Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ДОПУСТИТИ ДО ЗАХИСТУ:
В.о. завідувача кафедри
Кібербезпеки та захисту
інформації
_____ Іван ПАРХОМЕНКО
«___» червня 2025 р.

ПОЯСНЮВАЛЬНА ЗАПИСКА

кваліфікаційної роботи

галузь знань 12 Інформаційні технології
(шифр і назва галузі знань)
спеціальність 125 «Кібербезпека»
(код і назва спеціальності)
освітній ступень бакалавр
освітня програма Кібербезпека
(назва освітньо-професійної програми)

на тему: «Метод протидії кібератакам з використанням OSINT технологій»

Виконавець: студент IV курсу, групи КБ-42

_____ **Дмитро КОВАЛЬ**
(підпис) (ім'я прізвище)

	Підпис	**Ім'я, прізвище**
Керівник роботи		Микола БРАЇЛОВСЬКИЙ
Нормоконтроль		Олександр ЛУКАШОВ

Київ 2025

Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ЗАТВЕРДЖЕНО:
В.о. завідувача кафедри
кібербезпеки
та захисту інформації
_____ Іван ПАРХОМЕНКО
«29» листопада 2024 р.

ЗАВДАННЯ
на виконання кваліфікаційної роботи

спеціальності 125 Кібербезпека
(код і назва спеціальності)

освітньої програми Кібербезпека
(назва освітньої-професійної програми)

студенту **КБ-42** **Ковалю Дмитру Олеговичу**
(група) (прізвище ім'я по батькові)

Тема кваліфікаційної роботи Метод протидії кібератакам з використанням OSINT технологій

1. ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Тема кваліфікаційної роботи затверджена на засіданні кафедри кібербезпеки та захисту інформації протокол №6 від 28.11.2024 р.

2. ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Підходи до протидії кібератакам з використанням OSINT-технологій.

3. ЗМІСТ РОЗРАХУНКОВО-ПОЯСНЮВАЛЬНОЇ ЗАПИСКИ

У пояснювальній записці аналізуються загрози, що базуються на OSINT, оцінюються існуючі підходи, розробляється власний метод протидії таким кібератакам.

4. ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Практична цінність Практично орієнтований метод, який дозволяє підприємствам виявляти цифрові вразливості через OSINT та посилювати свою кібербезпеку.

5. ДАТА ВИДАЧІ ЗАВДАННЯ

Дата видачі завдання: 29 листопада 2024 року

Завдання видав _____ Микола БРАІЛОВСЬКИЙ
(підпис) (ім'я, прізвище)

Завдання прийняв до виконання _____ Дмитро КОВАЛЬ
(підпис) (ім'я, прізвище)

КАЛЕНДАРНИЙ ПЛАН

№ п/п	Найменування етапів робіт	Строки виконання робіт (початок-кінець)	Відмітка про виконання
1	Уточнення постановки задачі	29.11.2024 – 22.01.2025	*виконано*
2	Аналіз літератури	23.01.2025 – 11.02.2025	*виконано*
3	Обґрунтування вибору методу дослідження	12.02.2025 – 15.02.2025	*виконано*
4	Аналіз технологій OSINT як інструменту атак і моделювання загроз	16.02.2025 – 04.03.2025	*виконано*
5	Дослідження підходів до захисту корпоративної інформації від OSINT-атак	05.03.2025 – 21.03.2025	*виконано*
6	Розробка методу протидії кібератакам з використанням OSINT-технологій	22.03.2025 – 08.04.2025	*виконано*
7	Оцінка ефективності запропонованого методу	09.04.2025 – 10.05.2025	*виконано*
8	Оформлення пояснювальної записки	11.05.2024 – 27.05.2024	*виконано*
9	Підготовка до захисту кваліфікаційної роботи	28.05.2025 – 13.06.2025	*виконано*

Завдання видав _____ Микола БРАІЛОВСЬКИЙ
(підпис) (ім'я, прізвище)

Завдання прийняв до виконання _____ Дмитро КОВАЛЬ
(підпис) (ім'я, прізвище)

Термін подання кваліфікаційної роботи до ЕК 13 червня 2025 року

УДК 004.35.004.49

РЕФЕРАТ

Кваліфікаційна робота складається зі вступу, трьох розділів, загальних висновків, списку використаних джерел, додатків, має 86 сторінок основного тексту, 20 рисунків, 5 таблиць. Список використаних джерел містить 35 найменувань і займає 3 сторінки. Крім того, робота містить 1 додаток із загальною кількістю сторінок 6.

Метою роботи є розробка методу протидії кібератакам, що здійснюються з використанням OSINT-технологій.

