

виявляти публічні настрої та тенденції стає важливим інструментом для визначення глобальних трендів та прогнозування можливих змін.

З несумлінним використанням технології OSINT пов'язані етичні та правові виклики. Збір та аналіз відкритої інформації може порушувати приватність осіб та викликати питання етики використання такої інформації.

Етичний аспект включає в себе обов'язок дотримуватися принципів справедливості та захисту особистої приватності під час збору та використання відкритої інформації. Правові вимоги стосуються використання інформації, отриманої з відкритих джерел, та вимагають дотримання законодавства щодо захисту даних та інших відповідних норм.

Технологічний розвиток та постійні зміни в інформаційному ландшафті безперервно визначають нові тенденції у сфері технології OSINT. Останні роки свідчать про стрімкий прогрес у цьому напрямі, включаючи вдосконалення методів збору, обробки та аналізу великих обсягів даних з різноманітних відкритих джерел.

Зростання обчислювальних можливостей та розвиток штучного інтелекту (ШІ) відкривають нові перспективи для технології OSINT. Автоматизація процесів збору та аналізу даних стає все більш важливою для ефективного використання цієї технології. Розвиток алгоритмів машинного навчання дозволяє створювати інтелектуальні системи, які можуть самостійно виявляти патерни та здійснювати аналіз великих обсягів даних, що в значній мірі підвищує точність та швидкість роботи з інформацією.

Розвиток Інтернету та поява нових віртуальних платформ призводять до зростання обсягу доступної інформації. Спільноти, форуми, блоги та інші онлайн-ресурси стають додатковими джерелами, які можна використовувати в рамках технології OSINT. Важливою тенденцією є

розширення зон доступу та вдосконалення інструментів для збору інформації з цих ресурсів.

Ще однією ключовою тенденцією є зростання використання геопросторової інформації в рамках технології OSINT. З розвитком систем навігації та геолокації в смартфонах і інших пристроях з'являється можливість аналізувати дані, пов'язані з конкретними географічними місцями. Це розширює спектр можливостей для виявлення певних зв'язків та отримання точної інформації.

У зв'язку з популярністю соціальних мереж, з'являються нові техніки та методи аналізу інформації, отриманої з цих джерел. Аналіз поведінки користувачів, вивчення соціальних зв'язків та використання алгоритмів для передбачення поведінки стають необхідними елементами сучасної технології OSINT.

Зростання уваги до кібербезпеки та приватності в Інтернеті викликає розробку технік та методів, спрямованих на захист особистої інформації в рамках технології OSINT. Розробка етичних стандартів та впровадження технічних рішень для захисту приватності користувачів стають актуальними завданнями.

Остання тенденція полягає в інтеграції технології OSINT з іншими інноваційними технологіями, такими як блокчейн, квантові обчислення та Інтернет Речей. Це відкриває нові можливості для створення більш безпечних та ефективних механізмів збору та обробки інформації.

Враховуючи глобальний характер технології OSINT, наближається час співробітництва та стандартизації в цій області. Розвиток міжнародних стандартів та спільних підходів до використання технології OSINT може значно полегшити обмін інформацією та забезпечити її більш ефективне використання.

Висновок з технологічного розвитку та тенденцій технології OSINT вказує на те, що цей напрямок не тільки залишається актуальним, але й

постійно розвивається відповідно до вимог сучасного інформаційного суспільства. Автоматизація, розширення джерел, використання ШІ та інші інновації стають тими факторами, які визначають майбутнє технології OSINT та її вплив на різні сфери життя.

1.2 Приклади практичного застосування OSINT

У даному розділі наведемо приклади, в яких методи розслідування з відкритих джерел були використані в реальному житті для розкриття злочину, виявлення підозрюваного, допомоги комусь, хто її потребує, виправдання підозрюваного або просто для демонстрації вражаючих можливостей, які можна отримати за допомогою цифрових розслідувань.

Ми не робитимемо жодних висновків про чиюсь вину чи невинність в даних прикладах, пов'язаних з кримінальними розслідуваннями, незалежно від того, винесено вирок чи ні.

Історія Маркуса Хатчинса

Розпочнемао з блискучого дослідження, проведеного Брайаном Кребсом з KrebsonSecurity про раннє життя молодого хакера на ім'я Маркус Хатчінс (Marucs Hutchins) (рис. 1.1). Хатчінс зазнав досить широкого розголосу в зв'язку з описаними тут подіями, але також отримав значну підтримку інтернет-спільноти завдяки тому, що він фактично самотужки врятував весь інтернет. І це без перебільшення. Ми також включили посилання на дуже ґрунтовне особисте інтерв'ю Маркуса, зроблене Wired [38], яке допоможе вам побачити іншу сторону цієї дійсно захоплюючої історії.

Рисунок 1.1 – Маркус Хатчінс

На початку серпня 2017 року агенти ФБР у Лас-Вегасі заарештували 23-річного британського дослідника безпеки Маркуса Хатчінса за підозрою в створенні та/або продажу "Кроноса" - шкідливого програмного забезпечення, призначеного для викрадення банківських облікових даних в Інтернеті. Хатчінс був практично невідомим для більшості фахівців з безпеки до травня 2017 року, коли британські ЗМІ представили його як "випадкового героя", який ненавмисно зупинив глобальне поширення WannaCry - вірусу-здирника з вимогою викупу, що захопив світ за кілька днів до того.

До його арешту про це мало хто знав, але Хатчінс багато років був автором популярного блогу про кібербезпеку MalwareTech. Коли цей факт став більш відомим - у поєднанні з його статусом героя за зупинку Wannacry - багато читачів MalwareTech швидко стали на його захист, щоб засудити його арешт. Вони стверджували, що урядова версія була побудована на хитких і мізерних доказах, зазначаючи, що Хатчінс невтомно працював над викриттям кіберзлочинців та їхніх шкідливих інструментів. На сьогоднішній день близько 226 прихильників пожертвували понад 14 000 доларів до його фонду захисту.

Спочатку ми не вірили, що звинувачення, висунуті проти Хатчінса, витримають ретельну перевірку. Але коли ми почали заглиблюватися в історію, пов'язану з десятками псевдонімів на хакерських форумах, адресами електронної пошти та доменами, які він, очевидно, використовував протягом останнього десятиліття, почала вимальовуватися зовсім інша картина [39].

Як ФБР вистежило ймовірного підпалювача Лор-Елізабет

Ця історія зосереджена на використанні інформації з відкритих джерел, яка привела ФБР до підозрюваного в підпалі (рис. 1.2). На цей слід може натрапити будь-хто, а використаний тут поворот є чудовим прикладом встановлення зв'язків, необхідних для відстеження об'єкта, в даному випадку - футболки, яку носив підозрюваний.

Рисунок 1.2 - Лор-Елізабет Блюменталь

Ось як ФБР викрило жінку, звинувачену в підпалі поліцейських машин у Філадельфії

Мабуть, Ви чули, як агенти ФБР ідентифікували агітаторку, яку звинувачують у підпалі двох поліцейських машин у Філадельфії під час заворушень? Можна сказати, хороша "новомодна" робота поліції.

Серед доказів, зібраних агентами ФБР, були кадри новин про заворушення 30 травня 2023 року, а також близько 500 фотографій, зроблених фотографом-аматором.

На фотографіях було зображено жінку, яка жбурляє палаючий шматок барикади в поліцейський позашляховик, припаркований біля мерії Філадельфії.

На жінці були вогнетривкі рукавички, захисні окуляри та синя футболка з написом "ТРИМАЙТЕ ІММІГРАНТІВ, ДЕПОРТУЙТЕ РАСИСТІВ".

Вона купила цю футболку не в супермаркеті. Вона була пошита на замовлення і продана на Etsy, де користувач під ніком "Xx Mv" залишив про неї відгук, згідно зі скаргою ФБР, поданою до Окружного суду США у Філадельфії.

Вона поставила йому п'ять зірок ("швидка доставка, велике спасибі"), йдеться у скарзі.

URL-адреса цього облікового запису ("alleycatlore") вказувала на те, що користувач проживає у Філадельфії, йдеться у федеральній скарзі.

Застосовуючи ще більш примітивні методи розслідування, агенти загуглили "alleycatlore" і знайшли користувача на ім'я Lore-Elisabeth на Poshmark, йдеться у скарзі.

Вони також знайшли сторінку в Instagram з фотографією палія в масці і характерним татуюванням у вигляді знаку миру на її правому передпліччі (рис. 1.3).

Рисунок 1.3 – Фото з Instagram

Ще один простий пошук - "Лора-Елізабет Філадельфія" - виявив сторінку в мережі LinkedIN жінки, яка працює масажисткою в одній з компаній у Філадельфії, йдеться у скарзі (згодом її було видалено).

У компанії є акаунт на Vimeo з відеозаписами жінки з таким самим татуюванням, йдеться у скарзі.

На вимогу суду продавець футболки надав документи, які підтверджують, що "Xx Mv" придбала цю футболку, йдеться у скарзі.

Футболка була відправлена жінці у Філадельфії, чиє фото на водійських правах збігалося з фотографією жінки на відео з Vimeo, йдеться у скарзі.

Агенти ФБР швидко розшукали 33-річну Лор-Елізабет Блюменталь, взяли її під варту і висунули звинувачення у двох випадках підпалу.

За словами представників влади, вона не прийшла мирно, відмовившись впустити їх у будинок, де вона перебувала, і намагалася втекти.

Врешті-решт агенти виламали двері та схопили Блюменталь, яка боролася і кричала, повідомили вони.

Під час обшуку в будинку були знайдені рукавички, окуляри і рюкзак, які були на палії, йдеться в їхній скарзі.

Федеральний суддя постановив утримувати Блюменталя під вартою без права на заставу.

Прокурор США Вільям М. МакСвейн написав у твіттері: "Усі, хто вносив кошти у фонд застави, тепер можуть вимагати повернути свої гроші".

Блюменталь загрожує обов'язковий мінімум семирічний термін у федеральній в'язниці - і, можливо, набагато більше - на додаток до штрафів і звільнення під наглядом, якщо її визнають винною у підпалі. У федеральній тюремній системі немає умовно-дострокового звільнення.

"Розслідування внутрішньої безпеки повністю поважає право всіх людей висловлювати свою думку без втручання, в тому числі шляхом мирних зібрань і протестів", - заявив Брайан А. Майкл, спеціальний агент, відповідальний за роботу федерального офісу розслідувань внутрішньої безпеки у Філадельфії.

"На жаль, деякі протестувальники вдалися до насильства, що призвело до руйнування майна по всій Філадельфії", - сказав Майкл. "У таких випадках HSI тісно співпрацює з федеральними, державними та місцевими правоохоронними органами, щоб забезпечити притягнення до відповідальності тих, хто завдає шкоди, яка впливає на безпеку нашої громади".

