МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ПОЛІСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет інформаційних технологій,
обліку та фінансів
Кафедра комп'ютерних технологій
і моделювання систем

Кваліфікаційна робота
на правах рукопису

Заглинський Вадим Анатолійович
(прізвище, ім'я, по батькові здобувача освіти)

УДК 004.056:004.9

КВАЛІФІКАЦІЙНА РОБОТА

Дослідження технологій OSINT-розвідки для виявлення і реагування на загрози кібербезпеки

(тема роботи)

125 «Кібербезпека та захист інформації»

(шифр і назва спеціальності)

Подається на здобуття освітнього ступеня магістр

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

В.А.Заглинський

(підпис, ініціали та прізвище здобувача вищої освіти)

Керівник роботи
Молодецька Катерина Валеріївна
(прізвище, ім'я, по батькові)
д.т.н., професор
(науковий ступінь, вчене звання)

Житомир – 2024

АНОТАЦІЯ

Заглинський В.А. Дослідження технологій OSINT-розвідки для виявлення і реагування на загрози кібербезпеки. – Кваліфікаційна робота на правах рукопису.

Кваліфікаційна робота на здобуття освітнього ступеня магістр за спеціальністю 125 – кібербезпека. – Поліський національний університет, Житомир, 2024.

Зважаючи на постійний та невпинний розвиток загроз виникає необхідність використання інструментів OSINT для ідентифікації та прогнозування загроз.

Дипломна робота спрямована на дослідження та покращенні сучасних методик використання OSINT в сфері інформаційної безпеки та кіберзахисту.

Отримані результати можуть бути використані для розуміння принципу використання OSINT з метою попередження та раннього виявлення загроз, а також слугувати основою для подальшого поглибленого вивчення даної проблематики.

Ключові слова: OSINT, КІБЕРЗАГРОЗИ, МЕТОДИКА, ІНФОРМАЦІЯ, ВІДКРИТІ ДАНІ.

SUMMARY

Zahlynsky V. A. Research of OSINT intelligence technologies for detecting and responding to cybersecurity threats. - Qualification work on the rights of the manuscript.

Qualification work for the master's degree in specialty 125 – cybersecurity. - Polis National University, Zhytomyr, 2024.

Due to the constant and continuous development of threats, there is a need to use OSINT tools to identify and predict threats.

The thesis is aimed at research and improvement of modern methods of using OSINT in the field of information security and cyber defense.

The results obtained can be used to understand the principle of using OSINT for Threat Prevention and early detection, as well as serve as a basis for further in-depth study of this issue.

Keywords: OSINT, CYBER THREATS, METHODOLOGY, INFORMATION, OPEN DATA.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ……...5

ВСТУП……..6

РОЗДІЛ 1 АНАЛІЗ СУЧАСНОГО СТАНУ ЗАСТОСУВАННЯ ТЕХНОЛОГІЙ OSINT-РОЗВІДКИ ДЛЯ ВИЯВЛЕННЯ І РЕАГУВАННЯ НА ЗАГРОЗИ КІБЕРБЕЗПЕКИ……...8

1.1 OSINT як технологія добування інформації з відкритих джерел…….8

1.2 Підходи до застосування технологій OSINT в кібербезпеці……...11

Висновки до розділу 1……...12

РОЗДІЛ 2 МЕТОДИКА ЗАСТОСУВАННЯ ТЕХНОЛОГІЙ OSINT ДЛЯ ВИЯВЛЕННЯ І РЕАГУВАННЯ НА КІБЕРЗАГРОЗИ……...13

2.1 Класифікація загроз, які виявляються засобами OSINT…….....13

2.2 Розроблення методики використання OSINT……...16

Висновки до розділу 2……...22

РОЗДІЛ 3 ЕКСПЕРИМЕНТАЛЬНЕ ДОСЛІДЖЕННЯ ЕФЕКТИВНОСТІ ТЕХНОЛОГІЙ OSINT ДЛЯ ВИЯВЛЕННЯ І РЕАГУВАННЯ НА КІБЕРЗАГРОЗИ…….23

3.1 Приклад використання OSINT для аналізу та реагування на кіберзагрози…….…23

3.2 Оцінка ефективності запропонованої методики та практичні рекомендації…….27

Висновки до розділу 3……...29

ВИСНОВКИ……31

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ……...32

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

OSINT – Open source intelligence;

США – Сполучені Штати Америки;

OSIF – open source information;

ЗМІ – засоби масової інформації;

CVEs – Common Vulnerabilities and Exposures;

SSL/TLS – Secure Sockets Layer/Transport Level Security.

ВСТУП

Актуальність теми. У сучасному світі стрімкий розвиток інформаційних технологій і цифрових інфраструктур створює нові можливості, але водночас породжує значні виклики, зокрема у сфері кібербезпеки. З огляду на зростання кількості кібератак і їх різноманітності, технології збору інформації з відкритих джерел (OSINT) стають надзвичайно актуальними для виявлення та попередження потенційних загроз. OSINT дозволяє своєчасно отримувати необхідну інформацію для аналізу та реагування на інциденти, що робить її важливим інструментом у боротьбі з кіберзагрозами[1].

Актуальність обраної теми полягає в дослідженні ефективності OSINT-технологій як ключового елемента сучасної кібербезпеки[2]. Використання таких інструментів є важливим для підвищення рівня захисту інформаційних систем, виявлення вразливостей і попередження можливих атак, що дозволяє мінімізувати ризики для користувачів та організацій.

Мета і задачі дослідження. Метою даної роботи є розроблення та аналіз методики застосування технологій OSINT для виявлення і реагування на кіберзагрози.

Основними завданнями є:

1. аналіз сучасного стану використання OSINT у сфері кібербезпеки;
2. розроблення методики застосування OSINT для ефективного реагування на загрози;
3. експериментальне дослідження запропонованої методики та оцінка її ефективності.

Об’єкт дослідження. Об’єктом дослідження є процес виявлення та реагування на кіберзагрози із застосуванням технологій OSINT.

Предмет дослідження. Предметом дослідження виступають технології OSINT, їх методи і підходи для забезпечення кібербезпеки, а також способи їх практичного застосування.

Наукова новизна одержаних результатів. Науковою новизною роботи є вдосконалення методики використання OSINT для виявлення та реагування на кіберзагрози, яка відрізняється від відомих врахуванням типу загрози для визначення послідовності дій, що довзоляє не лише підвищити оперативність виявлення загроз, а й підвищити рівень захисту.

Практичне значення одержаних результатів. Запропонована методика та способи її реалізації доцільно використовувати для підвищення рівня захисту інформаційних систем, моніторингу потенційних загроз та забезпечення оперативного реагування. Результати дослідження сприятимуть підвищенню ефективності кіберзахисту як у приватному, так і в державному секторах.

1 АНАЛІЗ СУЧАСНОГО СТАНУ ЗАСТОСУВАННЯ ТЕХНОЛОГІЙ OSINT-РОЗВІДКИ ДЛЯ ВИЯВЛЕННЯ І РЕАГУВАННЯ НА ЗАГРОЗИ КІБЕРБЕЗПЕКИ

1.1. OSINT як технологія добування інформації з відкритих джерел

У XXI столітті відбувається інтенсивний розвиток інформаційних технологій, що зумовлює зростання ролі та значення інформації у всіх сферах діяльності. Станом на сьогодні до 95% інформації можна знайти в мережі інтернет, що робить доступ до даних швидким і зручним[3]. В умовах глобальної цифровізації виникає необхідність у визначенні концепції Open Source Intelligence (OSINT), її методів та інструментів для забезпечення інформаційної безпеки.