Для досягнення зазначеної мети було поставлено наступні завдання:

- Провести аналіз основних принципів і видів OSINT-технологій, а також їх застосування в кіберрозвідці та моделюванні кіберзагроз.
- Проаналізувати механізми анонімізації, обмеження доступу, моніторингу відкритих джерел та захисту корпоративних доменів від витоків інформації через OSINT.
- Розробити метод протидії кібератакам з використанням OSINT, що включає технічні, організаційні та кадрові заходи захисту корпоративних даних і персональної інформації співробітників.
- Провести порівняльний аналіз ефективності розробленого методу з існуючими підходами та оцінити його практичну застосовність у реальних умовах.

Об'єктом дослідження є процес протидії кібератакам, реалізованим за допомогою OSINT-технологій у корпоративній інфраструктурі.

Предметом дослідження є методи виявлення, аналізу та нейтралізації загроз, які виникають внаслідок використання відкритих джерел інформації (OSINT) у контексті захисту корпоративної інформаційної інфраструктури.

Методи дослідження: аналіз наукової та технічної літератури з кібербезпеки, вивчення сучасних тенденцій використання OSINT у атаках на організації, а також розгляд реальних інцидентів і сценаріїв таких атак.

Практичною цінністю роботи є розробка методу, який забезпечує комплексний підхід до захисту корпоративної інформації від загроз, пов'язаних із використанням OSINT. Це дозволяє суттєво мінімізувати ризики витоку даних і підвищити рівень інформаційної безпеки підприємств. Запропоновані заходи можуть бути впроваджені в різних організаціях для зміцнення стійкості до кіберзагроз і забезпечення ефективного реагування на них.

Найважливіші результати дослідження. У ході роботи було здійснено класифікацію потенційних джерел відкритих даних, які можуть бути використані для проведення розвідки проти компаній. Визначено критичні вразливості, пов'язані з витоком публічної інформації, що дозволяє хакерам використовувати їх на початкових етапах кібератак. Розроблено покроковий метод протидії загрозам, що виникають унаслідок використання OSINT-технологій. Сформовано практичні рекомендації для підприємств, які дозволяють мінімізувати цифровий слід організації у відкритому доступі.

Пропозиції щодо продовження досліджень включають проведення поглибленого аналізу новітніх технологічних загроз, що виникають у зв'язку з розвитком автоматизованих OSINT-інструментів. Також варто застосовувати спеціалізовані інструменти моніторингу та виявлення витоку відкритої інформації.

Ключові слова: кібербезпека, OSINT, інформаційна розвідка, захист інформації, цифровий слід, корпоративна безпека, метод протидії, відкриті джерела, атаки.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

OSINT	–	Open Source Intelligence
VPN	–	Virtual Private Network
IP	–	Internet Protocol
TOR	–	The Onion Router
IoC	–	Indicators of Compromise
EXIF	–	Exchangeable Image File Format
APT	–	Advanced Persistent Threat
CVE	–	Common Vulnerabilities and Exposures
SQL-атаки	–	SQL Injection
XSS	–	Cross-Site Scripting
RCE	–	Remote Code Execution
ПЗ	–	програмне забезпечення
ОС	–	операційна система
API	–	Application Programming Interface
WAF	–	Web Application Firewall
OWASP	–	Open Worldwide Application Security Project
DNS	–	Domain Name System

ВСТУП

В сучасному світі інформація стає найважливішим ресурсом. Доступність та відкритість інформації вражає — кожна людина може знайти терабайти інформації на будь-яку тему в будь-якій пошуковій системі без великих зусиль. Такий метод отримання інформації називається OSINT.

OSINT (Open source intelligence, OSINT) — це технологія пошуку та отримання будь-якої потрібної інформації з відкритих джерел, без порушення законів. Користувач, що використовує методи OSINT-розвідки даних найчастіше орієнтується на дані з: форумів, новин, сайтів, пошукових систем, блогів, соціальних мереж, сервісів, що хостять файли, геолокаційні ресурси. Таким чином можна отримати наступну інформацію: персональні дані людини чи групи людей (ПІБ, контакти, місця роботи, соц. мережі, відносини з іншими людьми), інформацію про компанію (структура, керівництво, IP-адреси), технічні дані (сервіси, що використовуються, відкриті порти, конфігурація системи, веб-додатки) та інші [1].

Базовою потребою користувачів, що використовують пошукові системи, є отримання певної інформації задля своїх, часто рутинних задач. Але використання таких технологій полегшує життя не тільки звичайним людям, а й хакерам. Найчастіше хакери використовують OSINT-технології для збору інформації про ціль, на яку планується здійснити певну атаку. В методології Cyber Kill Chain розвідка (Reconnaissance) – є першим етапом в ланцюжку дій для атаки на ціль. Зловмисники намагаються зібрати таку інформацію, як email-адреси та інші контакти працівників, версії сервісів та їх конфігурацію, IP адреси та порти ресурсів та інше.