Великий злом Twitter

Використовуючи поєднання соціальної інженерії та технічних ноу-хау, кількох підозрюваних звинуватили у зламі твіттера та розміщенні афери з біткоїнами від імені одних з найвідоміших у світі людей. І знову

Брайан Кребс з KrebsonSecurity з детальним описом того, як були ідентифіковані підозрювані, і подальшою статтею про арешт.

Twitter був вкинутий в хаос після того, як акаунти деяких найбільш впізнаваних світових громадських діячів, керівників і знаменитостей почали публікувати посилання на біткоїн-шахрайство. Twitter заявляє, що атака сталася через те, що хтось обманом або примусом змусив співробітника надати доступ до інтернету з середини компанії.

Трьом особам були пред'явлені звинувачення за їхню ймовірну роль у зламі Twitter 15 липня 2023 року, в результаті якого профілі деяких найвідоміших світових знаменитостей, керівників і громадських діячів у Twitter почали розсилати твіти з рекламою біткойн-шахрайства.

Архіви OSINT-розслідувань InformNapalm

Ця сторінка може зайняти вас на все життя. Учасники InformNapalm зібрали разом понад 2000 фантастичних OSINT-розслідувань як "волонтерську розвідувальну спільноту, що представляє свою інтерактивну базу даних, яка відображає російську агресію проти України, а також Грузії та Сирії". Тут зібрані дійсно чудові матеріали, що охоплюють різні OSINT-дисципліни.

РОЗДІЛ 2. ЗАСОБИ РЕАЛІЗАЦІЇ ТЕХНОЛОГІЇ OSINT

2.1 Популярні інструменти OSINT

Розвідка з відкритих джерел (OSINT) - це практика збору інформації з опублікованих або інших загальнодоступних джерел. Операції OSINT, незалежно від того, чи проводяться вони фахівцями з IT-безпеки, зловмисними хакерами або санкціонованими державою оперативниками розвідки, використовують передові методи для пошуку у величезному стосі видимих даних, щоб знайти голки, які вони шукають для досягнення своїх цілей.

OSINT багато в чому є дзеркальним відображенням операційної безпеки (OPSEC) - процесу безпеки, за допомогою якого організації захищають публічні дані про себе, які при належному аналізі можуть виявити шкідливу правду. Внутрішні команди безпеки проводять OSINT-операції у своїх організаціях, щоб зміцнити операційну безпеку. Вони намагаються знайти конфіденційну інформацію, про яку компанія може не знати, що вона є публічною. Це дозволяє їм захистити вразливі дані або передбачити, яку інформацію про організацію може мати зловмисник. Ця інформація має вирішальне значення при оцінці ризиків, визначенні пріоритетності ресурсів безпеки, а також при вдосконаленні практик і політик безпеки.

Відкритий код у цьому контексті не стосується руху за відкрите програмне забезпечення, хоча багато інструментів OSINT мають відкритий код. Замість цього він описує публічний характер даних, що аналізуються.

У 1980-х роках військові та розвідувальні служби почали зміщувати акценти у своїй діяльності зі збору інформації від таємних дій, таких як спроби прочитати пошту супротивника або прослуховування його телефонів, щоб дізнатися приховані секрети. Замість цього зусилля були

спрямовані на пошук корисних розвідувальних даних, які були у вільному доступі або навіть офіційно опубліковані.

Світ у той час змінювався, і хоча соціальні мережі ще не вийшли на сцену, було багато джерел, таких як газети та загальнодоступні бази даних, які містили цікаву, а іноді й корисну інформацію, особливо якщо хтось знав, як з'єднати багато крапок над "і". Термін OSINT спочатку був придуманий для позначення цього виду шпигунства.

Ці ж методи тепер можна застосувати до кібербезпеки. Більшість організацій мають величезні публічні інфраструктури, які охоплюють безліч мереж, технологій, хостингових сервісів і просторів імен. Інформація може зберігатися на робочих столах співробітників, на застарілих локальних серверах, на пристроях, що належать співробітникам, у хмарі, вбудована в пристрої, такі як веб-камери, або навіть прихована у вихідному коді активних додатків і програм.

Насправді, співробітники служби безпеки та IT-спеціалісти великих компаній майже ніколи не знають про кожен актив на своєму підприємстві, незалежно від того, публічний він чи ні. Додайте до цього той факт, що багато організацій також володіють або опосередковано контролюють кілька додаткових активів, наприклад, свої акаунти в соціальних мережах, і ви отримаєте потенційно велику кількість інформації, яка може бути небезпечною в чужих руках.

OSINT має вирішальне значення для відстеження цього інформаційного хаосу. IT-спеціалісти повинні виконувати три важливі завдання в рамках OSINT, і для задоволення цих потреб було розроблено широкий спектр інструментів OSINT. Більшість інструментів виконують усі три функції, хоча багато з них досягають успіху в одній конкретній сфері.

Найпоширеніша функція - допомогти IT-командам виявити загальнодоступні ресурси та визначити, якою інформацією володіє кожен з

них, що може стати потенційним об'єктом атаки. Їхнє основне завдання - фіксувати інформацію, яку хтось може дізнатися про активи компанії, не вдаючись до злому, не шукаючи вразливості в програмах і не проводячи тестування на проникнення.

Другорядною функцією, яку виконують деякі інструменти OSINT, є пошук потрібної інформації за межами організації, наприклад, у публікаціях в соціальних мережах або на доменах і локаціях, які можуть знаходитися за межами чітко визначеної мережі. Ця функція може виявитися дуже корисною для організацій, які здійснили багато придбань, прихопивши з собою IT-активи компанії, з якою вони зливаються. Враховуючи надзвичайне зростання і популярність соціальних мереж, пошук конфіденційної інформації за межами периметру компанії, ймовірно, буде корисним практично для будь-якої групи.

Нарешті, деякі інструменти OSINT допомагають зібрати і згрупувати всю знайдену інформацію в корисні та дієві розвідувальні дані. Запуск OSINT-сканування для великого підприємства може дати сотні тисяч результатів, особливо якщо охопити як внутрішні, так і зовнішні ресурси. Зібрати всі ці дані воєдино і мати можливість вирішити найсерйозніші проблеми в першу чергу може бути надзвичайно корисно.

Використання правильного інструменту OSINT для вашої організації може покращити кібербезпеку, допомагаючи виявити інформацію про вашу компанію, співробітників, IT-активи та інші конфіденційні або чутливі дані, які можуть бути використані зловмисником. Виявлення цієї інформації, а потім її приховування або видалення, може зменшити ризики від фішингу до атак типу "відмова в обслуговуванні" (DoS). Професіонали, які регулярно виконують OSINT-операції, часто використовують набір інструментів, залежно від середовища та вподобань.

Нижче (в довільному порядку) перераховані деякі з найпопулярніших інструментів, що використовуються для OSINT, області, в яких вони

спеціалізуються, чому вони унікальні і відрізняються один від одного, і яку конкретну цінність вони можуть принести зусиллям організації в області кібербезпеки.

- Maltego
- Mitaka
- SpiderFoot
- Spyse
- BuiltWith
- Intelligence X
- DarkSearch.io
- Grep.app
- Recon-ng
- theHarvester
- Shodan
- Metagoofil
- Searchcode
- SpiderFoot
- Babel X

Maltego

Maltego спеціалізується на виявленні зв'язків між людьми, компаніями, доменами та загальнодоступною інформацією в Інтернеті. Вона також відома тим, що бере величезні обсяги знайденої інформації і відображає їх у зручних для читання діаграмах і графіках. Графіки добре справляються із завданням перетворення необробленої інформації на практичні дії, і кожен графік може містити до 10 000 точок даних.

Програма Maltego працює шляхом автоматизації пошуку в різних відкритих джерелах даних, тому користувачі можуть натиснути на одну кнопку і виконати кілька запитів. План пошуку в програмі називається

"дією перетворення", і за замовчуванням Maltego постачається з багатьма з них, які включають поширені джерела публічної інформації, такі як записи DNS, записи whois, пошукові системи та соціальні мережі. Оскільки програма використовує загальнодоступні інтерфейси для пошуку, вона сумісна майже з будь-яким джерелом інформації, що має загальнодоступний інтерфейс, тому можна легко додати більше пошукових запитів до дії перетворення або створити абсолютно нову дію.

Після того, як інформація зібрана, Maltego встановлює зв'язки, які можуть виявити приховані зв'язки між іменами, електронними адресами, псевдонімами, компаніями, веб-сайтами, власниками документів, зв'язками та іншою інформацією, яка може виявитися корисною в розслідуванні або для пошуку потенційних майбутніх проблем. Сама програма працює на Java, тому вона працює з платформами Windows, Mac і Linux.

Існує безкоштовна версія програми з обмеженими можливостями під назвою Maltego CE. Настільні версії Maltego XL коштують $1,999 за екземпляр. Серверні інсталяції для масштабного комерційного використання починаються від $40,000 і поставляються з повною навчальною програмою.

Mitaka

Доступний у вигляді розширення для Chrome і доповнення для Firefox, Mitaka дозволяє шукати IP-адреси, домени, URL-адреси, хеші, ASN, адреси біткойн-гаманців і різні індикатори компрометації (IOC) у більш ніж шести десятках пошукових систем з вашого веб-браузера. Ax Sharma

Розширення економить ваш час, діючи як ярлик до різних онлайн-баз даних, які можна запитувати одним кліком.

Для тих, хто віддає перевагу сфокусованому, більш обмеженому набору, також доступне альтернативне розширення Sputnik.

Spiderfoot

Spiderfoot - це безкоштовний інструмент OSINT-розвідки, який інтегрується з різними джерелами даних для збору та аналізу IP-адрес, діапазонів CIDR, доменів і субдоменів, ASN, адрес електронної пошти, номерів телефонів, імен та імен користувачів, адрес BTC тощо. Доступний на GitHub, Spiderfoot поставляється як з інтерфейсом командного рядка, так і з вбудованим веб-сервером для забезпечення інтуїтивно зрозумілого веб-графічного інтерфейсу.

Сама програма має понад 200 модулів, що робить її ідеальним інструментом для розвідувальної діяльності, щоб дізнатися більше інформації про вашу ціль або виявити, що ви або ваша організація могли ненавмисно виставити в Інтернеті.

Spyse

Spyse описує себе як "найповніший реєстр інтернет-активів", орієнтований на фахівців з кібербезпеки. Спираючись на такі проекти, як OWASP, IntelligenceX та вищезгаданий Spiderfoot, Spyse збирає загальнодоступні дані про веб-сайти, їхніх власників, пов'язані з ними сервери та пристрої Інтернету речей. Потім ці дані аналізуються механізмом Spyse, щоб виявити будь-які ризики для безпеки та зв'язки між цими різними об'єктами.