OSINT — це сукупність методів і технологій для збору, аналізу та використання інформації з відкритих джерел з метою ухвалення обґрунтованих рішень у сфері безпеки[4]. Важливо зазначити, що під розвідкою в контексті OSINT слід розуміти не лише збір даних, але й аналітичну обробку, результатом якої є створення інтелектуальної інформації та аналітичних звітів [5].

Актуальність дослідження OSINT обумовлена стрімким зростанням кіберзагроз та підвищенням ролі інформаційної безпеки у сучасному суспільстві[6]. Згідно зі звітом компанії Cybersecurity Ventures, збитки від кіберзлочинності у 2023 році сягнули 8 трильйонів доларів США і, за прогнозами, можуть зрости до 10,5 трильйонів доларів до 2025 року[7]. Цей стрімкий ріст обумовлює необхідність використання інструментів для ідентифікації та прогнозування загроз, серед яких OSINT займає ключову позицію.

У контексті цифрової трансформації різних сфер діяльності — від державного управління до приватного бізнесу — зростає попит на своєчасну та достовірну інформацію з відкритих джерел. Згідно з дослідженням Forrester Research, понад 53% організацій повідомили про підвищення попиту на інструменти моніторингу відкритих джерел для запобігання загрозам[5]. OSINT

дозволяє оперативно ідентифікувати потенційні загрози, прогнозувати можливі ризики та приймати обґрунтовані управлінські рішення[8].

Зростання масштабів кіберзлочинності підтверджується також даними від IBM X-Force, які показують, що кількість атак типу "ransomware" зросла на 13% у 2023 році порівняно з попереднім роком[9]. Використання OSINT-методів дозволяє організаціям ідентифікувати такі загрози ще на стадії їх планування, наприклад, шляхом моніторингу даркнет-форумів, де злочинці часто обговорюють свої майбутні атаки[10].

OSINT відрізняється від Open Source Information (OSIF), що включає загальнодоступні дані та інформацію, яка циркулює у відкритих медіаканалах. На відміну від OSIF, OSINT є цілеспрямованим збором і систематизацією інформації для розв’язання конкретних завдань[11]. Проблемним аспектом виступає необхідність ідентифікації надійних джерел та оцінки достовірності отриманої інформації.

Відкриті джерела інформації включають різноманітні ресурси, такі як:

- інтернет-форуми, блоги, соціальні мережі, відеоплатформи (YouTube);
- Вікіпедія, реєстраційні записи доменів Whois, метадані цифрових файлів;
- веб-сайти даркнету, геолокаційні дані, IP-адреси та контактні дані;
- дипломатичні місії, архіви, бібліотеки, дослідницькі центри, а також тези та дисертації [12].

Критичне значення має здатність відрізняти достовірні джерела від недостовірних та корелювати інформацію з різних джерел для зменшення ризику отримання недостовірних відомостей.

Послідовність пошуку інформації з відкритих джерел зображено на рис. 1.1.

Інформація з відкритих джерел має низку переваг, які підвищують її цінність порівняно з таємними розвідувальними даними:

- швидкість — у разі кризової ситуації в певному географічному регіоні, відсутність локальних джерел інформації може бути компенсована пошуком відомостей у відкритих джерелах (телебачення, Інтернет);

Рисунок 1.1 – Послідовність пошуку інформації з відкритих джерел

- кількість — кількість блогерів, журналістів та аналітиків, що працюють із відкритими джерелами, значно перевищує кількість професійних розвідників;
- якість — інформація з відкритих джерел, зазвичай, менш спотворена, ніж та, що надходить із конфіденційних джерел;
- прозорість — відкриті джерела дозволяють оцінити надійність отриманої інформації, що не завжди можливо у випадку секретної розвідки;
- простота використання — доступ до відкритої інформації не обмежується секретністю та не потребує спеціальних дозволів;
- вартість — збирання інформації з відкритих джерел є значно дешевшим порівняно з запуском та обслуговуванням розвідувальних супутників[13].

1.2 Підходи до застосування технологій OSINT в кібербезпеці

Методи розвідки на основі відкритих джерел корисними для експертів із безпеки у виявленні внутрішніх і зовнішніх загроз для організацій та приватних осіб. Вони дозволяють знаходити дані про співробітників, структуру компаній, фінансові звіти та іншу інформацію, що може бути використана

зловмисниками[14].

Особливу загрозу становлять метадані, опубліковані фізичними чи юридичними особами, які можуть включати:

- незахищені з’єднання та порти пристроїв;
- неоновлене програмне забезпечення;
- інформацію про пристрої, версії програмного забезпечення, мережу та IP-адреси;
- витік вихідного коду на платформах типу GitHub [15].

Потенційні точки входу для зловмисників можна класифікувати на кілька категорій:

- інформаційні системи на периметрі мережі (сервери, робочі станції);
- мобільні пристрої співробітників, що використовуються як усередині, так і за межами периметра;
- хмарні сервіси та облікові записи, зокрема ті, що використовуються у приватних цілях [16].

Точки входу можуть бути використані для проведення фішингових атак або отримання доступу до корпоративної мережі, що створює додаткові вектори атак. У сучасних умовах концепція периметра мережі поступово зникає через поширення хмарних технологій та концепцію BYOD (Bring Your Own Device), що ускладнює контроль за потоком даних між внутрішніми та зовнішніми ресурсами компанії[17].

Невидима мережа (Deep Web) включає ресурси, які не індексуються стандартними пошуковими системами. Вона охоплює приватні соціальні мережі, закриті бази даних та інтранети, доступ до яких можливий лише за допомогою спеціальних інструментів. Хоча ці ресурси вважаються загальнодоступними, для доступу до них потрібні спеціалізовані знання та технології [18].

Висновки до першого розділу

Методи та інструменти OSINT дозволяють збирати, аналізувати та структурувати інформацію з відкритих джерел з метою забезпечення інформаційної безпеки. Використання OSINT як превентивного заходу може запобігти масштабним кібератакам та зменшити ризики витоку інформації. Аналітика, отримана за допомогою OSINT, сприяє посиленню фінансової безпеки організацій та захисту від можливих загроз. У майбутньому розвиток технологій OSINT та інтеграція з методами штучного інтелекту дозволить ще ефективніше ідентифікувати вразливості та нейтралізувати кіберзагрози.

2 МЕТОДИКА ЗАСТОСУВАННЯ ТЕХНОЛОГІЙ OSINT ДЛЯ ВИЯВЛЕННЯ І РЕАГУВАННЯ НА КІБЕРЗАГРОЗИ

2.1 Класифікація загроз, які виявляються засобами OSINT

Застосування технологій OSINT у сфері кібербезпеки дозволяє ідентифікувати, аналізувати та запобігати різноманітним загрозам, що можуть поставити під загрозу безпеку інформаційних систем, конфіденційність даних та стабільність бізнес-процесів. Завдяки широкому спектру інструментів та методів, OSINT забезпечує гнучкість і ефективність виявлення загроз різної природи, походження та критичності[19]. Розглянемо детальну класифікацію таких загроз.

Загрози, які можна виявити за допомогою OSINT, класифікуються за кількома критеріями: джерело походження**,** тип загрози**,** вектор атаки та ступінь критичності[20]. Кожен із цих критеріїв дозволяє краще зрозуміти природу загроз та визначити оптимальні стратегії протидії.