Саме розвідка цілі є першим і найважливішим етапом, що визначає, чи є взагалі сенс атакувати ціль, чи буде ця атака вдалою? Інформацію можна знайти навіть про занадто малу ціль, про яку, начебто, ніхто ніколи не чув і не знав. Тому саме зменшення кількості даних чи їх санітізація, очищення або зміна є

найважливішим етапом для підвищення інформаційної безпеки компанії. Саме з цієї причини кожна організація, яка робить реальні кроки для посилання кіберзахисту своїх ресурсів – дуже серйозно відноситься до наявної відкритої інформації про систему, а фахівці з ІБ досліджують, аналізують та прогнозують, як ця інформація може бути використана для атак на ціль.

Наразі залишається купа невирішених проблем, пов'язаних з використанням технології OSINT хакерами та наявності певної інформації у відкритих джерелах, що може бути корисною для здійснення атак.

Тенденція така, що:

Зловмисники намагаються автоматизувати процес отримання даних про ціль. Автоматизація процесу розвідки виконується завдяки використанню великої кількості різноманітного програмного забезпечення та веб-сервісів. Якщо колись для детального збору інформації про сервіс потрібно було витрачати години часу – зараз потрібно менше години для отримання гігабайтів потрібної інформації. В багатьох сервісах достатньо лише вказати адресу чи додаткові дані цілі та вибрати необхідні параметри пошуку [2].

Наразі відсутні ефективні та комплексні методи захисту та протидії поширення важливої інформації про систему. Більшість компаній зосереджена саме на технічних, програмних засобах захисту системи, коли використання OSINT технологій займає друге місце по важливості.

Також немає ефективних методів запобіганням атакам соціальної інженерії, для яких теж потрібно володіння великою кількістю інформації про систему та співробітників компанії. Наявні базові методи та план дій для запобіганням атакам соц. інженерії, чого може бути недостатньо.

Багато компаній не враховують швидкість розповсюдження інформації. Те, що колись хоча б один раз з'явилося в мережі Інтернет (наприклад відкритий файл з паролями чи ключами в директорії серверу), залишається там назавжди. І навіть видалення цієї інформації не гарантує, що ніхто її не отримує. Наприклад сервіс Web Archive (Internet Archive) сканує і зберігає сторінки в режимі

реального часу, а таких сервісів безліч. Також існують пошукові роботи, що індексують файли, Shodan – система, що сканує вразливі хости, Censys та інші.

Метою роботи є розробка методу протидії кібератакам, що здійснюються з використанням OSINT-технологій.

Об'єктом дослідження є процес протидії кібератакам, реалізованим за допомогою OSINT-технологій у корпоративній інфраструктурі.

Предметом дослідження є методи виявлення, аналізу та нейтралізації загроз, які виникають внаслідок використання відкритих джерел інформації (OSINT) у контексті захисту корпоративної інформаційної інфраструктури.

Актуальність дослідження зумовлена зростанням кількості кібератак із використанням відкритих джерел інформації (OSINT), що створює серйозні ризики для корпоративної безпеки. Недостатній контроль над доступом до корпоративної інформації у відкритих мережах підвищує ймовірність витоку даних і компрометації організаційних ресурсів. У цьому контексті використання OSINT-технологій як інструменту моделювання загроз дає змогу своєчасно виявляти потенційні атаки та підвищувати ефективність заходів інформаційної безпеки. Тому впровадження розробленого методу протидії кібератакам з використанням OSINT є важливим кроком для зміцнення захисту корпоративної інфраструктури в умовах сучасних кіберзагроз.

Основні результати роботи були представлені у вигляді наукової роботи:

Коваль Д., Браіловський М. Метод протидії кібератакам з використанням OSINT-технологій в корпоративній середі // Проблеми кібербезпеки інформаційно-комунікаційних систем (PCSICS): зб. матеріалів доп. та тез VIII Міжнар. наук.-практ. конф. (Київ, 11 квіт. 2025 р.) / редкол.: В.В. Ільченко, С.В. Толюпа, О.А. Лаптєв та ін. – Київ: Київський національний університет імені Тараса Шевченка, 2025. – С. 37–38. [3]

РОЗДІЛ 1
OSINT ЯК ІНСТРУМЕНТ ІНФОРМАЦІЙНОЇ РОЗВІДКИ, АТАК ТА МОДЕЛЮВАННЯ ЗАГРОЗ

1.1 Основи OSINT технологій

Визначення OSINT-технологій

Згідно визначення інститутом SANS — OSINT (Open-Source Intelligence) визначається як розвідка, отримання інформації шляхом збору, оцінки та аналізу з метою відповіді на конкретне поставлене запитання. Оскільки для такого способу розвідки використовуються саме відкриті джерела інформації, то цей процес є повністю законним та етичним. Основною метою OSINT можна назвати пошук та використання публічної інформації для досягнення розвідувальних цілей — наприклад, в контексті ІБ, для виявлення загроз чи вразливостей, даних про корпоративну систему або людей, що працюють в компанії.