Доступний безкоштовний план, хоча для розробників, які планують створювати додатки з використанням API Sypse, може знадобитися платна підписка.

BuiltWith

Як випливає з назви, BuiltWith дозволяє знайти, на чому побудовані популярні веб-сайти. Різні технологічні стеки та платформи працюють на різних сайтах. Наприклад, BuiltWith може визначити, чи використовує веб-сайт WordPress, Joomla або Drupal в якості CMS, і надати додаткову інформацію.

BuiltWith також генерує чіткий список відомих бібліотек JavaScript/CSS (наприклад, jQuery або Bootstrap), які використовує веб-сайт. Крім того, сервіс надає список плагінів, встановлених на веб-сайтах, фреймворків, інформацію про сервер, аналітику та інформацію для відстеження тощо. BuiltWith можна використовувати в розвідувальних цілях.

Що ще? Поєднуйте BuiltWith зі сканерами безпеки веб-сайтів, такими як WPScan, які, наприклад, інтегруються з WordPress Vulnerability Database API, щоб виявити типові вразливості безпеки, що впливають на веб-сайт.

Для тих, хто хоче визначити переважно технічний стек сайту, краще підійде Wappalyzer, оскільки він надає більш сфокусовані та стислі результати. Спробуйте і BuiltWith, і Wappalyzer, щоб зрозуміти, який з них краще відповідає вашим потребам.

Intelligence X

Intelligence X - це перший у своєму роді архівний сервіс і пошукова система, яка зберігає не тільки історичні версії веб-сторінок, але й цілі набори даних, які в іншому випадку видаляються з Інтернету через неприйнятний характер контенту або з юридичних причин. Хоча це може здатися схожим на те, що робить Wayback Machine від Internet Archive, Intelligence X має деякі суттєві відмінності, коли мова йде про тип контенту, на збереженні якого сервіс зосереджується. Коли йдеться про збереження наборів даних, якими б суперечливими вони не були, Intelligence X не робить різниці.

Раніше Intelligence X зберігав список з понад 49 000 VPN-мереж Fortinet, які були визнані вразливими до уразливості Path Traversal. Пізніше протягом тижня на хакерських форумах також були опубліковані відкриті паролі до цих VPN, які, знову ж таки, хоча і були видалені з цих форумів, але були збережені Intelligence X.

Раніше сервіс індексував дані, зібрані з поштових серверів відомих політичних діячів, таких як Гілларі Клінтон і Дональд Трамп. Іншим нещодавнім прикладом медіа, проіндексованих на Intelligence X, є кадри заворушень на Капітолійському пагорбі у 2021 році та витік даних 533 мільйонів профілів у Facebook. Для збирачів розвідданих, політичних аналітиків, репортерів та дослідників безпеки така інформація може бути неймовірно цінною в різних аспектах.

DarkSearch.io

Хоча постійні відвідувачі темного інтернету вже можуть бути знайомі з тим, де і що шукати, для тих, хто є новачком, DarkSearch.io може стати гарною платформою для початку дослідницької діяльності. Як і інша пошукова система темного інтернету Ahmia, DarkSearch є безкоштовною, але постачається з безкоштовним API для запуску автоматизованого пошуку. Хоча і Ahmia, і DarkSearch мають сайти в домені .onion, вам не обов'язково переходити на версії .onion або використовувати Tor для доступу до будь-якої з цих пошукових систем. Достатньо зайти на darksearch.io зі звичайного веб-браузера і ви зможете шукати в темній павутині.

Grep.app

Як шукати серед півмільйона git-репозиторіїв в інтернеті? Звичайно, ви можете спробувати окремі пошукові рядки на GitHub, GitLab або BitBucket, але Grep.app робить цю роботу надзвичайно ефективно. Насправді, Grep.app нещодавно неодноразово використовувався користувачами Twitter і журналістами, щоб отримати уявлення про те, скільки репозиторіїв використовують Codecov Bash Uploader:

Grep.app також може бути корисним при пошуку рядків, пов'язаних з IOC, вразливим кодом або шкідливим програмним забезпеченням (наприклад, Octopus Scanner, Gitpaste-12 або зловмисні криптомайнінгові PR-повідомлення GitHub Action), що ховаються в репозиторіях OSS.

Recon-ng

Розробники, які працюють на Python, мають доступ до потужного інструменту Recon-ng, написаного цією мовою. Його інтерфейс дуже схожий на популярний Metasploit Framework, що має скоротити час навчання для тих, хто вже має досвід роботи з ним. Він також має функцію інтерактивної довідки, якої бракує багатьом модулям Python, тому розробники зможуть швидко її освоїти.

Recon-ng автоматизує трудомісткі дії в OSINT, такі як вирізання та вставка. Recon-ng не претендує на те, що за допомогою його інструменту можна виконувати всі операції зі збору OSINT, але він може бути використаний для автоматизації більшості найпопулярніших видів збору, залишаючи більше часу для речей, які все ще доводиться робити вручну.

Розроблений таким чином, що навіть наймолодші розробники Python можуть створювати пошуки загальнодоступних даних і отримувати хороші результати, він має дуже модульний фреймворк з великою кількістю вбудованих функцій. Стандартні завдання, такі як стандартизація виводу, взаємодія з базами даних, створення веб-запитів та управління ключами API, є частиною інтерфейсу. Замість того, щоб програмувати Recon-ng для виконання пошуку, розробники просто вибирають, які функції вони хочуть, щоб він виконував, і створюють автоматизований модуль всього за кілька хвилин.

Recon-ng - це безкоштовне програмне забезпечення з відкритим вихідним кодом. Доступна вікі містить вичерпну інформацію для початку роботи з інструментом, а також найкращі практики його використання.

theHarvester

Один з найпростіших у використанні інструментів у цьому списку, theHarvester призначений для збору публічної інформації, яка існує за межами мережі, що належить організації. Він може знаходити випадкові речі і у внутрішніх мережах, але більшість інструментів, які він

використовує, орієнтовані на зовнішні мережі. Він буде ефективним як розвідувальний крок перед тестуванням на проникнення або подібними вправами.

Джерела, які використовує theHarvester, включають популярні пошукові системи, такі як Bing і Google, а також менш відомі, такі як dogpile, DNSdumpster і механізм метаданих Exalead. Він також використовує Netcraft Data Mining і AlienVault Open Threat Exchange. Він навіть може використовувати пошукову систему Shodan для виявлення відкритих портів на знайдених хостах. Загалом, інструмент Harvester збирає електронні листи, імена, субдомени, IP-адреси та URL-адреси.

TheHarvester може отримати доступ до більшості загальнодоступних джерел без будь-якої спеціальної підготовки. Однак, деякі з використовуваних джерел вимагають наявності ключа API. Ви також повинні мати Python 3.6 або новішої версії у вашому середовищі.

Будь-хто може отримати theHarvester на GitHub. Рекомендується використовувати virtualenv для створення ізольованого середовища Python при клонуванні звідти.

Shodan

Shodan - це спеціальна пошукова система, яка використовується для пошуку інформації про такі пристрої, як мільярди пристроїв, що складають інтернет речей (IoT), які не часто можна знайти, але які сьогодні є скрізь. Його також можна використовувати для пошуку відкритих портів і вразливостей на цільових системах. Деякі інші OSINT-інструменти, такі як theHarvester, використовують його як джерело даних, хоча для глибокої взаємодії з Shodan потрібен платний акаунт.

Кількість місць, які Shodan може відстежувати і шукати в рамках OSINT-атаки, вражає. Це одна з небагатьох систем, здатних досліджувати операційні технології (OT), такі як ті, що використовуються в промислових системах управління на електростанціях і виробничих об'єктах. Будь-які

зусилля зі збору OSINT-даних в галузях, що використовують як інформаційні технології, так і операційні технології, без такого інструменту, як Shodan, втратили б величезний шматок цієї інфраструктури.

На додаток до пристроїв Інтернету речей, таких як камери, будівельні датчики і охоронні пристрої, Shodan також можна використовувати для перевірки баз даних, щоб побачити, чи є якась інформація у відкритому доступі через інші шляхи, окрім основного інтерфейсу. Він навіть може працювати з відеоіграми, виявляючи такі речі, як Minecraft або Counter-Strike: Global Offensive, які ховаються в корпоративних мережах там, де їх не повинно бути, і які вразливості вони створюють.

Будь-хто може придбати ліцензію Freelancer і використовувати Shodan для сканування до 5 120 IP-адрес на місяць, отримуючи до мільйона результатів. Це коштує $59 на місяць. Серйозні користувачі можуть придбати ліцензію Corporate, яка надає необмежену кількість результатів і сканування до 300 000 IP-адрес щомісяця. Корпоративна версія, яка коштує $899 на місяць, включає фільтр пошуку вразливостей і преміум-підтримку.

Metagoofil

Ще один вільно доступний інструмент на GitHub, Metagoofil, оптимізований для вилучення метаданих з публічних документів. Metagoofil може досліджувати майже будь-який тип документів, до яких він може отримати доступ через загальнодоступні канали, включаючи .pfd, .doc, .ppt, .xls та багато інших.

Кількість цікавих даних, які може зібрати Metagoofil, вражає. Пошук повертає такі речі, як імена користувачів, пов'язані зі знайденими документами, а також справжні імена, якщо вони доступні. Він також відображає шляхи, як дістатися до цих документів, що, в свою чергу, надає такі дані, як імена серверів, спільні ресурси та інформацію про дерево каталогів про організацію, що їх розмістила.

Все, що знаходить Metagoofil, може бути дуже корисним для хакера, який може використовувати його для таких речей, як запуск атак грубого перебору паролів або навіть фішингових листів. Організації, які хочуть захистити себе, можуть замість цього взяти ту ж саму інформацію, зібрану OSINT, і захистити або приховати її до того, як зловмисник зможе перехопити ініціативу.

Searchcode

Для тих, кому потрібно заглибитися в складну матрицю збору OSINT-даних, searchcode - це вузькоспеціалізована пошукова система, яка шукає корисну інформацію у вихідному коді. Цей потужний механізм, на диво, є роботою одного розробника.

Оскільки репозиторій коду потрібно спочатку додати до програми, перш ніж він стане доступним для пошуку, searchcode балансує на межі між інструментом OSINT та інструментом, призначеним для пошуку інших речей, окрім публічної інформації. Однак його все одно можна вважати інструментом OSINT, оскільки розробники можуть використовувати його для виявлення проблем, пов'язаних з наявністю конфіденційної інформації, доступної в коді як запущених програм, так і тих, що перебувають на стадії розробки. В останньому випадку ці проблеми можна виправити до розгортання у виробничому середовищі.