Загрози можуть мати як зовнішнє, так і внутрішнє походження.

Зовнішні загрози походять від суб'єктів, що перебувають за межами організації. Серед них найпоширеніші такі:

- кіберзлочинці та хакерські угруповання — зловмисники, що здійснюють атаки для викрадення даних, шантажу або зловживання ресурсами організації. OSINT дозволяє виявити підготовку до таких атак шляхом моніторингу форумів даркнету, соціальних мереж та публікацій у ЗМІ;

- конкуренти — у деяких випадках конкуренти можуть використовувати OSINT для шпигунства та отримання стратегічної інформації про компанію, її клієнтів або продукти. Моніторинг активності конкурентів у відкритих джерелах дозволяє виявляти можливі спроби отримання конфіденційної інформації;

- державні структури — деякі уряди використовують OSINT для проведення розвідки та здійснення кібероперацій. Державні організації можуть проводити інформаційні кампанії, спрямовані на дезінформацію або шпигунство,

а також аналізувати діяльність приватних організацій з метою підготовки до кібератак[21].

Внутрішні загрози виникають унаслідок дій співробітників або партнерів організації. Вони можуть бути:

- ненавмисні — помилки співробітників, що призводять до витоків інформації або створення уразливостей у системі. Прикладом є випадкове оприлюднення конфіденційної інформації у відкритих джерелах, що може бути виявлено за допомогою OSINT;

- навмисні — зловмисні дії працівників, що мають доступ до критично важливої інформації (саботаж, крадіжка даних, передача інформації конкурентам). Використовуючи OSINT, можна відстежувати діяльність таких співробітників у соціальних мережах або інтернет-форумах.

OSINT дозволяє виявити як технічні, так і інформаційні загрози[22].

Технічні загрози — це уразливості, пов’язані з апаратним та програмним забезпеченням. Серед них:

- вразливості програмного забезпечення (Zero-Day) — виявлення публікацій про уразливості у відкритих джерелах або на форумах даркнету. OSINT-інструменти можуть автоматично моніторити такі ресурси для швидкого реагування на можливі загрози;

- небезпечні конфігурації — помилкові налаштування мережевих пристроїв або серверів, що можуть бути знайдені через відкриті сканери, такі як Shodan або Censys;

- застарілі системи — відомості про використання застарілого ПЗ, яке більше не підтримується розробниками, можуть бути виявлені через повідомлення у відкритих джерелах або форумах технічної підтримки[23].

Інформаційні загрози стосуються маніпулювання та витоку інформації. Основні приклади:

- фішинг — ідентифікація підроблених веб-сайтів або електронних листів, що збираються через OSINT-інструменти, які відстежують фішингові домени[24];

- витік конфіденційної інформації — пошук витоків у публічних базах даних, а також витоків через несанкціоновані публікації співробітників у соціальних мережах[25].

- маніпуляції в соціальних мережах — створення фейкових акаунтів для поширення дезінформації або маніпулювання суспільною думкою[24].

OSINT дозволяє виявити загрози, які спрямовані як на інформаційні системи організації, так і на людський фактор[26]. Атаки на системи включають:

- використання уразливостей у системах — пошук інформації про вразливі сервери або бази даних через сканери та даркнет-ресурси;

- атаки на інфраструктуру — відстеження кіберзлочинних обговорень у форумах даркнету щодо планованих атак на певні організації[27].

Атаки на користувачів зосереджені на співробітниках та клієнтах організації:

- соціальна інженерія — OSINT дозволяє ідентифікувати інформацію про співробітників (контакти, звички, місця перебування), яка може бути використана для проведення таргетованих атак;

- фішинг та спірфінг — відстеження підроблених листів, доменів та фальшивих сайтів[28].

OSINT дає можливість оцінити загрозу за її критичністю для організації:

- критичні загрози — інциденти, що можуть призвести до значних фінансових втрат, зупинки бізнес-процесів або компрометації ключових систем.

Загрози середньої критичності — вони можуть негативно впливати на певні процеси, але не зупиняють їх повністю.

Незначні загрози — загрози, які мають мінімальний вплив на організацію, але у випадку ігнорування можуть накопичуватися та перерости у більш серйозні проблеми[29].

2.2 Розроблення методики використання OSINT

Розробка та реалізація плану досліджень OSINT — це ключовий етап у забезпеченні кібербезпеки організації. Використання OSINT дозволяє отримувати цінну інформацію з відкритих джерел, яка допомагає виявляти загрози, оцінювати ризики та ухвалювати обґрунтовані управлінські рішення[30]. Щоб досягти максимальної ефективності, OSINT-дослідження має проводитися за чітко визначеним планом, який враховує всі етапи процесу — від формулювання цілей до підготовки звіту та впровадження заходів реагування. На рис. 2.1 показано узагалений вигляд послодосності дій від моменту початку дослідження загрози і д моменту реагування на неї.

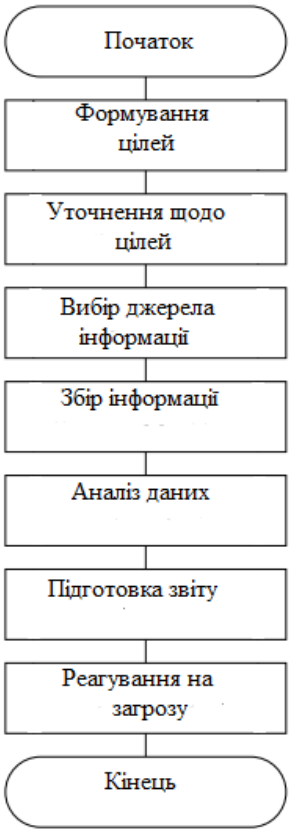

Рисунок 2.1 – Послідовність дій під час реагування на загрозу

Етап 1. На першому етапі відбувається формулювання цілей дослідження. Воно являється першим та ключовим етапом у процесі OSINT-аналізу. Він дозволяє визначити, що саме потребує уваги та які завдання слід вирішити.

Етап 2. На цьому етапі чітке формулювання цілей дозволяє оптимізувати процес дослідження, уникнути зайвих витрат ресурсів та забезпечити якісні результати, але можливі труднощі із деталізацією цілей, що може ускладнити наступні кроки дослідження[31].

Етап 3. Третій крок – це вибір джерел інформації. На цьому етапі визначаються джерела, з яких буде отримана інформація, та інструменти, які забезпечують ефективний збір даних. Правильно обрані джерела забезпечують швидкість і точність збору даних, а от у випадку неправильного їх обрання можна отримати неревалентні результати[32].

Етап 4. Після попередніх трьох на етапів ми починаємо збір інформації. Використання спеціалізованих інструментів дозволяє автоматизувати процес збору та аналізу великих обсягів даних, що значно підвищує швидкість і точність виявлення загроз[33].

Have I Been Pwned — це популярний веб-сервіс, що дозволяє перевірити, чи були ваші облікові дані скомпрометовані у відомих витоках інформації[25]. Принцип роботи даного сервісу полягає у пошуку в базах даних витоків, зокрема адрес електронної пошти та паролів. Перевагами є простота використання, безкоштовний доступ, швидке отримання результатів. До недоліків варто віднести обмежений набір даних, неможливість автоматизованого моніторингу у реальному часі.

SpiderFoot — це потужний інструмент для автоматизованого збору даних із різних джерел, що дозволяє проводити комплексний аналіз кіберзагроз[27]. Інструмент використовує понад 200 модулів для збору даних про домени, IP-адреси, акаунти тощо. Його перевагою є автоматизація збору великих обсягів даних, інтеграція з іншими інструментами. А недоліком можна віднести потребу в налаштуванні модулів, можливе перевантаження інформацією, яку необхідно додатково фільтрувати.