Основні принципи та етапи збору інформації

Розвідка на основі відкритих джерел вимагає дотримання певних правил і принципів для ефективної роботи, а саме:

Взагалі, якщо фахівець з ІБ займається OSINT`ом — звісно, що він працює тільки у правовому полі. Але хакер (BlackHat) може і скоріш за все буде використовувати будь-які ресурси задля отримання інформації про ціль. Приклади ресурсів, що може використати хакер і це буде порушенням закону: злиті бази даних, бази паролів, бази користувачів. Інформація з DarkNet (покупка інформації, пошук незаконно отриманої інформації) [4].

Але, як фахівець ІБ, так і хакер будуть дотримуватися ідентичного паттерну при зборі інформації.

Забезпечення анонімності оператора (OSINT`ера) шляхом, наприклад, використання технології VPN або TOR. Під час пошуку будь-якої інформації, користувач залишає цифрові відбитки, за якими, теоретично, його можна

відслідкувати. Звісно, що під час пошуку інформації система збирає багато параметрів, наприклад IP-адресу, браузер та девайс, з якого ведеться пошук та інші.

Оцінка достовірності як ресурсу, з якого отримується інформація, так і самої інформації. Очевидно, що отримана інформація повинна буди ідентифікована, класифікована та перевірена на достовірність. Більш того, потрібно розуміти, з якого ресурсу було зібрано дані і як вони опинилися на ньому. Використання неперевіреної інформації може бути причиною неефективної роботи та помилок в роботі в подальшому.

Останнім важливим принципом є класифікація, систематизація та уточнення інформації шляхом її перевірки різними джерелами. В більшості випадків, інформація перевіряється різними способами.

Етапи збору інформації за допомогою OSINT технологій

Визначення цілі

Звісно, що першим етапом є визначення цілі, про яку буде збиратися інформація. В контексті кібербезпеки, ціллю може бути IP адреса, пул IP адрес чи ASN (Autonomous System Number). Можуть бути випадки, коли всі наявні дані — це назва компанії. Тоді ціль — компанія, про яку потрібно зібрати інформації з різних “сторін” [5].

Підготовка та планування пошуку інформації

Коли ціль визначена, потрібно планувати, яка інформація повинна бути зібрана. Загалом, дані про компанію, які більше всього цікавлять фахівця ІБ або хакера можна класифікувати наступним чином:

Класифікація даних про компанію, яка цікавить OSINT-спеціаліста.

Основні відомості про компанію

Загальна інформація:

- Офіційне найменування компанії;
- Дата реєстрації та історія заснування;
- Юридичний статус компанії (ТОВ, АТ, ПАТ і т.д.);
- Місцезнаходження головного офісу (адреса, країна);

– Контактні дані (телефони, електронні адреси);

– Вебсайт компанії;

– Реєстраційні номери (ЄДРПОУ, ІНН).

Державні та комерційні реєстри:

– Реєстраційні записи в державних органах (податкові або торгові реєстри);

– Доступна фінансова звітність (якщо компанія публічна або зобов'язана її надавати);

– Наявність судових справ або юридичних процесів.

Інформація про діяльність компанії

Продукти та послуги:

– Опис продукції або послуг, які компанія надає;

– Список партнерів та постачальників;

– Цільова аудиторія та ринок (географічні регіони, галузі).

Корпоративна культура:

– Склад керівництва та топ-менеджменту;

– Членство в асоціаціях, організаціях;

– Відгуки про компанію в профільних соціальних мережах та форумах (LinkedIn, Glassdoor).

Інвестиції та фінансування:

– Рівень інвестицій та наявність партнерських угод;

– Публічні дані про раунди інвестування або залучення капіталу.

Онлайн-присутність компанії

Вебсайт компанії:

– Технічні деталі сайту (сервери, домени, сертифікати безпеки);

– Веб-архіви (наприклад, через Wayback Machine) для історії сайту.

Соціальні мережі:

– Профілі на Facebook, Twitter, LinkedIn, Instagram, YouTube;

– Кількість підписників, взаємодія з користувачами.

– Використовувані соціальні медіа-платформи для реклами та просування.

Огляди та згадки в інтернеті:

– Відгуки та рейтинги на різних платформах (наприклад, Trustpilot, форуми, блогери);

– Згадки в новинах та публікаціях.

Технічна інфраструктура

IT-інфраструктура:

– Технічні рішення, що використовуються в компанії (CMS, хмарні сервіси, системи безпеки);

– Доступні відкриті інтерфейси, такі як API або інші сервіси;

– Системи захисту даних і політика безпеки (SSL-сертифікати, брандмауери).

Доменні імена та IP-адреси:

– Власність доменів, зворотний пошук по IP-адресах;

– Публічні IP-адреси, які використовує компанія;

– Можливі зв'язки з іншими компаніями через інфраструктуру (наприклад, спільні IP-адреси, хостинг).

Електронна пошта:

– Виявлення шаблонів електронних адрес (наприклад, ім'я@company.com, support@company.com);

– Пошук за ключовими словами в листах або на форумах.