Хоча все, що пов'язано з кодом, вимагає більше знань, ніж, скажімо, пошук в Google, searchcode робить все можливе, щоб зробити свій інтерфейс максимально простим у використанні. Користувачі просто вводять свої пошукові запити, і searchcode повертає релевантні результати з пошуковими термінами, виділеними в рядках коду. Запропоновані пошукові запити включають імена користувачів, уразливості безпеки, такі як виклики eval $_GET, небажані активні функції, такі як re.compile, та спеціальні символи, які можуть бути використані для запуску атак з впровадженням коду.

Здебільшого результати, які повертає searchcode, не потребують пояснень. Однак, за необхідності, ви можете натиснути на ці результати, щоб знайти більш детальну інформацію або відповідні проблеми.

Babel X

Відповідна інформація не завжди є англійською мовою. За даними Statista, лише близько чверті інтернет-користувачів розмовляють англійською як рідною мовою, хоча різні джерела стверджують, що 55% інтернет-контенту є англійською. Інформація, яка вам потрібна, може бути китайською, іспанською або тамільською мовами.

Babel X від Babel Street - це багатомовний пошуковий інструмент для загальнодоступного Інтернету, включаючи блоги, соціальні мережі, дошки оголошень і сайти новин. Він також здійснює пошук у темній павутині, включаючи сайти Onion, і деякий глибокий веб-контент, до якого Babel X може отримати доступ на основі угод або ліцензій від власників контенту. Продукт здатний визначати географічне розташування джерела знайденої інформації, а також може виконувати аналіз тексту для виявлення релевантних результатів. Наразі Babel X може здійснювати пошук більш ніж 200 мовами.

Багатомовний пошук може бути корисним, наприклад, для пошуку світових новин, щоб бути в курсі ситуації - наприклад, знати тенденції в націлюванні атак зловмисників з вимогами викупу. Він також може бути використаний для виявлення інтелектуальної власності компанії, виставленої на продаж на іноземному веб-сайті, або інформації, яка свідчить про те, що ключовий партнер був скомпрометований. Клієнти також використовували Babel X для пошуку логінів підозрюваних зловмисників на неангломовних дошках оголошень.

Основний продукт Babel X є хмарним і дозволяє клієнтам налаштовувати його, додаючи власні джерела даних для пошуку. Babel Box - це локальна версія, але їй бракує деяких функцій Babel X, наприклад,

доступу до глибоких веб-джерел даних. Babel Channels, найдешевший варіант, - це кураторська колекція джерел даних. Для всіх варіантів доступний мобільний додаток.

OSINT Framework

Хоча ці інструменти пропонують безліч даних про OSINT, існує багато інших інструментів і методів, які допоможуть вам повністю зрозуміти публічний слід вашої організації. Чудовим ресурсом для пошуку додаткових інструментів є OSINT Framework, який пропонує веб-інтерфейс, що розбиває різні тематичні області, які цікавлять дослідників OSINT, і з'єднує вас з інструментами, які можуть допомогти вам знайти потрібну інформацію.

Інструменти, на які вкаже вам OSINT Framework, є безкоштовними, хоча деякі з них вимагають реєстрації або мають більш повнофункціональні платні версії. Деякі з них - це просто інструменти, які допомагають створювати розширені пошукові запити в Google, які можуть дати дивовижну кількість інформації. OSINT Framework підтримується Джастіном Нордіном (Justin Nordine) і має сторінку проекту на GitHub.

Хоча методи OSINT часто використовуються зловмисниками для розвідки перед початком незаконної атаки, здебільшого самі інструменти та методи є цілком легальними - адже вони призначені для того, щоб допомогти вам знайти дані, які опубліковані або іншим чином знаходяться у відкритому доступі. Навіть державні установи заохочуються до використання OSINT-технологій для пошуку дірок у власних системах кібербезпеки.

Однак, йдучи по сліду, відкритому цими OSINT-запитами, ви можете потрапити в правову сіру зону. Media Sonar дає кілька корисних порад про те, як залишатися на правильному боці закону. Наприклад, не є незаконним доступ до загальнодоступних ділянок темної мережі, і це може бути важливо, якщо ви намагаєтеся визначити, чи були дані вашої організації

зламані або викрадені; але ви не повинні намагатися купувати колекції викрадених даних як частину вашого дослідження або видавати себе за співробітника правоохоронних органів, щоб вибити інформацію з сумнівних персонажів.

Загалом, важливо заздалегідь розробити кодекс поведінки, який регулюватиме поведінку ваших співробітників під час таких експедицій, і документувати все, що ви робите, щоб продемонструвати, що ви дотримуєтесь цих правил і не порушуєте законів.

Не кожен злом або вторгнення пов'язані з передовими постійними загрозами або глибоким, складним проникненням. Хакери, як і всі інші, обирають найпростіший шлях до своїх цілей. Немає необхідності намагатися зламати надійний кіберзахист за допомогою багатомісячних зусиль, якщо інформація, яку вони хочуть отримати, доступна через загальнодоступний канал. Принаймні, конфіденційна інформація може бути використана як короткий шлях до отримання дійсних облікових даних або для планування ефективного вторгнення з меншими зусиллями і ризиком.

Інструменти OSINT можуть допомогти організаціям отримати уявлення про те, яка інформація доступна про них, їхні мережі, дані та користувачів. Швидкий пошук цієї інформації є ключовим фактором, оскільки це дозволить видалити її до того, як хтось зможе нею скористатися. Ці інструменти можуть стати потужною підтримкою під час цієї найважливішої гонки.

2.2 Використання OSINT у соціальних мережах

Розвиток платформ соціальних мереж змінив спосіб спілкування та доступу до інформації. Розвідка з використанням відкритих джерел (OSINT) стала важливим інструментом для організацій, урядових установ

та приватних осіб для збору та аналізу даних з різних онлайн-джерел, включаючи соціальні мережі. У цьому розділі ми надамо вам необхідні знання та ресурси для розуміння OSINT у соціальних мережах, а також приклади, посилання та курси.

OSINT в соціальних мережах - це процес збору, аналізу та використання інформації з платформ соціальних мереж для збору розвідувальних даних. Він передбачає систематичний пошук, моніторинг та аналіз публічних даних для отримання релевантної та дієвої інформації.

З мільярдами користувачів по всьому світу, соціальні медіа-платформи стали золотою жилою для збору розвідувальної інформації. OSINT в соціальних мережах може надати цінну інформацію для різних цілей, таких як оцінка загроз, конкурентний аналіз, кримінальні розслідування тощо.

OSINT соціальних мереж охоплює різні платформи, інструменти та методи збору інформації. Для того, щоб максимізувати можливості збору розвідувальної інформації, необхідно добре розуміти особливості платформ, їхні пошукові функції та потенційні вразливості.

У цьому розділі ми розглянемо найпопулярніші соціальні медіа-платформи та їхні специфічні OSINT-можливості.

Facebook

Facebook є потужною платформою для OSINT завдяки своїй великій базі користувачів і численним функціям, включаючи особисті профілі, бізнес-сторінки і групи. Ключові аспекти OSINT включають аналіз профілю, геолокаційні дані та аналіз контенту.

Twitter (X)

Twitter (X) є цінною платформою для OSINT, оскільки дозволяє відстежувати події та розмови в режимі реального часу. Методи OSINT включають моніторинг хештегів, ключових слів і облікових записів користувачів, а також вилучення геолокаційних даних.

Instagram

Instagram - це візуальна платформа, яка пропонує можливості OSINT за допомогою зображень, геолокаційних даних та користувацького контенту. Основні методи збору розвідувальної інформації включають аналіз зображень, профілювання користувачів і відстеження хештегів.

LinkedIn

LinkedIn є важливою платформою для OSINT у професійному та корпоративному світі. Завдяки детальним профілям і сторінкам компаній, це цінний ресурс для конкурентного аналізу, виявлення талантів і корпоративного шпигунства. Основні методи включають аналіз профілю, картографування мережі та аналіз вакансій.

YouTube

YouTube - це багате джерело мультимедійного контенту, який може надати цінну інформацію для OSINT. Методи збору розвідувальної інформації включають аналіз відео, профілювання користувачів, аналіз коментарів і вилучення метаданих.

Reddit

Reddit - це платформа для дискусій та обміну контентом, з численними тематичними спільнотами, які називаються підресурсами. Можливості OSINT на Reddit включають відстеження популярних тем, моніторинг конкретних субредітів та аналіз поведінки користувачів.

TikTok

TikTok - це платформа для створення коротких відео, яка за останні роки набула величезної популярності. Методи OSINT для TikTok включають аналіз відео, моніторинг хештегів та профілювання користувачів.

Тепер, коли ми вивчили потенціал різних платформ соціальних мереж для OSINT, давайте розглянемо деякі інструменти і методи, які можна використовувати для збору розвідувальної інформації з цих платформ.

Методи ручного пошуку передбачають безпосереднє використання вбудованих пошукових функцій платформи або застосування розширених пошукових операторів для звуження результатів. Цей підхід вимагає глибокого розуміння пошукових можливостей і обмежень кожної платформи.

Автоматизовані інструменти можуть спростити процес OSINT і заощадити час, скануючи кілька платформ і агрегуючи дані. Прикладами таких інструментів є Maltego, Hunchly та Social Bearing.

Для збору великих обсягів даних з платформ соціальних мереж можна використовувати інтерфейси прикладного програмування (API) та методи веб-скрепінгу. Такий підхід часто вимагає навичок програмування та знання обмежень API кожної платформи.

Проводячи OSINT в соціальних мережах, важливо пам'ятати про етичні та юридичні аспекти, пов'язані з цим.

Повага до приватності та збереження анонімності є ключовими аспектами OSINT в соціальних мережах. Важливо уникати порушення прав на приватність і захищати свою особистість під час проведення досліджень.

OSINT-спеціалісти повинні знати про правові наслідки збору інформації з платформ соціальних мереж, включаючи закони про захист даних, умови угод про надання послуг і питання авторських прав.

Дотримання етичних принципів та найкращих практик є важливим для проведення відповідального OSINT у соціальних мережах. Це включає в себе отримання інформації тільки з загальнодоступних джерел, перевірку інформації, а також відмову від хакерства та інших незаконних дій.

Щоб краще зрозуміти застосування і переваги OSINT в соціальних мережах, давайте розглянемо деякі реальні приклади і тематичні дослідження.

OSINT відіграє важливу роль у відстеженні та моніторингу діяльності терористичних та екстремістських груп у соціальних мережах, що призводить до арештів та запобігання потенційним атакам.

Компанії використовують OSINT в соціальних мережах, щоб отримати уявлення про стратегії конкурентів, виявити потенційні слабкі місця і розкрити нові можливості.

Правоохоронні органи та приватні детективи використовують OSINT в соціальних мережах для пошуку зниклих безвісти, збору доказів для кримінальних справ та відстеження підозрюваних.