Maltego — це один із найбільш відомих інструментів OSINT, який спеціалізується на візуалізації зв’язків між різними об’єктами. Завдяки цьому інструменту аналітики можуть проводити розслідування та відстежувати зв’язки

між доменами, IP-адресами, соціальними профілями, організаціями та іншими сутностями. Основна перевага Maltego полягає у здатності будувати графічні схеми взаємозв'язків, що дозволяє простіше і швидше ідентифікувати потенційні загрози [33].

Інструмент дозволяє користувачам проводити розслідування кіберінцидентів, виявляти цифрові сліди та будувати взаємозв'язки між різними об'єктами, що сприяє виявленню складних мереж загроз. Він активно використовується фахівцями з кібербезпеки, правоохоронними органами та приватними компаніями для аналізу кіберзлочинності та проведення OSINT-розслідувань.

Недолікими даного інструмента можна назвати високу вартість – ліцензія на повну версію Maltego може бути досить дорогою, що може бути перешкодою для малих компаній або індивідуальних користувачів, а також складність в навчанні – інструмент має досить складний інтерфейс, що може вимагати значного часу для освоєння.

На рис. 2.2 показано приклад роботи Maltego

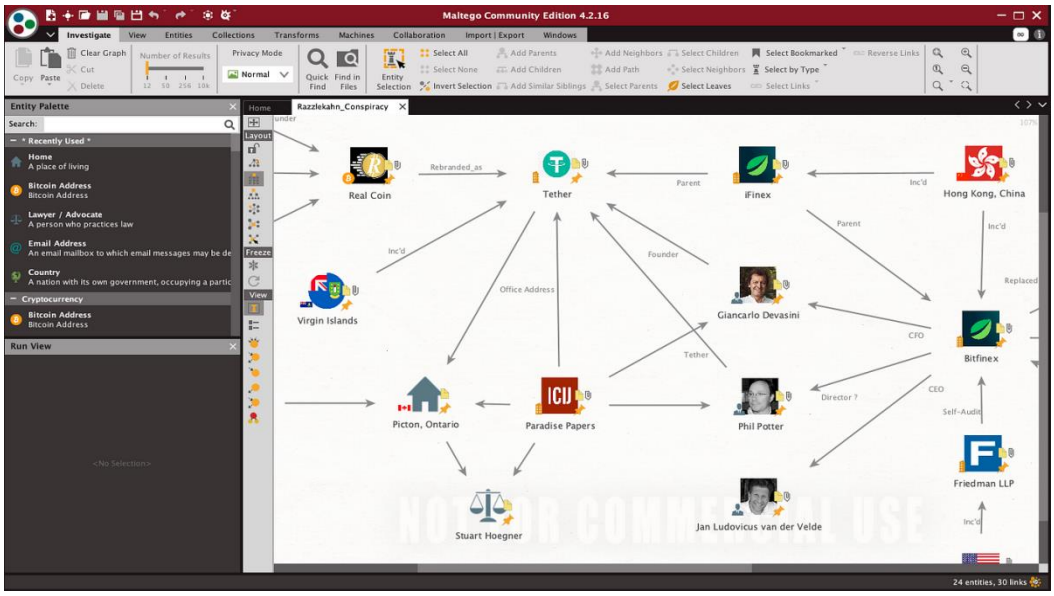

Рисунок 2.2 – Приклад роботи програми Maltego

Sherlock — це інструмент для пошуку облікових записів користувачів у соціальних мережах за іменем користувача[34]. Він особливо корисний для виявлення потенційно підозрілих акаунтів. Пошук акаунтів у різних соцмережах

здійснюється за заданим іменем користувача. Простота використання, висока швидкість пошуку, підтримка численних платформ являється плюсом даного інструменту, але в нього також є і недоліки – залежність від API соцмереж, обмежена функціональність без додаткових налаштувань.

OSRFramework — це набір інструментів для пошуку та аналізу даних про облікові записи, домени та інші відкриті джерела інформації[35]. За його допомогою здійснюється аналіз облікових записів і доменів для отримання інформації про цільові об’єкти. Перевагами являється широкий спектр підтримуваних джерел, гнучкість у використанні. Потреба в налаштуванні та складність для новачків являються його мінусом.

Social-Searcher і Brandwatch — це інструменти для моніторингу згадок брендів у соціальних мережах і збору аналітичних даних[36]. Вони активно використовуються для вивчення конкурентів і аналізу громадської думки. За допомогою цих інструментів можна побудувати також звіти про активність. Доступ до даних у реальному часі, зручний інтерфейс для аналітики являються позитивною стороною цих інструментів, але вони мають обмежені можливості в безкоштовних версіях, а вартість повного функціоналу досить висока.

Shodan — це унікальна пошукова система(рис. 2.3), яка дозволяє знаходити пристрої, підключені до інтернету, та отримувати інформацію про їхні відкриті порти, конфігурації та інші технічні параметри[37]. На відміну від традиційних пошукових систем, які індексують веб-сторінки, Shodan фокусується на виявленні серверів, маршрутизаторів, камер спостереження, пристроїв Інтернету речей (IoT) та інших мережевих пристроїв[38].

Shodan дозволяє користувачам проводити пошук пристроїв, які мають відкриті порти або надають публічний доступ до своїх інтерфейсів. Завдяки цьому аналітики можуть визначити пристрої, які можуть бути вразливими до атак. інструмент сканує відкриті порти на пристроях, що дозволяє виявити, які саме служби та програми працюють на цих пристроях. Це дає змогу визначити, які саме служби можуть бути вразливими.