Безпека та уразливості

Інциденти безпеки:

– Можливі інциденти або історія порушень безпеки (наприклад, витоки даних, фішинг);

– Публічні записи про вразливості або атаки (наприклад, через бази даних CVE).

Перевірка на наявність шкідливого ПО:

– Перевірка сайтів або файлів компанії на наявність шкідливих програм (з використанням інструментів, як VirusTotal);

– Визначення наявності шкідливих IP-адрес або доменів, які можуть бути причетні до атаки.

Публічні зв'язки та інтерв'ю з топ-менеджментом

Інтерв'ю з керівниками компанії:

– Прес-релізи та публікації, де фігурують співробітники компанії;

– Стратегії та перспективи розвитку компанії за офіційними заявами.

Зв'язки з медіа:

– Публікації у професійних та галузевих ЗМІ;

– Згадки у новинах, статтях, відео та інших джерелах медіа.

Пошук і збір інформації з відкритих джерел

На цьому етапі здебільшого використовуються пошукові системи, веб-сайти, програмне забезпечення, портали новин для збору необхідних даних про ресурс [6].

Фільтрація та обробка отриманих даних

Після повного збору інформації, вона потрібно бути, класифікована та відфільтрована. Звичайною практикою є те, що далеко не всі дані знадобляться на наступних етапах роботи.

Аналіз та перевірка інформації

Коли всі дані отримані, класифіковані та відфільтровані – маємо певний документ чи наприклад дошку, де знаходиться необхідна інформація для роботи. Кінцевим кроком буде перевірка інформації на достовірність. Якщо є змога – підтвердження її різними джерелами.

Різниця в OSINT підході для фахівця ІБ та для зловмисника

Потрібно чітко розуміти, що цілі та можливості співробітника з відділу ІБ, який може зібрати інформацію про компанію для її захисту і цілі та можливості хакера, який хоче проникнути у систему – різні. В такому випадку потрібно враховувати можливості хакера. Тільки так можна ефективно захиститися,

розуміючи, яку інформацію може отримати зловмисник [7]. Порівняння можливостей фахівця ІБ та зловмисника в використанні OSINT-технологій показані в табл. 1.1.

Таблиця 1.1

Порівняння можливостей фахівця ІБ та зловмисника в використанні OSINT-технологій.

Критерії	**Фахівець ІБ**	**Зловмисник**
Цілі збору інформації	Оцінка безпеки, моніторинг вразливостей, визначення загроз	Підготовка до атаки, пошук вразливих точок для вторгнення
Морально-етичні, правові принципи	Дотримання етичних, моральних і правових норм. Пошук інформації для захисту систем. Дотримання всіх державних та міжнародних законів	Ігнорування будь-яких норм, використання усіх можливих способів отримання інформації
Мета використання інформації	Виявлення вразливостей, пошук злитої інформації з обмеженим доступом для її видалення (якщо можливо), підвищення рівня кіберзахисту систему	Використання отриманої інформації для здійснення атаки на ціль

Продовження табл. 1.1

Типи використаних інструментів	Легальні ресурси та ПЗ, вендори, що надають певну інформацію у разі запиту	Використання будь-якого ПЗ та ресурсів, наприклад DarkNet. Викуп необхідної інформації за гроші. Використання фішингу, соц. інженерії
Тип інформації	Публічно доступні дані про компанії, сервіси, продукти, співробітників	Конфіденційні дані, паролі, особиста інформація співробітників, дані для зловживань. Будь-яка інша інформація, що може бути у пригоді для зламу системи
Аналіз даних	Оцінка потенційних загроз, аналіз вразливих точок системи	Пошук найслабших ланок для проникнення в систему
Діяльність після збору інформації	Рекомендації щодо посилення безпеки, створення звітів, ведення політики безпеки	Відправка фішингових листів, запуск атак на уразливі точки
Пріоритети	Безпека корпоративних даних, захист систем і мереж	Викрадення даних, злом мереж або маніпулювання системами

1.2 Види OSINT розвідки

На схемі позначено основні методи OSINT (рис.1.1).