Аналітики використовують OSINT в соціальних мережах для моніторингу глобальних подій, відстеження конфліктів та оцінки потенційних загроз в режимі реального часу.

Щоб отримати максимальну користь від OSINT в соціальних мережах, скористайтеся наступними порадами:

Розробка чітко визначеного плану дослідження допомагає забезпечити систематичний і ретельний підхід до OSINT в соціальних мережах. Це включає визначення цілей, визначення цільових платформ і вибір відповідних інструментів і методів.

1) Організованість

Відстеження зібраних даних та їх аналіз мають вирішальне значення для ефективного OSINT. Використання таких інструментів, як електронні таблиці, додатки для ведення нотаток і засоби візуалізації даних, може допомогти підтримувати організацію і спростити процес аналізу.

2) Перевірка інформації

Забезпечення точності та надійності зібраної інформації має вирішальне значення для успіху OSINT в соціальних мережах. Перехресні посилання на дані, перевірка декількох джерел і використання таких інструментів, як зворотний пошук зображень, можуть допомогти перевірити отримані дані.

3) Управління часом

Ефективний тайм-менеджмент має важливе значення для проведення OSINT у соціальних мережах, оскільки інформація може швидко застаріти.

Визначення пріоритетності завдань, встановлення дедлайнів і використання інструментів автоматизації можуть допомогти оптимізувати процес дослідження.

4) Курси, сертифікати та навчальні програми

Щоб поглибити свої знання та навички з OSINT в соціальних мережах, розгляньте можливість проходження курсів, отримання сертифікатів або участі в навчальних програмах.

5) Онлайн-курси

Численні онлайн-курси пропонують навчання з OSINT в соціальних мережах, починаючи від початкового і закінчуючи просунутим рівнем. Наприклад, Bellingcat's Online Investigation Toolkit, SANS SEC487: Збір та аналіз розвідувальних даних з відкритих джерел (OSINT), а також курси OSINT від Udemy.

6) Особисте навчання

Очні навчальні програми та семінари надають практичний досвід навчання та можливість поспілкуватися з колегами-практиками з OSINT. Такі заходи, як OSINTcon та конференція OSMOSIS, пропонують цінні навчальні сесії.

7) Сертифікації

Сертифікація може допомогти підтвердити ваші навички OSINT та підвищити ваш професійний авторитет. Наприклад, сертифікація Certified in Open Source Intelligence (COSI) та GIAC Open Source Intelligence (GOSI).

8) Ресурси та спільноти

Щоб бути в курсі останніх тенденцій, інструментів і методів OSINT в соціальних мережах, важливо взаємодіяти з ресурсами і спільнотами, які можуть підтримати ваш навчальний процес.

9) Веб-сайти та блоги

Різноманітні веб-сайти та блоги пропонують цінну інформацію, поради та оновлення про OSINT в соціальних мережах. Наприклад, Bellingcat, IntelTechniques та OSINTCurious.

10) Книги та публікації

Книги та публікації можуть надати глибокі знання та інформацію про OSINT в соціальних мережах. Серед найбільш відомих видань - "Методи розвідки з відкритим вихідним кодом" Майкла Баззелла, "Мистецтво OSINT" Кріса Поултера та "Полювання на кіберзлочинців" Вінні Тройя.

11) OSINT-спільноти в соціальних мережах

Онлайн-спільноти, форуми та групи в соціальних мережах - це платформи, де фахівці з OSINT можуть ділитися знаннями, ставити запитання та бути в курсі останніх тенденцій та інструментів. Приклади включають OSINT subreddit, форум OSINT.team, а також різні групи в LinkedIn і Facebook.

Соціальні мережі OSINT є потужним інструментом для збору розвідувальної інформації в різних сферах. Володіючи відповідними знаннями, інструментами і методами, окремі особи і організації можуть використовувати багатство інформації, доступної на платформах соціальних мереж, для прийняття обґрунтованих рішень, зниження ризиків і отримання конкурентних переваг. Цей вичерпний посібник слугує відправною точкою для тих, хто прагне дослідити та опанувати світ OSINT у соціальних мережах. Продовжуйте вчитися, будьте допитливими і не забувайте ділитися своїми знаннями та досвідом з широкою спільнотою OSINT-спеціалістів.

Тепер, коли у вас є вичерпний перелік з OSINT в соціальних мережах, ви готові розпочати власну подорож зі збору розвідувальної інформації. Незалежно від того, чи є ви приватною особою, яка прагне дізнатися більше про певну тему, чи організацією, яка прагне посилити свої конкурентні переваги, знання і ресурси, стануть вам у нагоді.

РОЗДІЛ 3. РОЗРОБКА ІНСТРУМЕНТУ НА ОСНОВІ OSINT ДЛЯ СОЦІАЛЬНИХ МЕРЕЖ

3.1 Застосування API у розвідці за допомогою OSINT

В епоху цифрових технологій, коли інформація стала ключовим ресурсом, важливо визнати роль відкритого джерела інформації (OSINT) у здійсненні розвідки. OSINT дозволяє отримувати відомості з різних джерел, доступних громадськості, з метою збільшення обсягу інформації, доступної аналітикам та дослідникам. Одним із важливих інструментів для отримання даних з відкритих джерел є застосування API (Application Programming Interface).

API - це набір протоколів та інструментів, які дозволяють різним програмам взаємодіяти між собою. У випадку розвідки та OSINT, використання API може значно полегшити збір та аналіз інформації. Ось декілька способів, які демонструють важливість та ефективність використання API у розвідці:

Соціальні мережі: Багато соціальних мереж надають API, які дозволяють отримувати дані про користувачів, їх публічні записи, фотографії та інші відомості. Це може бути корисно при аналізі особистостей або груп для визначення їхнього впливу та поведінки в мережі.

Географічні дані: API картографічних сервісів дозволяють отримувати інформацію про місцезнаходження об'єктів. Це може використовуватися для визначення маршрутів пересування осіб, локацій подій чи спостереження за географічним розташуванням об'єктів інтересу.

Веб-скрапінг: API веб-скрапінгу дозволяють отримувати дані з веб-сайтів шляхом автоматизованого звертання до їхніх ресурсів. Це може бути корисно для отримання інформації про компанії, організації або події.

Кіберзахист: API можуть використовуватися для моніторингу та аналізу загроз в Інтернеті. За допомогою спеціальних сервісів, можна отримувати інформацію про потенційні загрози, вразливості та інші кібербезпекові аспекти.

Фінансові дані: API фінансових інструментів дозволяють отримувати дані про компанії, фінансові ринки та інші аспекти економіки. Це може бути важливим при аналізі економічних аспектів певного сектору чи підприємства.

Використання API у розвідці за допомогою OSINT дозволяє збільшити швидкість та точність збору інформації. Однак важливо дотримуватися етичних стандартів та правових обмежень, щоб уникнути порушення конфіденційності та приватності. Завдяки ефективному використанню API, можна підняти якість розвідки та забезпечити більш повний та збалансований образ ситуації в обраній сфері аналізу.

3.2 Розробка плану пошуку з використанням OSINT

В епоху цифрових технологій розвідка за допомогою відкритих джерел інформації (OSINT) стає все більше важливою для аналітиків, дослідників та спеціалістів з безпеки. Однак успішність розвідки значно залежить від якості та організованості процесу пошуку інформації. У цьому розділі магістерської роботи ми розглянемо ключові кроки та рекомендації для створення ефективного плану пошуку при OSINT розвідці.

1. Визначення цілей та завдань розвідки

Перед тим як розпочати пошук інформації, важливо чітко сформулювати цілі та завдання розвідки. Визначте, що саме ви хочете дізнатися чи вивчити. Це допоможе визначити необхідні напрямки пошуку та ефективно використовувати час та ресурси.

2. Вибір основних джерел інформації

Оберіть основні джерела інформації, які вам слід перевірити. Це можуть бути соціальні мережі, відкриті бази даних, форуми, новинні статті, публічні реєстри тощо. Концентруйтеся на тих джерелах, які мають найбільший потенціал для надання потрібної Вам інформації.

3. Створення ключових запитань та термінів пошуку

Розробіть перелік ключових запитань та термінів пошуку, які ви будете використовувати при OSINT. Враховуйте варіації термінів та схожі ключові слова, щоб забезпечити максимальне охоплення інформації.

4. Використання спеціальних інструментів та платформ

Розвідники зазвичай користуються різноманітними спеціальними інструментами та платформами для ефективного збору інформації. Використовуйте інструменти для аналізу соціальних мереж, моніторингу інтернет-ресурсів, перевірки доменів, аналізу зображень тощо.

5. Аналіз зібраної інформації

Не обмежуйтеся лише збором інформації. Постійно аналізуйте отримані дані, враховуючи їх джерело та достовірність. Використовуйте аналітичні навички для з'ясування взаємозв'язків та визначення можливих слабких місць.

6. Забезпечення конфіденційності та легальності

Важливо дотримуватися принципів конфіденційності та легальності при проведенні OSINT розвідки. Уникайте порушення законів щодо конфіденційності та приватності осіб.

7. Документування та звітність

Ведіть детальний журнал всіх етапів розвідки, включаючи використані джерела, методи пошуку та отримані результати. Це полегшить подальший аналіз та може бути важливим у випадку необхідності подати звіт.

Створення плану пошуку при OSINT розвідці вимагає уважного підходу та стратегічного мислення. Правильно підготовлений план

дозволить ефективно використовувати ресурси та максимально використовувати можливості відкритих джерел інформації для досягнення поставлених цілей.

3.3 Створення та перевірка інструменту для OSINT у соціальних мережах

Ні для кого не секрет, що сучасні соціальні мережі являють собою величезні БД, що містять багато цікавої інформації про приватне життя своїх користувачів. Через веб-додаток особливо багато даних не витягнеш, але ж у кожної мережі є свій API. Подивимося, як цим можна скористатися для пошуку користувачів і збору інформації про них.

В американській розвідці існує така дисципліна, як OSINT (Open source intelligence), що відповідає за пошук, збирання та вибір інформації із загальнодоступних джерел. До одного з найбільших постачальників загальнодоступної інформації можна віднести соціальні мережі. Адже практично в кожного з нас є обліковий запис (а в когось і не один) в одній або декількох соцмережах. Тут ми ділимося своїми новинами, особистими фотографіями, уподобаннями (наприклад, лайкаючи щось або вступаючи в якусь групу), колом своїх знайомств. Причому робимо це з власної доброї волі та практично зовсім не замислюємося про можливі наслідки. Зазвичай, для того щоб витягувати з соцмереж цікаві дані потрібно було вручну здійснити якісь маніпуляції. Але для успішної розвідки логічніше скористатися спеціальними утилітами. Існує кілька Open Source утиліт, що дають змогу витягувати інформацію про користувачів із соцмереж.