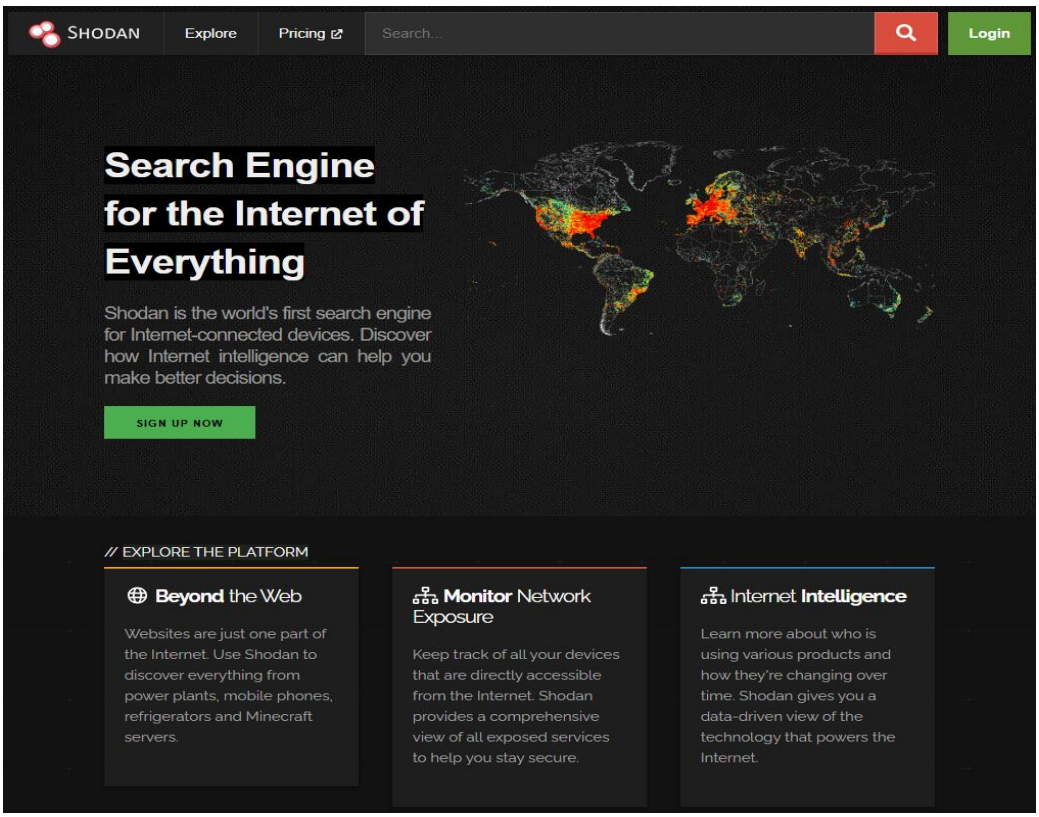

Рисунок 2.3 – Головна сторінка інструменту OSINT – Shodan

Shodan допомагає ідентифікувати пристрої з незахищеними налаштуваннями, застарілим програмним забезпеченням або відомими вразливостями, які можуть бути використані для атак зловмисниками.

Shodan дозволяє контролювати стан мережевих пристроїв та відстежувати зміни в їхній конфігурації. Це може бути корисним для своєчасного виявлення несанкціонованих змін або нових пристроїв, підключених до мережі. Разом з тим, Shodan отримує інформацію виключно з відкритих портів пристроїв. Якщо порт закрито або доступ обмежено брандмауером, Shodan не зможе ідентифікувати пристрій або зібрати про нього дані.

Для того, щоб ефективно використовувати можливості Shodan, користувачі повинні володіти глибокими знаннями у сфері мережевих технологій, зокрема розуміти, як працюють порти, протоколи та методи доступу до пристроїв.

Повний доступ до функціоналу Shodan можливий лише за наявності платної підписки, яка відкриває більше можливостей для глибокого сканування та доступу до архівних даних.

Shodan активно використовується у сфері кібербезпеки для оцінки рівня

захищеності мережевої інфраструктури. Завдяки здатності виявляти пристрої з незахищеними конфігураціями, кібербезпекові фахівці можуть своєчасно вжити заходів для усунення вразливостей. Shodan також використовується у процесах аудиту безпеки та оцінки ризиків, дозволяючи компаніям визначати слабкі місця у своїх мережах.

Загалом, Shodan — це потужний інструмент для аналізу мережевих пристроїв та оцінки стану кібербезпеки організацій. Він дозволяє виявляти вразливі пристрої та контролювати мережеву інфраструктуру в реальному часі. Хоча інструмент потребує певного рівня технічної підготовки, його можливості роблять його цінним інструментом для аудиту безпеки та моніторингу мереж.

Автоматизація пошуку інформації спрощує роботу та пришвидшує отримання необхідної інформації, але у випадку неправильно вибраного інструменту можна отримати не зовсім актуальні дані.

Етап 5. На п’ятому етапі проводимо аналіз даних, що дозволяє виявити зв’язки між об’єктами та оцінити ризики.

Дії на даному етапі дозволяють виявити приховані загрози, але насправді він може бути неймовірно затратним у часу через великий обсях даних.

Етап 6. Наступним кроком у нас іде підготовка звіту.

Етап 7. На цій стадії у нас є реагування на загрози, на якому виконуються заходи для нейтралізації загроз.

Разом з тим, якщо слідувати виключно до вищевказаних кроків, то це буде не зовсім доцільно і результативно, оскільки кількість інструментів та програм для OSINT використовується у кібербезпеці, вони стосуються переважно загального порядку проведення розвідки на основі відкритих джерел. Саме тому, коли мова йде про використання OSINT в забезпеченні інформаційної чи кібербезпеки, то ми повинні розробити нові методики для оперативного реагування на їх виникнення[39]. Наявність швидкого доступу до даних дозволяє знизити ризик витоку інтелектуальної власності або інших конфіденційних даних. Також варто чітко сформулювати перелік інструментів, які будемо застосовувати залежно від дослідження можливих загроз. Це особливо актуально в умовах, коли

компанії ведуть бізнес на міжнародному рівні, і деякі загрози можуть надходити з-за кордону.

Висновок до другого розділу

Завдяки широкому спектру інструментів, таких як Shodan, Maltego, SpiderFoot та інші, OSINT дозволяє здійснювати моніторинг та аналіз відкритих джерел для виявлення зовнішніх і внутрішніх загроз, оцінки їх критичності та формування стратегій реагування.

Класифікація загроз за джерелами, типом, вектором атаки і ступенем критичності сприяє глибшому розумінню їх природи та мінімізації ризиків. Важливою частиною роботи з OSINT є розробка чіткого плану досліджень, визначення цілей та об’єктів, а також використання сучасних інструментів для збору та аналізу даних.

Попри певні обмеження, як-от складність освоєння чи вартість деяких інструментів, OSINT забезпечує високу точність та швидкість виявлення загроз, підвищуючи рівень кібербезпеки організацій. Ефективне використання цих технологій дозволяє не лише протидіяти поточним загрозам, але й запобігати можливим атакам у майбутньому. І, незважаючи на усі переваги OSINT та його окремих інструментів, потрібно працювати над їх вдосконаленням.

3 ЕКСПЕРИМЕНТАЛЬНЕ ДОСЛІДЖЕННЯ ЕФЕКТИВНОСТІ ТЕХНОЛОГІЙ OSINT ДЛЯ ВИЯВЛЕННЯ І РЕАГУВАННЯ НА КІБЕРЗАГРОЗИ

3.1. Приклад використання OSINT для аналізу та реагування на кіберзагрози

OSINT являє собою сукупність методик і технологій збору та аналізу інформації з відкритих джерел з метою виявлення потенційних загроз. І для забезпечення кібербезпеки пропонується використовувати інші методики, ніж ті, які є загальноприйнятими, адже завчасно ми розуміємо який тип загрози збираємося досліджувати.

Перший спосіб реалізації методики. Виявлення вразливостей у публічних ресурсах. Для цього використовують пошукові системи, такі як Shodan, Censys та ZoomEye, для аналізу IP-адрес, відкритих портів та активних служб.

Процес відбувається у наступній послідовності:

1. ідентифікація діапазону IP-адрес та цільових пристроїв для сканування;
2. використання інструментів OSINT для збору інформації про відкриті порти, версії програмного забезпечення та служби, що працюють на цільових пристроях;
3. зіставлення отриманих даних із відомими вразливостями (CVEs) та створення звітів про ризики.

В результаті використання даної методики відбувається виявлення небезпечних служб та пристроїв, таких як веб-сервери, маршрутизатори, камери спостереження, що дозволяє запобігати можливим атакам.

Другий спосіб реалізації методики. Моніторинг даркнету та форумів зловмисників. В даному випадку використовують сервіси моніторингу «темного інтернету», такі як DarkOwl, Constella та спеціалізованих ботів для автоматичного збору інформації.

Послідовність застосування:

1. визначення ключових слів і тем для моніторингу на форумах даркнету;
2. використання ботів для автоматичного відстеження нових публікацій та дискусій;
3. аналіз зібраної інформації та виділення потенційних загроз.