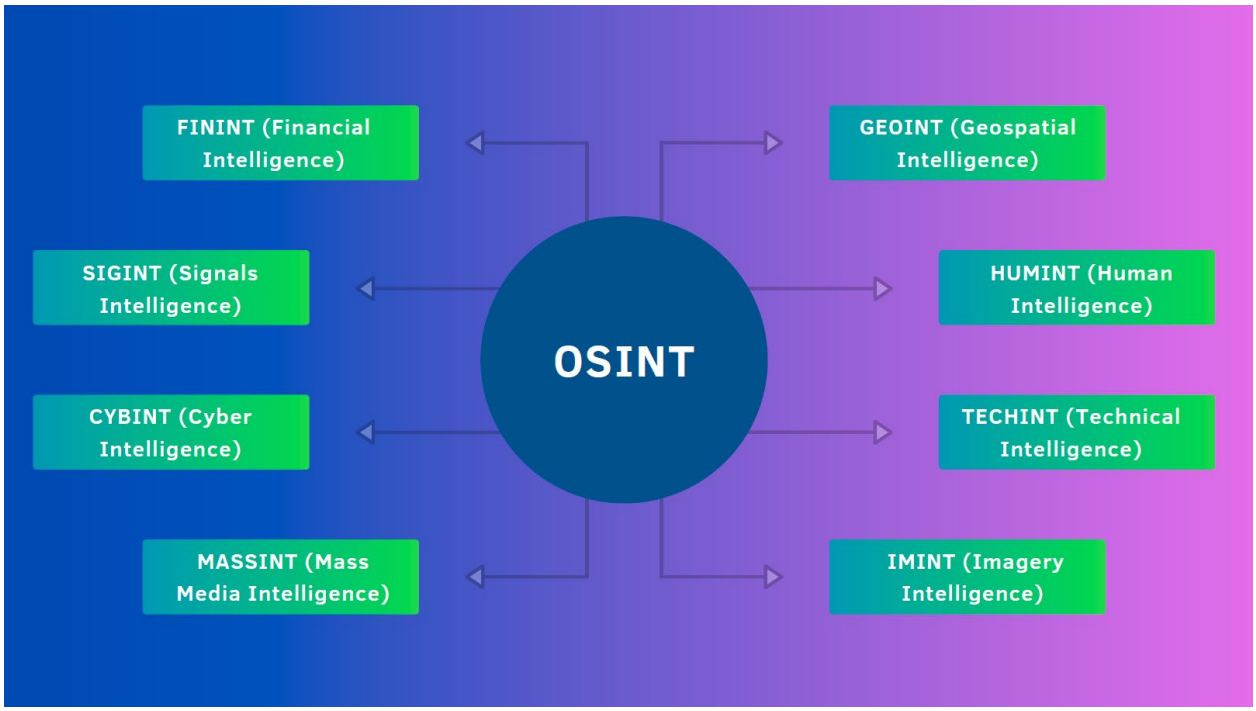

Рисунок 1.1. Основні методи OSINT.

Класифікація кожного OSINT методу

FININT (Financial Intelligence)

Метод збору і обробки фінансової інформації, банківських чи криптовалютних транзакцій для виявлення корупції чи грошових потоків. Наприклад: Аналіз транзакцій та їх звітів, використання криптовалютних бірж та сервісів для стеження та відслідковування транзакцій, відкриті бази даних фінансових установ для виявлення підозрілих операцій.

Особливості FININT:

– Збір і аналіз фінансових транзакцій;

– Виявлення підозрілих чи незаконних грошових переказів;

– Моніторинг криптовалют через блокчейн-аналізатори (наприклад, Chainalysis, CipherTrace).;

– Аналіз фінансових звітів, санкційних списків.

GEOINT (Geospatial Intelligence)

Аналіз даних на місцевості. Геопросторова розвідка. Використовуються різні види карт, від Google Maps до аеро- та супутникових знімків. Мета цього типу розвідки - орієнтування на місцевості, відстеження об'єктів (машин, техніки), деталізація об'єктів, ідентифікація інфраструктури.

Особливості GEOINT:

– Стеження за пересуванням або змінами на території;

– Картографування територій (OpenStreetMap, Google Maps);

– Зіставлення координат, геотегів у соцмережах, метаданих;

– Виявлення розташування об'єкта за фото або відео (GeoGuessing).

SIGINT (Signals Intelligence)

Розвідка джерел електромагнітних сигналів, збір даних шляхом перехоплення сигналів. Аналіз сигналів і комунікацій, наприклад радіо, інтернет-трафік, телефони та інше.

Особливості SIGINT:

– Перехоплення та аналіз електромагнітних сигналів;

– Прослуховування радіо-, телефонного чи VoIP-зв’язку;

– Аналіз мережевого трафіку;

– Розвідка через Wi-Fi, Bluetooth, IoT-пристрої;

– Збір технічної інформації про частоти, протоколи, типи зв'язку.

HUMINT (Human Intelligence)

Розвідка на основі взаємодії з людьми. Наприклад спілкування, інтерв’ю, агентурна мережа, опитування персоналу.

Особливості HUMINT:

– Отримання інформацію напряму від людей;

– Використовуються інтерв'ю, комунікація, розмови, агентурна робота;

– Використовуються методи соціальної інженерії;

– Використовується для перевірки та підтвердження даних з інших джерел;

– Може бути як легальною (опитування, журналістика), так і прихованою (псевдоособи, інсайдери).

CYBINT (Cyber Intelligence)

Розвідка у сфері кібербезпеки. Збір інформація про загрози та вразливості, нові CVE та способи хакерських атак. Використовуються відкриті інструменти та бази даних, спеціальні сервіси.