Одна з найпопулярніших - Creepy. Вона призначена для збору геолокаційної інформації про користувача на основі даних з його акаунтів Twitter, Instagram, Google+ і Flickr. До переваг цього інструменту, який штатно входить до Kali Linux, варто зарахувати зрозумілий інтерфейс, дуже

зручний процес отримання токенів для використання API сервісів, а також відображення знайдених результатів мітками на карті (що, зі свого боку, дає змогу простежити за всіма переміщеннями користувача). До недоліків я б відніс слабенький функціонал. Додаток вміє збирати геотеги за перерахованими сервісами і виводити їх на Google-карті, показує, кого і скільки разів ретвітів користувач, рахує статистику за пристроями, з яких писалися твіти, а також за часом їхньої публікації. Але завдяки тому, що це Open Source інструмент, його функціонал завжди можна розширити самому.

Розглядати, як використовувати програму, не будемо - все чудово показано в офіційному відео, після перегляду якого не повинно залишитися жодних запитань з приводу роботи з інструментом (рис. 3.1).

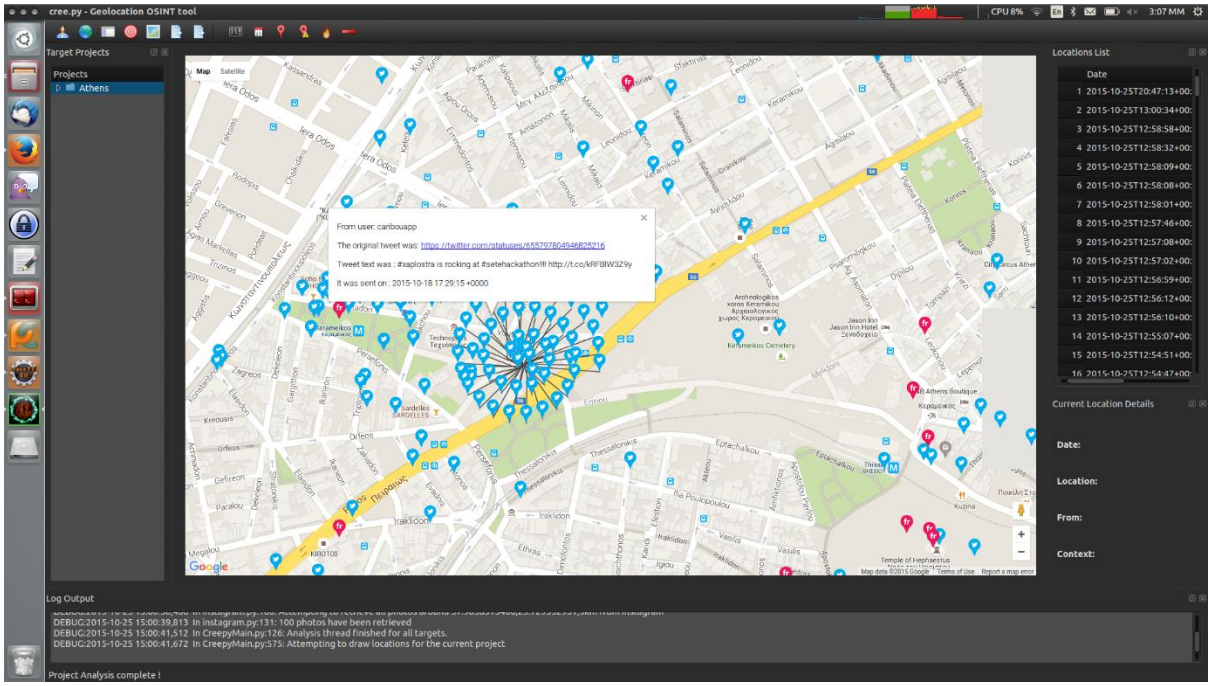

Рисунок 3.1 - Приклад роботи Creepy

Ще два інструменти, які менш відомі, але мають сильний функціонал і заслуговують на твою увагу, - fbStalker і geoStalker.

fbStalker призначений для збору інформації про користувача на основі його Facebook-профілю. Дозволяє отримати такі дані:

- відео, фото, пости користувача;
- хто і скільки разів лайкнув його записи;
- геоприв'язки фоток;
- статистика коментарів до його записів і фотографій;
- час, у який він зазвичай буває в онлайні.

Для роботи цього інструменту тобі знадобиться Google Chrome, ChromeDriver, який встановлюється таким чином:

wget http://goo.gl/Kvh33W

unzip chromedriver_linux32_23.0.1240.0.zip

cp chromedriver /usr/bin/chromedriver

chmod 777 /usr/bin/chromedriver

Крім цього, знадобиться встановлений Python 3, а також *pip* для встановлення таких пакетів:

pip install pytz

pip install tzlocal

pip install termcolor

pip install selenium

pip install requests --upgrade

pip install beautifulsoup4

І нарешті, знадобиться бібліотека для парсингу GraphML-файлів:

git clone https://github.com/hadim/pygraphml.git

cd pygraphml

python3 setup.py install

Після цього можна буде поправити *fbstalker.py*, вказавши там свою пошту, пароль, ім'я користувача, і починати пошук. Користуватися додатком досить просто:

python fbstalker.py -user [ім'я користувача, що цікавить]

Geostalker значно цікавіший. Він збирає інформацію за координатами, які йому передали. Наприклад:

- місцеві Wi-Fi-точки на основі бази wigle.net (зокрема, їхні essid, bssid, geo);
- чекіни з Foursquare;
- Instagram- і Flickr-акаунти, з яких постили фотки з прив'язкою до цих координат;
- усі твіти, зроблені в цьому районі.

Для роботи інструменту, як і в попередньому випадку, знадобиться *Chrome & ChromeDriver, Python 3, pip* (для встановлення таких пакетів: *google, python-instagram, pygoogle, geopy, lxml, oauth2, python-linkedin, pygeocoder, selenium, termcolor, pysqlite, TwitterSearch, foursquare*), а також *pygraphml* і *gdata*:

git clone https://github.com/hadim/pygraphml.git
cd pygraphml
python3 setup.py install
wget https://gdata-python-client.googlecode.com/files/gdata-2.0.18.tar.gz
tar xvfz gdata-2.0.18.tar.gz
cd gdata-2.0.18
python3 setup.py install

Після цього редагуємо *geostalker.py*, заповнюючи всі необхідні API-ключі та access-токени (якщо для будь-якої соцмережі ці дані не будуть вказані, то вона просто не братиме участі в пошуку). Після чого запускаємо інструмент командою *sudo python3 geostalker.py* і вказуємо адресу або

координати. У результаті всі дані збираються і розміщуються на Google-карті, а також зберігаються в HTML-файл.

До цього йшлося про готові інструменти. Здебільшого їхнього функціоналу не вистачатиме і доведеться або їх допрацьовувати, або писати свої додатки - усі популярні соцмережі надають свої API. Зазвичай вони постають у вигляді окремого піддомена, на який ми шлемо GET-запити, а у відповідь отримуємо XML/JSON-відповіді. Наприклад, для Instagram - це api.instagram.com, для "ВКонтакте" - api.vk.com. Звичайно, у більшості таких API є свої бібліотеки функцій для роботи з ними, але ж ми хочемо розібратися, як це працює, та й обтяжувати скрипт зайвими зовнішніми бібліотеками через одну-дві функції не практично. Отже, давайте візьмемо і напишемо власний інструмент, який би давав змогу шукати фотографії з VK(рис. 2.3) та Instagram (рис. 2.2): за заданими координатами і проміжком часу.

Використовуючи документацію до API VK та Instagram, складаємо запити для отримання списку фотографій за географічною інформацією та часом.

Instagram API Request:

```
url = "https://api.instagram.com/v1/media/search?"
    + "lat=" + location_latitude
    + "&lng=" + location_longitude
    + "&distance=" + distance
    + "&min_timestamp=" + timestamp
    + "&max_timestamp=" + (timestamp + date_increment)
    + "&access_token=" + access_token
```

Vkontakte API Request:

```
url = "https://api.vk.com/method/photos.search?"
    + "lat=" + location_latitude
```

+ "&long=" + location_longitude

+ "&count=" + 100

+ "&radius=" + відстань

+ "&start_time=" + timestamp

+ "&end_time=" + (timestamp + date_increment)

Тут використовуються змінні:

location_latitude - географічна широта;

location_longitude - географічна довгота;

distance - радіус пошуку;

timestamp - початкова межа інтервалу часу;

date_increment - кількість секунд від початкової до кінцевої межі інтервалу часу;

access_token - токен розробника.

Як з'ясувалося, для доступу до Instagram API потрібен access_token. Отримати його нескладно, але доведеться трохи заморочитися. ВКонтакте же більш лояльно ставиться до незнайомців, що дуже добре для нас.

Отримання Instagram Access Token

Для початку реєструємось в інстаграмі. Після реєстрації переходимо за наступним посиланням:

http://instagram.com/developer/clients/manage/

Натискаємо Register a New Client. Вводимо номер телефону, очікуємо SMS і вводимо код. У вікні створення нового клієнта, що відкрилося, важливі для нас поля потрібно заповнити наступним чином:

OAuth redirect_url: http://localhost/

Disable implicit OAuth: галочка має бути знята!!!

Інші поля заповнюються довільно. Щойно все заповнили, створюємо нового клієнта. Тепер потрібно отримати токен. Для цього вписуємо в адресний рядок браузера наступний URL:

https://instagram.com/oauth/authorize/?client_id=[CLIENT_ID]&redire ct_uri=http://localhost/&response_type=token

де замість [CLIENT_ID] вказуємо Client ID створеного нами клієнта.

Після цього робимо перехід за посиланням, що вийшло, і якщо ми зробили усе правильно, то нас переадресує на http://localhost і в адресному рядку якраз буде написано Access Token.

http://localhost/#access_token=[Access Token]

Детальніше про цей метод отримання токена можна почитати за наступним посиланням: *http://jelled.com/instagram/access-token.*

Тепер спробуємо автоматизувати даний процес

Отже, ми навчилися складати потрібні запити, але вручну розбирати відповідь сервера (у вигляді JSON/XML) - не найкрутіше заняття. Набагато зручніше зробити невеликий скриптик, який робитиме це за нас. Використовувати ми будемо знову ж таки Python 3. Логіка така: ми шукаємо всі фото, які потрапляють у заданий радіус відносно заданих координат у заданий проміжок часу. Але враховуйте один дуже важливий момент - виводиться обмежена кількість фотографій. Тому для великого проміжку часу доведеться робити кілька запитів із проміжними інтервалами часу (якраз date_increment). Також враховуй похибку координат і не вказуй радіус у кілька метрів. І не забувай, що час потрібно вказувати в timestamp.