Як результат ми отримуємо інформацію про можливі витоки даних, майбутні атаки та продаж краденої інформації.

Третій спосіб реалізації методики. Виявлення витоків конфіденційної інформації. В даній методиці застосовуються інструменти для моніторингу, такі як SpyCloud, Have I Been Pwned? та OSINT-платформи, що спеціалізуються на пошуку публікацій у відкритих джерелах[40].

Послідовність дій:

1. постійний моніторинг спеціалізованих майданчиків та баз даних з відкритим доступом;
2. сканування інтернет-ресурсів на наявність даних компанії (логінів, паролів, номерів рахунків тощо);
3. повідомлення відповідальних осіб про виявлення витоку та запуск процесу інцидентного реагування.

Завдяки виявленню витоків конфіденційної інформації є можливість швидко виявити факт витоку даних та вжити необхідних заходів для мінімізації збитків.

Четвертий спосіб реалізації методики. Виявлення фальшивих облікових записів у соціальних мережах. Для того, щоб виконати необхідні дії, використовуємо платформи, як Maltego, Social-Searcher та інших систем для моніторингу соціальних мереж.

Використовуючи дану методику, спершу відбувається налаштування фільтрів для відстеження підозрілих акаунтів за допомогою спеціалізованих інструментів. Потім відбувається виявлення акаунтів, що використовують схожі імена або фото з легітимних облікових записів. Наступним кроком буде ідентифікація та

позначення підозрілих акаунтів для подальшого аналізу та можливого блокування.

В результаті роботи буде заблоковано підозрілі акаунти та попереджено користувачів про загрози.

П’ятий спосіб реалізації методики. Відстеження реєстрації доменів та змін сертифікатів SSL/TLS. В даному випадку використовуються сервіси для моніторингу реєстрації доменів, такі як WhoisXML API та інструменти для відстеження змін у сертифікатах SSL/TLS[41].

Процес відстеження відбувається відповідно до наступних пунктів:

1. налаштування моніторингу для відстеження нових реєстрацій доменів, схожих на корпоративні;

2. аналіз змін у сертифікатах SSL/TLS для своєчасного виявлення нових сайтів, які можуть імітувати офіційний сайт компанії;

3. оповіщення про підозрілі домени та сертифікати для вжиття заходів реагування;

4. В результаті використання даної методики вдається виявляти спроби створити фішингові сайти та захиститися від атак на користувачів компанії.

Узагальнено кожну з методик, інструменти, що використовуються під час її реалізації, а також чітку послідовність дій під час реалізації показано у таблиці 3.1.

Таблиця 3.1 – Узагальнені дані по методиці

Спосіб метоодики	**Основні OSINT інструменти, що використовуються**	**Послідовність дій**
Виявлення вразливостей у публічних ресурсах	Shodan, Censys та ZoomEye	1.ідентифікація діапазону IP-адрес та цільових пристроїв для сканування; 2.використання інструментів OSINT для збору інформації про відкриті порти, версії програмного забезпечення та служби, що працюють на цільових пристроях; 3.зіставлення отриманих даних із відомими вразливостями (CVEs) та створення звітів про ризики.

Продовження Таблиці 3.1.

Назва методики	**Основні OSINT інструменти, що використовуються**	**Послідовність дій**
Моніторинг даркнету та форумів зловмисників	DarkOwl, Constella	1.визначення ключових слів і тем для моніторингу на форумах даркнету; 2.використання ботів для автоматичного відстеження нових публікацій та дискусій; **3.аналіз зібраної інформації та** потенційних загроз.
Виявлення витоків конфіденційної інформації	SpyCloud, Have I Been Pwned?	1.постійний моніторинг спеціалізованих майданчиків та баз даних з відкритим доступом; 2.сканування інтернет-ресурсів на наявність даних компанії (логінів, паролів, номерів рахунків тощо); 3.повідомлення відповідальних осіб про виявлення витоку та запуск процесу інцидентного реагування.
Виявлення фальшивих облікових записів у соціальних мережах	Maltego, Social-Searcher	1.налаштування фільтрів для відстеження підозрілих акантів; 2.ідентифікація та позначення підозрілих акантів 3.блокування підозрілих акантів.
Відстеження реєстрації доменів та змін сертифікатів SSL/TLS	WhoisXML API	1.налаштування моніторингу для відстеження нових реєстрацій доменів, схожих на корпоративні; 2.аналіз змін у сертифікатах SSL/TLS для своєчасного виявлення нових сайтів, які можуть імітувати офіційний сайт компанії; 3.оповіщення про підозрілі домени та сертифікати для вжиття заходів реагування.

Відповідно до даних таблиці, можна зробити висновок, що при використанні запропонованих методик для реагування на кіберзагрози ми скорочуємо кількість кроків з семи (рисунок 2.1) до трьох (рисунок 3.1), що дозволяє нам скоротити час реагування чи виявлення загрози.

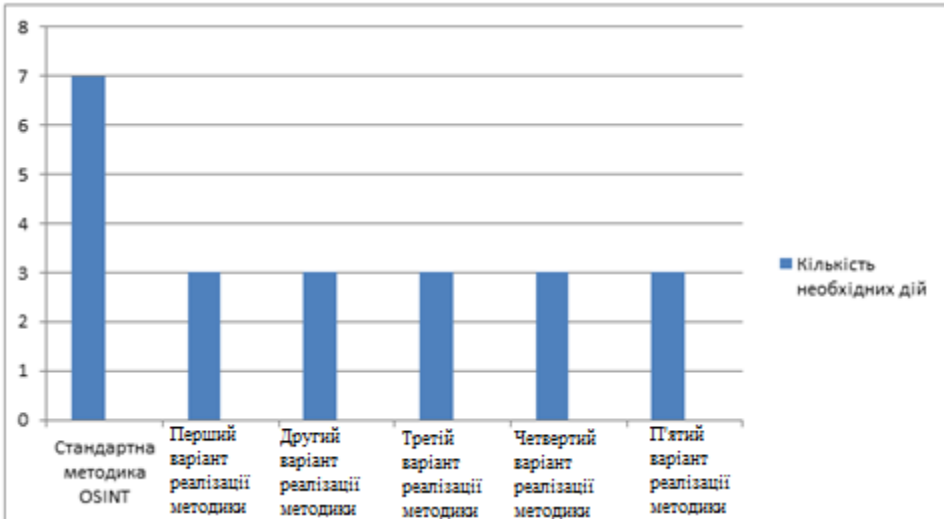

Рисунок 3.1 – Кількість кроків, необхідних для реагування на загрозу

3.2 Оцінка ефективності запропонованої методики та практичні рекомендації

Запропонована методика забезпечення кібербезпеки, що базуються на аналізі відкритих джерел інформації, є важливими інструментами для ефективного виявлення та запобігання потенційним загрозам. Кожна з них має свої переваги та особливості застосування, проте для досягнення максимального ефекту важливо поєднувати їх у комплексній системі моніторингу, що дозволяє отримати більш детальну картину ситуації[42].

Методика виявлення вразливостей у публічних ресурсах, що передбачає використання пошукових систем для аналізу відкритих портів, IP-адрес і служб, є необхідною для своєчасного виявлення небезпечних елементів у мережі. Вона дозволяє організаціям ідентифікувати слабкі місця своїх систем, які можуть бути використані зловмисниками для несанкціонованого доступу. Однак її застосування потребує чіткої регламентації, щоб уникнути порушення етичних

норм і правових аспектів, оскільки сканування мереж без належних дозволів може бути незаконним. Враховуючи високий темп розвитку нових уразливостей і змін у технологіях, важливо, щоб методика постійно адаптувалася до нових викликів і включала актуальні бази даних про вразливості.