Особливості CYBINT:

– Моніторинг даркнету, форумів, Telegram-каналів;

– Використання OSINT-інструментів: Shodan, Censys, VirusTotal, Whois;

– Збір технічної інформації: IP-адреси, домени, хеші файлів, індикатори компрометації (IoC);

– Аналіз артефактів: cookie, user-agent, цифрові сліди.

TECHINT (Technical Intelligence)

Технічна розвідка. Збір інформації про технологічні досягнення чи стандарти. Наприклад виявлення особливостей роботи певної системи.

Особливості TECHINT:

– Збір даних про технічні характеристики систем, технологій, ПЗ;

– Дослідження технологічного рівня супротивника або компанії;

– Реверс-інжиніринг (якщо є дозвіл або можливість).

MASSINT (Mass Media Intelligence)

Пошук інформації з медіа джерел (новини, телебачення, прямі ефіри, соц. мережі).

Особливості MASSINT:

– Аналіз новин, ЗМІ, телеефірів, відео, стрімів;

– Аналіз суспільних настроїв, відслідковування інформаційних операцій;

– Відстеження реакції населення, поширення фейків;

– Виявлення джерел дезінформації чи пропаганди.

IMINT (Imagery Intelligence)

Розвідка, для якої використовується аналіз зображень (схоже з GEOINT). Аналізуються зображення з аерофотозйомки, супутникові знімки і тд. Визначаються і характеризуються об'єкти, що зображені на фото. Якщо взяти групове фото людей у певні компанії, визначаються персональні дані та посада кожної людини.

Особливості IMINT:

– Аналіз зображень, фото, відео;

– Аналіз метаданих зображень (EXIF);

– Може перетинатись із GEOINT, але фокусується саме на зображеннях;

– Можливість визначити особу за фото через розпізнавання облич (FaceCheck, PimEyes).

1.3 Атаки з використанням OSINT-технологій та їх значення

Як було вказано вище, розвідка (майже завжди OSINT) — є одним із перших етапів планування атаки на ціль. Атаки з використанням OSINT-технологій спрямовані на збір, аналіз та використання відкритих даних про компанію, її співробітників, IT-інфраструктуру, партнерів та процеси з метою отримання переваги або компрометації. Відмінність цих атак полягає у їх прихованості, мінімальних витратах та відсутності необхідності у фізичному або технічному доступі до внутрішніх систем. Все робиться через мережу і, майже завжди, непомітно для цілі [8].

Основні OSINT-джерела, які можуть бути використані зловмисниками:

– Соціальні мережі (LinkedIn, Facebook, Instagram, Twitter/X);

– Корпоративні веб-сайти;

– Онлайн-резюме співробітників, публікації у відкритих профілях;

– Витоки даних (бази логінів і паролів з попередніх інцидентів);

– Пошукові системи (Google Dorks — спеціалізовані запити для пошуку конфіденційних файлів);

– DNS-інформація, WHOIS-записи, SSL-сертифікати;

– Платформи типу Shodan або Censys, які дозволяють виявляти відкриті порти, сервера, пристрої.

Етапи атак з використанням OSINT-технологій

Інформаційна розвідка

Виявлення цілей атаки, збір максимальної кількості відкритої інформації: адреса компанії, працівники, технічні домени, технологічний стек [9].

Створення профілів компанії

Аналіз організаційної структури, визначення ключових посад, прив'язка технічного забезпечення (активів) до працівників, виявлення потенційно вразливих активів.

Аналіз знайдених вразливостей

Аналіз вразливостей, побудова структури атаки, визначення точок входу — відомі дані від пошт, сервісів, документи з метаданими, знайдені паролі в базах даних, API-ключі та інші.

Експлуатація

Підготовка фішингових листів, побудова сценаріїв соціальної інженерії, атаки через вразливості веб-сервісів або систем віддаленого доступу (наприклад, через неправильну конфігурація VPN або відкритий RDP).

Значення таких атак для корпоративного середовища

Невидимість атаки — збір інформації через відкриті джерела не викликає тривоги в системах моніторингу безпеки. Здебільшого, вони просто не бачать такі дії. Якщо не йдеться, наприклад, про сканування портів системи.

Висока ефективність — розуміння внутрішніх процесів організації дозволяє ефективно планувати подальші атаки.

Використання методів соціальної інженерії

Наявність великого об'єму інформації дозволяє створювати цільові фішингові листи, які важко розпізнати навіть уважним співробітникам.

1.4 OSINT у моделюванні загроз: аналіз релевантних атак на корпоративну інфраструктуру

Модель загроз — формалізоване представлення аналізу потенційних загроз для ІКС організації.

Вона враховує:

– Активи організації (сервери, дані, користувачі);

– Можливих зловмисників (APT-групи, конкуренти, внутрішні загрози);

– Вектори атак (фішинг, соц. інженерія, технічні експлойти);

– Імовірність реалізації загроз та рівень впливу.