Починаємо писати наш скрипт. Для початку підключимо всі необхідні нам бібліотеки:

import httplib

import urllib

import json

import datetime

Напишемо функції для отримання даних з API через HTTPS. За допомогою переданих аргументів функції ми складаємо GET-запит і повертаємо відповідь сервера рядком.

```
def get_instagram(широта, довгота, відстань, min_timestamp, max_timestamp, access_token):
    get_request = '/v1/media/search?lat=' + широта
    get_request += '&lng=' + довгота
    get_request += '&distance=' + відстань
    get_request += '&min_timestamp=' + str(min_timestamp)
    get_request += '&max_timestamp=' + str(max_timestamp)
    get_request += '&access_token=' + access_token
    local_connect = httplib.HTTPSConnection('api.instagram.com', 443)
    local_connect.request('GET', get_request)
    return local_connect.getresponse().read()
def get_vk(широта, довгота, відстань, min_timestamp, max_timestamp):
    get_request = '/method/photos.search?lat=' + location_latitude
    get_request += '&long=' + location_longitude
    get_request += '&count=100'
    get_request += '&radius=' + відстань
    get_request += '&start_time=' + str(min_timestamp)
    get_request += '&end_time=' + str(max_timestamp)
    local_connect = httplib.HTTPSConnection('api.vk.com', 443)
    local_connect.request('GET', get_request)
    return local_connect.getresponse().read()
```

Ще накопичимо невелику функцію конвертації timestamp в нормальний вигляд:

```
def timestamptodate(timestamp):
    return  datetime.datetime.fromtimestamp(timestamp).strftime('%Y-%m-%d %H:%M:%S')+' UTC').
```

Тепер пишемо основну логіку пошуку картинок, попередньо розбивши часовий відрізок на частини, результати зберігаємо в HTML-файл. Функція має громіздкий вигляд, але основну складність у ній становить розбиття часового інтервалу на блоки. В іншому це звичайний парсинг JSON і збереження потрібних даних у HTML.

```
def parse_instagram(location_latitude, location_longitude, distance, min_timestamp, max_timestamp, date_increment, access_token):
    print 'Починаємо розбір instagram...'
    print 'GEO:',location_latitude,location_longitude
    print 'TIME: from',timestamptodate(min_timestamp),'to',timestamptodate(max_timestamp)
    file_inst = open('instagram_'+location_latitude+location_longitude+'.html','w')
    file_inst.write('<html>')
    local_min_timestamp = min_timestamp
    while (1):
        if ( local_min_timestamp >= max_timestamp ):
            break
        local_max_timestamp = local_min_timestamp + date_increment
        if ( local_max_timestamp > max_timestamp ):
            local_max_timestamp = max_timestamp
        print timestamptodate(local_min_timestamp),'-',timestamptodate(local_max_timestamp)
        local_buffer = get_instagram(location_latitude, location_longitude, distance, local_min_timestamp, local_max_timestamp, access_token)
    instagram_json = json.loads(local_buffer)
        for local_i in instagram_json['data']:
```

```
                file_inst.write('<br>')
                file_inst.write('<img
src='+local_i['images']['standard_resolution']['url']+'><br>')

file_inst.write(timestamptodate(int(local_i['created_time']))+'<br>')
                file_inst.write(local_i['link']+'<br>')
                file_inst.write('<br>')
            local_min_timestamp = local_max_timestamp
        file_inst.write('</html>')
        file_inst.close()
```

HTML-формат вибрано не просто так. Він дозволяє нам не зберігати картинки окремо, а лише вказати посилання на них. При запуску сторінки результати в браузеры картинки автоматично підгрузяться.

Пишем точно таку ж функцію для «ВКонтакте».

```
    def parse_vk(location_latitude, location_longitude, distance,
min_timestamp, max_timestamp, date_increment):
        print 'Starting parse vkontakte..'
        print 'GEO:',location_latitude,location_longitude
        print 'TIME:
from',timestamptodate(min_timestamp),'to',timestamptodate(max_timestamp)
        file_inst =
open('vk_'+location_latitude+location_longitude+'.html','w')
        file_inst.write('<html>')
        local_min_timestamp = min_timestamp
        while (1):
            if ( local_min_timestamp >= max_timestamp ):
                break
```

```
            local_max_timestamp = local_min_timestamp + date_increment
        if ( local_max_timestamp > max_timestamp ):
            local_max_timestamp = max_timestamp
        print timestamptodate(local_min_timestamp),'-
',timestamptodate(local_max_timestamp)
        vk_json = json.loads(get_vk(location_latitude, location_longitude,
distance, local_min_timestamp, local_max_timestamp))
        for local_i in vk_json['response']:
            if type(local_i) is int:
                continue
            file_inst.write('<br>')
            file_inst.write('<img src='+local_i['src_big']+'><br>')
            file_inst.write(timestamptodate(int(local_i['created']))+'<br>')
            file_inst.write('http://vk.com/id'+str(local_i['owner_id'])+'<br>')
            file_inst.write('<br>')
        local_min_timestamp = local_max_timestamp
    file_inst.write('</html>')
    file_inst.close()
```

І звичайно ж, самі виклики функцій (рис. 2.1):

```
parse_instagram(location_latitude, location_longitude, distance,
min_timestamp, max_timestamp, date_increment, instagram_access_token)
parse_vk(location_latitude, location_longitude, distance, min_timestamp,
max_timestamp, date_increment)
```

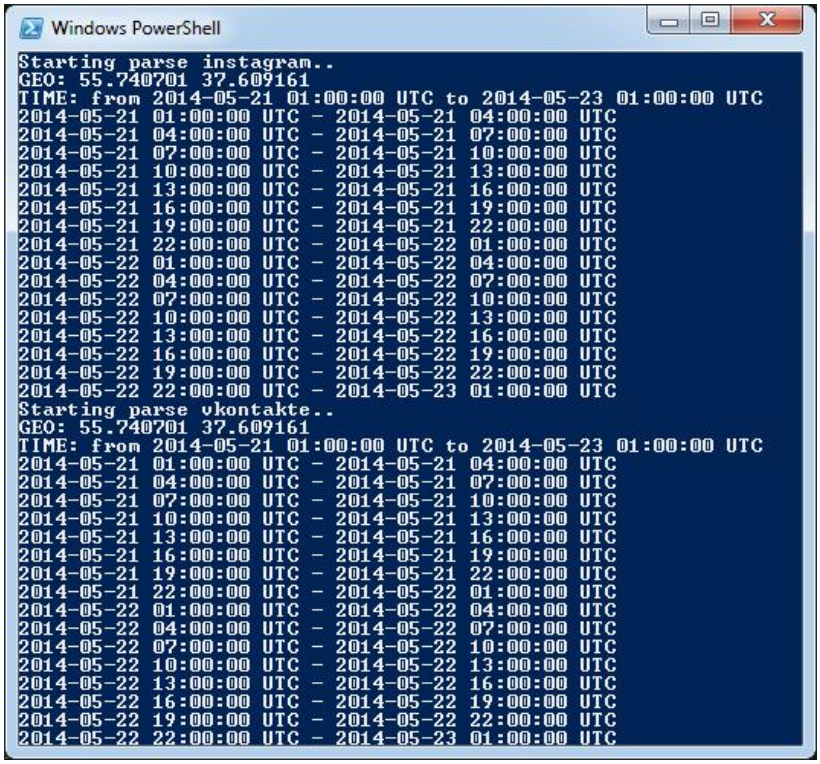

Рис. 2.1 - Результат роботи нашого скрипта в консолі

2014-05-22 18:15:57
http://instagram.com/p/[redacted]/

Рисунок 2.2 - Один із результатів парсингу Інстаграма

Рис 2.3 - Результат парсингу "ВКонтакте"

Конкрентні розвідники готові зачепитися за будь-яку можливість отримати нову інформацію, і API соціальних мереж їм у цьому можуть дуже непогано допомогти. В процесі написання магістерської роботи, ми вивчив ще кілька сервісів, зокрема Twitter, Facebook і LinkedIn, - чи є подібний функціонал. Позитивні результати дав тільки " Twitter ", що, безсумнівно, радує. А ось Facebook і LinkedIn засмутили, хоча ще не все втрачено і, можливо, в майбутньому вони розширять свої API. Загалом, будьте уважнішими, викладаючи свої фото з геоприв'язкою.

РОЗДІЛ 4 БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ, ОСНОВИ ОХОРОНИ ПРАЦІ

4.1 Поведінкові реакції населення під час надзвичайних ситуацій

Для вивчення поведінкових реакцій населення у надзвичайних ситуаціях важливо спочатку чітко визначити термін "надзвичайна ситуація". Така ситуація може виникнути внаслідок техногенного або природного події, такої як аварія, катастрофа, стихійне лихо чи інша небезпечна подія, включаючи епідемії, епізоотії, епіфітотії та пожежі, що призводять до неможливості проживання на певній території, зупинення господарської діяльності, загибелі людей та/або значних матеріальних втрат. Зона надзвичайної ситуації визначається як територія, де виникла така ситуація.

Розгляд поведінки людей під час різних надзвичайних ситуацій важливий для підготовки керівників, рятувальників та громадськості до дій у разі екстремальних подій. Особлива увага приділяється психології страху, оскільки люди, зіткнувшись з небезпеками, можуть відчувати страхові реакції, спричинені реальною чи уявною загрозою.

Сам страх виконує функцію сигналу тривоги, який активує захисні реакції людини. Незважаючи на те, що страх може бути негативним відчуттям, він також стимулює до індивідуальних чи колективних захисних дій, оскільки головна мета - збереження життя та продовження існування.

Слід враховувати, що в умовах небезпеки люди часто реагують необдумано і несвідомо. Різні фактори, такі як екстремальні температури, хімічні речовини, фізичні сили, біологічні фактори та іонізуюче випромінювання, можуть становити загрозу для життя людини через агресивний вплив.

Готовність людини до надзвичайних ситуацій вимагає високої емоційної стійкості, рішучості та витримки. Події такого роду можуть

викликати значну емоційну збудженість, що потребує надання допомоги постраждалим і рятування матеріальних цінностей.

У таких обставинах може бути порушений процес нормального мислення, втрачений контроль над собою та діями, що може мати непередбачувані наслідки. Подолання страху, як правило, залежить від почуття власної відповідальності та усвідомлення значущості виконуваної дії.

Люди, які відчувають страх і є незахищеними психологічно або необізнаними, можуть намагатися покинути небезпечні місця. Вони можуть виживати психологічний шок, який проявляється заціпенінням м'язів. У таких моментах порушується процес нормального мислення, втрачається контроль над почуттями та волею.

Реакція нервової системи на страх може виявлятися різноманітно, включаючи розширення зіниць, підвищення пульсу, зміни дихання, потовиділення, спазми кровоносних судин, втрату мови та зміни голосу. У деяких випадках раптовий страх може призвести до серйозних проблем зі здоров'ям серцево-судинної системи, навіть смерті.