Моніторинг даркнету та форумів зловмисників є ще одним важливим елементом стратегії кібербезпеки[43]. Використання автоматичних ботів для збору даних з цих джерел дозволяє швидко виявляти витоки конфіденційної інформації та попереджати про можливі загрози. Однак даркнет і зловмисні форуми є високодинамічними середовищами, де постійно змінюються методи та платформи для обміну інформацією. Тому важливо, щоб моніторингові системи були гнучкими та могли оперативно адаптуватися до нових умов. Також слід враховувати ризики, пов'язані з хибними спрацьовуваннями, і важливість правильної обробки отриманих даних, щоб уникнути зайвої тривоги або неадекватних реакцій.

Методика виявлення витоків конфіденційної інформації через спеціалізовані платформи дозволяє швидко реагувати на загрози, що виникають у результаті витоків даних з організацій. Це важливий інструмент для оперативного виявлення порушень безпеки та вжиття заходів з мінімізації збитків. Однак для забезпечення ефективності цієї методики необхідно, щоб платформи, що використовуються для моніторингу, мали доступ до актуальних баз даних і були здатні оперативно реагувати на нові загрози. Враховуючи постійне зростання кількості витоків конфіденційних даних, важливо, щоб ця методика постійно оновлювала свої алгоритми і забезпечувала максимальний рівень захисту.

Виявлення фальшивих облікових записів у соціальних мережах є необхідним для зменшення ризиків, пов'язаних з фішинговими атаками та іншими формами соціального інжинірингу. Враховуючи, що зловмисники часто використовують підроблені акаунти для маніпулювання інформацією, виявлення таких акаунтів є важливою складовою забезпечення безпеки в мережах. Проте важливо враховувати, що алгоритми для ідентифікації підозрілих акаунтів повинні постійно вдосконалюватися з урахуванням нових тактик, які

використовують зловмисники. Вони можуть застосовувати дедалі складніші методи маскування своїх акаунтів, тому традиційні підходи можуть виявитися недостатніми.

Моніторинг реєстрації доменів та змін сертифікатів SSL/TLS є важливим засобом для виявлення спроб створення підроблених вебсайтів, які можуть використовуватися для фішингових атак. Ця методика дозволяє оперативно виявляти підроблені сайти, що можуть маскуватися під офіційні ресурси, і забезпечувати своєчасну реакцію для запобігання атак. Однак для досягнення найкращих результатів важливо, щоб інструменти для моніторингу постійно оновлювалися і мали доступ до актуальних даних про реєстрації доменів та сертифікати SSL/TLS. Це дозволить знизити ризики помилок і забезпечити ефективний захист від фішингових атак.

В процесі проведення дослідження було встановлено, що завдяки розробленим методикам вдалося скоротити час реагування на можливі інциденти, оскільки ми завчасно розуміємо які інструменти використовуємо та що саме аналізуємо.

Загалом, запропоновані методики є важливими інструментами для забезпечення кібербезпеки, проте їх ефективність залежить від правильної інтеграції в загальну систему моніторингу та оперативного реагування на виявлені загрози. Використання таких методик потребує постійного вдосконалення та адаптації до нових умов кіберзагроз. Зокрема, важливим є забезпечення регулярного оновлення баз даних, адаптація інструментів до нових технологій та постійне навчання фахівців для правильного застосування цих методик.

Звісно, що кожну із запропонованих методик можна вдосконалювати. Це можна зробити різним чином. Наприклад, об’єднати усі п'ять методик у єдину платформу моніторингу, що дозволить оперативно отримувати дані з різних джерел та швидше реагувати на загрози. Така інтеграція підвищить ефективність та знизить витрати на управління окремими інструментами. Використання автоматизованих інструментів для збору та аналізу інформації зможе мінімізувати

вплив людського фактора та дозволить зменшити час реагування на кіберзагрози. Інтеграція з SIEM-системами забезпечить централізоване управління інцидентами безпеки. Ефективне використання OSINT-методик вимагає підготовки кваліфікованих фахівців, тому проведення тренінгів та навчальних програм підвищить рівень знань персоналу з питань виявлення загроз та роботи з сучасними інструментами кібербезпеки.

Збір інформації з відкритих джерел повинен здійснюватися відповідно до етичних норм та чинного законодавства. Дотримання конфіденційності та прав людини забезпечує легітимність використання OSINT-інструментів та знижує ризики юридичних санкцій.

Висновки до третього розділу

У третьому розділі було розглянуто застосування методик OSINT для аналізу та реагування на кіберзагрози, а також оцінено їхню ефективність. Представлені методики демонструють широкий спектр можливостей для виявлення потенційних загроз, зокрема виявлення вразливостей у публічних ресурсах, моніторинг даркнету, відстеження витоків конфіденційної інформації, ідентифікація фальшивих облікових записів у соціальних мережах та моніторинг реєстрацій доменів і змін SSL/TLS-сертифікатів.

Запропоновані методики довели свою ефективність у виявленні загроз та реагуванні на них. Їх використання дозволяє суттєво знизити ризики, пов'язані з кібератаками, витоками даних та іншими загрозами інформаційної безпеки. Проте важливим є дотримання етичних норм і законодавства, адаптація інструментів до змін у кіберпросторі, а також постійне навчання фахівців.

Серед ключових рекомендацій виділяється необхідність інтеграції методик в єдину платформу моніторингу для підвищення ефективності, автоматизація процесів збору та аналізу даних, а також співпраця з SIEM-системами для централізованого управління інцидентами.

Загалом, комплексний підхід до впровадження OSINT-методик забезпечує високий рівень захисту від кіберзагроз, дозволяє своєчасно ідентифікувати проблеми, а також підвищує оперативність реагування на них.

ВИСНОВКИ

У ході дослідження розглянуто методику використання OSINT для виявлення, аналізу та реагування на кіберзагрози. Встановлено, що сучасні технології розвідки з відкритих джерел надають унікальні можливості для аналізу загроз та зниження ризиків у сфері кібербезпеки. Завдяки використанню таких інструментів, як Shodan, Maltego, SpiderFoot, Sherlock та інших, можна ефективно моніторити інформацію, ідентифікувати вразливі об'єкти, аналізувати потенційні загрози та оперативно реагувати на них.

Основною перевагою OSINT є здатність оперативно обробляти великі обсяги інформації з різних джерел, забезпечуючи високу точність результатів. Однак, дослідження також виявило низку недоліків, серед яких складність освоєння деяких інструментів, висока вартість окремих ліцензій та можливість отримання нерелевантних даних через помилки у виборі джерел.

Розглянуто чіткий план використання OSINT, який включає всі етапи — від визначення цілей та об'єктів дослідження до підготовки звітів і впровадження заходів реагування. Особливу увагу приділено автоматизації процесів збору й аналізу інформації для підвищення ефективності.

Наголошено, що розробка нових методик та адаптація існуючих технологій до специфічних умов організації є критично важливою для своєчасного реагування на загрози. Використання OSINT у кібербезпеці дозволяє не лише виявляти поточні загрози, а й запобігати потенційним атакам, знижуючи ризик витоку інформації та втрати критичних активів. Дієвість запропонованих методик була доведена практично.

Таким чином, застосування OSINT сприяє підвищенню загального рівня безпеки організації. Проте, для максимального використання потенціалу цих технологій необхідно інвестувати у вдосконалення інструментів, навчання персоналу та інтеграцію OSINT у загальну стратегію кіберзахисту.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Заглинський В. А. Використання штучного інтелекту в OSINT: переваги та виклики // Штучний інтелект і безпека : матеріали науково-практичної конференції Інституту проблем моделювання в енергетиці ім. Г. Є. Пухова Національної академії наук України, Інституту проблем реєстрації інформації Національної академії наук України, 19–21 листопада 2024 р., Київ. Київ : ІПМЕ ім. Г. Є. Пухова НАН України, ІПРІ НАН України, 2024. С. 88–89.

2. Заглинський В. А. OSINT як інструмент інформаційної безпеки в умовах воєнних конфліктів // Інформаційні технології і автоматизація – 2024 : матеріали XVII міжнародної науково-практичної конференції, Одеса, 31 жовтня – 1 листопада 2024 р. Одеса : Видавництво ОНТУ, 2024. С. 194–195.

3. Карпінець А.В. Основи використання технологій OSINT для кібербезпеки / А.В. Карпінець. – Київ: Науковий центр, 2021. – 200 с.

4. Ivanov A. Open Source Intelligence for Cybersecurity / A. Ivanov. – New York: Cybersecurity Press, 2020. – 250 p.

5. Chen X. Advances in OSINT Methodologies: Identification and Prevention of Threats / X. Chen, Y. Wang // Cybersecurity Journal. – 2022. – Vol. 5, No. 2. – P. 102–123.

6. Заглинський В. А. OSINT як ключовий інструмент підготовки кібератаки // Безпека, технології, інновації: нові горизонти : збірник праць учасників міжфакультетської науково-практичної інтернет-конференції здобувачів вищої освіти і молодих вчених, 12 листопада 2024 р. Житомир : Поліський національний університет, 2024. С. 9-11.

7. Cybersecurity Ventures : веб сайт. URL: https://cybersecurityventures.com (дата звернення 12.11.2024)

8. Zhang Y. OSINT Techniques for Digital Forensics / Y. Zhang, L. Zhou // Digital Forensics Review. – 2021. – Vol. 6, No. 2. – P. 88–101.

9. Пономаренко І.В. Використання OSINT у сучасних умовах кіберзагроз / І.В. Пономаренко // Вісник інформаційної безпеки. – 2021. – № 3. – С. 45–56.

10. ThreatMiner : веб сайт. URL: https://www.threatminer.org (дата звернення 17.11.2024).

11. Moore J. Ethical Challenges in Open Source Intelligence / J. Moore // OSINT Ethics Journal. – 2022. – Vol. 8, No. 1. – P. 12–24.

12. OWASP Foundation : веб сайт. URL: https://owasp.org (дата звернення 15.11.2024).

13. Гнатюк С.М. Використання аналітичних платформ для OSINT / С.М. Гнатюк // Інформаційна аналітика. – 2019. – № 7. – С. 56–67.

14. Shmidt P. Automated Data Analysis in OSINT Research / P. Shmidt, K. Brown // Cyber Threat Intelligence. – 2022. – Vol. 7, No. 4. – P. 53–67.

15. Lin J. Data Mining in Open Source Intelligence / J. Lin, W. Liu // Data Science in Cybersecurity. – 2020. – Vol. 4, No. 3. – P. 33–49.

16. Трофименко С.М. Захист даних в OSINT-процесах / С.М. Трофименко // Практична кібербезпека. – 2021. – № 6. – С. 67–79.

17. Nguyen T. Emerging Trends in Open Source Threat Analysis / T. Nguyen // International Cyber Review. – 2021. – Vol. 9, No. 3. – P. 45–59.

18. Adams J. The Role of Social Media in OSINT / J. Adams, T. Smith // Digital Intelligence. – 2019. – Vol. 3, No. 1. – P. 21–34.

19. Малюк О.П. Соціальні мережі як джерело OSINT-даних / О.П. Малюк // Технології інформаційного моніторингу. – 2020. – № 4. – С. 23–34.

20. Нікітін О.В. Автоматизація процесів OSINT-аналізу: сучасні інструменти та їх ефективність / О.В. Нікітін // Інформаційні технології. – 2020. – № 5. – С. 78–90

21. Social-Searcher : веб сайт. URL: https://www.social-searcher.com (дата звернення 05.11.2024).

22. Центр інформаційної безпеки : веб сайт. URL: https://cybersecuritycenter.org (дата звернення 09.11.2024)

23. WhoisXML API : веб сайт. URL: https://whoisxmlapi.com (дата звернення 07.11.2024).

24. Digital Shadows : веб сайт. URL: – Режим доступу: https://www.digitalshadows.com (дата звернення 06.11.2024).

25. SpyCloud : веб сайт. URL: https://spycloud.com (дата звернення 31.10.2024).

26. Єсіна М. В., Азаров М. О. Дослідження та аналіз інструментів і методів, що використовує механізм osint //The 7 th International scientific and practical conference “Modern research in world science”(October 2-4, 2022) SPC “Sci-conf. com. ua”, Lviv, Ukraine. 2022. 1320 p. – 2022. – С. 251.

27. SpiderFoot : веб сайт. URL: https://www.spiderfoot.net (дата звернення 01.11.2024).

28. Have I Been Pwned : веб сайт. URL: https://haveibeenpwned.com (дата звернення 31.10.2024).

29. Перунов О.В. Розробка аналітичних інструментів для моніторингу витоків даних / О.В. Перунов // Аналітична кібербезпека. – 2020. – № 5. – С. 12–23.

30. Abatabaei, Fahimeh, and Douglas Wells. "OSINT in the Context of Cyber-Security." Open Source Intelligence Investigation: From Strategy to Implementation – 2017 – P. 213-231.

31. Кузьо О. О., Крилов В. К., Мацюк Н. Л. Використання технології osint для формування портрету користувача //Матеріали XI Міжнародної науково-практичної конференції молодих учених та студентів „Актуальні задачі сучасних технологій “. – 2022. – С. 140-140.

32. Центр аналізу кіберзагроз : веб сайт. URL: https://cyberthreatanalysis.org (дата звернення 14.11.2024)

33. Maltego : веб сайт. URL: https://www.maltego.com (дата звернення 01.11.2024).

34. Sherlock : веб сайт. URL: https://github.com/sherlock-project/sherlock (дата звернення 03.11.2024).

35. OSRFramework : веб сайт. URL: https://osrframework.readthedocs.io (дата звернення 05.11.2024).

36. Brandwatch : веб сайт. URL: https://www.brandwatch.com (дата звернення 06.11.2024).

37. Shodan : веб сайт. URL: https://www.shodan.io (дата звернення 07.11.2024).

38. Netcraft : веб сайт. URL: https://www.netcraft.com (дата звернення 18.11.2024).

39. ThreatMiner : веб сайт. URL: https://www.threatminer.org (дата звернення 17.11.2024).

40. Threat Intelligence Platform : веб сайт. URL: https://threatintelligenceplatform.com (дата звернення 10.11.2024).

41. SSL Checker : веб сайт. URL: https://www.sslshopper.com/ssl-checker.html(дата звернення 11.11.2024).

42. Меркулов І.А. Захист корпоративних ресурсів у соціальних мережах / І.А. Меркулов // Практичний аналіз загроз. – 2021. – № 6. – С. 56–67.

43. Grubbs R. Network Monitoring with Modern Tools / R. Grubbs // Network Security Review. – 2021. – Vol. 12, No. 4. – P. 34–48.