Такий стан може тривати від кількох годин до декількох днів. Часто під час ліквідації наслідків надзвичайних ситуацій спостерігаються люди, які перебувають у стані глибокої депресії і блукають безцільно серед руїн тривалий період.

Причини такої поведінки людей у надзвичайних ситуаціях можуть включати слабку морально-психологічну підготовку, неочікуване виникнення небезпеки, відсутність знань про характер та наслідки таких ситуацій, незнання правил поведінки в них, а також відсутність навичок та досвіду в боротьбі з ними.

4.2 Заходи, що забезпечують оптимальні метеорологічні умови в санітарно-побутових приміщеннях

Метеорологічні умови, такі як температура, вологість і швидкість руху повітря, мають важливий вплив на здоров'я і комфорт людей. Вони можуть впливати на терморегуляцію організму, сприяти поширенню хвороботворних мікроорганізмів і викликати неприємні відчуття.

Розрізняють оптимальні і припустимі метеорологічні умови.

Оптимальні метеорологічні умови - це такі умови, які забезпечують збереження нормального теплового стану організму без напруження механізмів терморегуляції. Вони сприяють відчуття теплового комфорту і підвищують продуктивність праці.

Припустимі метеорологічні умови - це такі умови, які при тривалому впливі можуть викликати незначні зміни в тепловому стані організму, але швидко нормалізуються. Вони не перевищують фізіологічні можливості адаптації, але можуть викликати незручні відчуття тепла, погіршення самопочуття і зниження продуктивності.

Забезпечення оптимальних метеорологічних умов в санітарно-побутових приміщеннях є важливим аспектом створення комфортного і безпечного середовища для людей. До основних заходів, які допомагають досягти цієї мети, відносяться:

Ефективна вентиляція забезпечує свіже повітря і видаляє забруднене повітря з приміщення. Вона може бути природною або механічною.

Рекомендована температура в санітарно-побутових приміщеннях становить 24°C.

Рекомендований діапазон вологості становить від 40% до 60%.

Правильне освітлення є важливим фактором для комфорту і безпеки в приміщенні. Рекомендується використовувати природне освітлення, а

також штучне освітлення в тих місцях, де недостатня кількість природного світла.

Санітарна оцінка якості повітря є важливою для виявлення наявності шкідливих речовин. Регулярне проведення аналізу повітря та очищення його від шкідливих речовин сприяє забезпеченню здорового середовища.

Забезпечення оптимальних метеорологічних умов в санітарно-побутових приміщеннях є важливим завданням, яке сприяє збереженню здоров'я і благополуччя людей. Правильна вентиляція, контроль температури, вологості та освітлення є ключовими елементами для досягнення цієї мети.

ВИСНОВКИ

В ході дослідження у кваліфікаційній роботі було аналізовано використання технології OSINT для збору, узагальнення та аналізу інформації, зокрема відомостей, отриманих з різних соціальних мереж. Основною метою було висвітлення проблематики, пов'язаної із значущістю соціальних мереж у процесі OSINT розвідки.

Під час виконання дослідження стану використання технології OSINT було зосереджено на розгляді популярних інструментів для збору та аналізу інформації у контексті OSINT розвідки. Також був розроблений план для проведення такої розвідки.

Для досягнення поставлених завдань у рамках роботи був створений власний інструмент на мові програмування Python. Цей інструмент використовував API одного з відкритих сервісів для отримання необхідної інформації. Також була проведена повноцінна OSINT розвідка, використовуючи популярні соціальні мережі та інші відкриті джерела, що дозволило отримати значну кількість цінної інформації.

Тема використання технології OSINT для збору, узагальнення та аналізу інформації на основі соціальних мереж вкрай актуальна. У сучасному цифровому світі, де соціальні мережі стали невід'ємною частиною життя багатьох людей, вони стають важливим джерелом відкритої інформації. Це може надати унікальні відомості та сприяти розумінню поведінки, інтересів та поглядів різних осіб. Майбутні перспективи у цій сфері виглядають дуже обіцяюче, з удосконаленням алгоритмів, розвитком штучного інтелекту та машинного навчання, що робить OSINT розвідку більш точною, швидкою та ефективною. Таким чином, використання технології OSINT для аналізу соціальних мереж має значний потенціал у різних сферах, включаючи безпеку, розвідку, бізнес-аналітику та громадську діяльність. Постійний розвиток цієї технології та її поєднання з іншими інноваційними підходами відкриває нові можливості для досягнень у майбутньому.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Vinny Troia. A Hacker’s Guide to Online Intelligence Gathering Tools and Techniques. 2020. с. 48

2. Michael Sankey. "The Manual to Online Public Records: The Researcher's Tool to Online Resources of Public Records and Public Information." 2016. с. 109

3. Robert David Steele. "The Open-Source Everything Manifesto: Transparency, Truth, and Trust." 2012. с. 59

4. Statista. Users worldwide visiting Reddit.com from April 2021 to April 2022. URL: https://www.statista.com/statistics/1310710/redditcom-monthly-users/

5. Statista. Forecast of the number of LinkedIn users in the World from 2017 to 2025. URL: https://www.statista.com/forecasts/1147197/linkedin-users-in-theworld

6. Statista. Number of monthly active Instagram users from 2013 to 2021. URL: https://www.statista.com/statistics/253577/number-of-monthly-activeinstagram-users

7. Statista. Number of monthly active Facebook users worldwide as of 1st quarter 2023. URL: https://www.statista.com/statistics/264810/number-of-monthlyactive-facebook-users-worldwide

8. Statista. Number of Twitter users worldwide from 2019 to 2024. URL: https://www.statista.com/statistics/303681/twitter-users-worldwide/

9. Michael Bazzell. "Hiding from the Internet: Eliminating Personal Online Information." 2016. с. 23

10. Michael Bazzell. "Open Source Intelligence Techniques: Resources for Searching and Analyzing Online Information." 2020. с. 53

11. Michael Bazzell. Open Source Intelligence Techniques. Resources for Searching and Analyzing. Sixth Edition. 2018. с. 58

12. Babak Akhgar, P. Saskia Bayerl, Fraser Sampson. "Open Source Intelligence Investigation: From Strategy to Implementation." 2019. с. 25

13. Закон України «Про затвердження Порядку класифікації надзвичайних ситуацій за їх рівнями»

14. Зеркалов Д. В. Безпека життєдіяльності. Навчальний посібник. 2011. - с. 263
15. Метеорологічні умови в приміщеннях URL: https://buklib.net/books/35226/
16. Національний стандарт України «ДСТУ-Н Б А.3.2.1:2007»
17. Розробка системи управління кіберінцидентами в мережах LTE // https://jrnl.nau.edu.ua/index.php/Infosecurity/article/view/13036/18086
18. Розвідка відкритих джерел інформації (OSINT) у розвідувальній практиці США / Кожушко Ольга Олегівна // http://jrnl.nau.edu.ua/index.php/IMV/article/viewFile/3264/321
19. Жидецький, В. І. Основи охорони праці / В. І. Жидецький – Л. : Афіша, 2005. – 349 с
20. Гандзюк, М. П. Основи охорони праці: підруч. / М. П. Гандзюк, Е. П. Желібо, М. О. Халимовський – К. : Каравела, 2005. – 393 с.
21. Бедрій, Я. І. Охорона праці : навч. посіб. / Я. І. Бедрій. – Львів: Афіша, 1997. – 258 с.
22. Дурдинця, В. В. Збірник нормативно-правових актів з питань надзвичайних ситуацій техногенного та природного характеру / В. В. Дурдинця. – К. : Чорнобиль інтерінформ, 2001. – 532 с.
23. Ткачук, К. Н. Охорона праці та промислова безпека / Ткачук К. Н., Зацарний В. В., Сабарно Р. В. – К. : Лібра, 2010. – 560 с.
24. Ткачук, К. Н. Основи охорони праці / К. Н. Ткачук, М. О. Халімовський, В. В. Зацарний. – К. : Основа, 2006. – 448 с.
25. Рожков, А. П. Пожежна безпека : навч. довід. / А. П. Рожков. – К., 1999. – 256 с.
26. 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.
27. Москальова, В. М. Основи охорони праці : підруч./ В. М. Москальова. – К., 2005. – 208 с.
28. Антонюк В. В. Організаційно-правові засади формування та реалізації державної політики інформаційної безпеки України: //

http://academy.gov.ua/pages/dop/138/files/8de62817-e4bf-40d8-acb0-96384ec79f34.pdf
29. ДСТУ ISO/IEC 27000:2015 Інформаційні технології. Методи захисту. Система управління інформаційною безпекою. Огляд і словник (ISO/IEC 27000:2014, IDT).
30. Заєць П.М., Іванова О.С. Визначення підходів щодо впровадження засобів і систем автоматизації процесів управління інформаційною безпекою організації // https://academy.ssu.gov.ua/uploads/p_57_35588992.pdf
31. ДСТУ ISO/IEC 27001:2015 Інформаційні технології. Методи захисту системи управління інформаційною безпекою. Вимоги (ISO/IEC 27001:2013; Cor1:2014, IDT).
32. Серватнюк М. Інтеграція методів OSINT в систему управління інформаційним ризиками. ІНФОРМАЦІЙНІ МОДЕЛІ, СИСТЕМИ ТА ТЕХНОЛОГІЇЇ : IX науково-техн. конф., м. Тернопіль, 8–9 груд. 2021 р. 2021. с.76.
33. Купчик, М. П. Основи охорони праці / М. П. Купчик. – К. : Основа, 2000. – 416 с.
34. Керб, л. П. Основи охорони праці : навч. Посіб. / л. П. Керб. – К. :кнеу, 2003. – 215 с.
35. Гончарук, В. Є. Оцінка обстановки у надзвичайних ситуаціях : навч. посіб. / В. Є. Гончарук. – Львів, Видавництво НУ “Львівська політехніка”, 2004. – 136 с.
36. Сєріков, Я. О. Основи охорони праці : навч. посіб. / Я. О. Сєріков. – Харків, ХНАМГ, 2007. – 227с.
37. Васюк К. В. Автоматизація збору корпоративної та особистої інформації з відкритих джерел : кваліфікаційна робота бакалавра за спеціальністю „125 — кібербезпека“ / К. В. Васюк — Тернопіль : ТНТУ, 2021. — 73 с.
38. Andy Greenberg. The Confessions of Marcus Hutchins, the Hacker Who Saved the Internet // https://www.wired.com/story/confessions-marcus-hutchins-hacker-who-saved-the-internet/

39. Who Is Marcus Hutchins? // https://krebsonsecurity.com/2017/09/who-is-marcus-hutchins/