На етапі створення моделі загроз, завдяки використанню OSINT, можна:

– Ідентифікувати цифрові сліди компанії (наприклад, через Shodan, Censys, DNSdumpster);

– Виявити витоки даних (через HaveIBeenPwned, Dehashed);

– Проаналізувати поведінку співробітників у соцмережах, що може слугувати точкою входу для атак;

– Відстежити згадки про компанію або її інфраструктуру на хакерських форумах, у Telegram, dark web тощо.

Класифікація атак за рівнем критичності:

– **Критичні:** можуть зупинити бізнес-процеси компанії (викрадення фінансових даних, доступ до внутрішньої мережі хакерами);

– **Суттєві:** обмежений вплив, але потрібно реагувати (наприклад, спроби фішингу чи використання соціальної інженерії);

– **Незначні:** не мають реального впливу (згадки в мережі на веб-сайтах без фактів витоку даних).

Переваги використання OSINT у моделюванні загроз наступні:

– Проактивний підхід - атаки можна ідентифікувати до їх реалізації;

– Актуальність - можна відслідковувати інформацію про компанію моментально. Пошукові роботи працюють 24/7;

– Мінімізація витрат - інструменти, здебільшого, безкоштовні.

Для ідентифікації основних типів загроз, що виникають внаслідок використання даних, отриманим завдяки OSINT-технологіям, доцільно розглянути модель загроз для атак з використанням OSINT-технологій, наведену в табл. 1.2.

Таблиця 1.2

Модель загроз для атак з використанням OSINT-технологій.

№	Тип загрози	Джерело OSINT	Ймовірність	Вплив	Приклад атаки
1	Компрометація корпоративної пошти	Витоки (Dehashed, Pastebin)	Середня	Високий	Вхід до системи через злиті облікові дані
2	Витік API-ключів	GitHub, Google Dorks	Середня	Високий	Доступ до внутрішніх API, управління бізнес-логікою
3	Доступ до відкритих RDP/VPN	Shodan, Censys	Висока	Високий	Атака через незащищений протокол

Продовження табл. 1.2

4	Повне картографування інфраструктури	DNSdumpster, Netcraft	Середня	Високий	Визначення слабких вузлів системи
5	Скомпрометована особиста інформація	Витоки персональних даних	Середня	Високий	Маніпуляції з банківськими даними, крадіжка особистості
6	Соціальна інженерія через відео/ЗМІ	YouTube, інтерв'ю керівників	Середня	Високий	Deepfake, підробка дзвінків чи повідомлень
7	Фішинг на основі ролей	LinkedIn, вакансії	Висока	Середній	Імітація внутрішнього HR або CEO
8	Використання відкритих CVE	Shodan, ExploitDB	Середня	Середній	Атака через незакриту вразливість у ПО
9	Ідентифікація хостингу чи провайдера	WHOIS, DNS-записи	Висока	Середній	Атака на сторонні сервіси компанії

Продовження табл. 1.2

10	Використання витоків резюме співробітників	Job-сайти, LinkedIn	Висока	Середній	Збір технічної інформації про стек, ПО, доступи
11	Виявлення незахищених CMS	BuiltWith, Wappalyzer	Висока	Середній	Атака через застарілу CMS чи плагіни
12	SEO-атака через схожі домени	WHOIS, перевірка доменів	Середня	Середній	Підміна вебсайту, перенаправлення трафіку
13	Спам-атаки через email-збір	Whois, Google, сайти	Висока	Низький	Масова розсилка небажаних листів
14	Визначення локації офісу/працівників	Google Maps, Instagram	Середня	Низький	Фізичний доступ, соціальна інженерія
15	Сканування технічного стеку сайту	Nmap	Середня	Низький	Розвідка, вибір цілей на основі версій ПЗ

Висновок за розділом 1

На основі аналізу тем, висвітлених у розділі 1, було зроблено такі висновки:

Технології OSINT, як галузь сучасної розвідувальної діяльності, є потужним інструментом для збору інформації з відкритих джерел, що значно збільшує ризики витоку конфіденційних даних та цілеспрямованих кібератак на корпоративні інформаційні системи.

Основні принципи OSINT включають доступність, відкритість, масштабованість та невидимість для об'єкта, що робить ці методи особливо привабливими для зловмисників.

Існує кілька типів розвідки OSINT (FININT, GEOINT, SIGINT, HUMINT, CYBINT, TECHINT, MASSINT, IMINT), кожен з яких має конкретні джерела, методи та цілі. Знання цих типів дозволяє більш ефективно оцінювати ризики та розробляти стратегії захисту.

Аналіз реальних атак на основі OSINT показує, що навіть базова інформація, отримана з відкритих джерел (соціальні мережі, метадані, публічні реєстри), може бути використана для побудови цільових сценаріїв вторгнення в корпоративні мережі.

Технології OSINT відіграють вирішальну роль у моделюванні загроз і є невід'ємним інструментом як для наступальних, так і для оборонних цілей у контексті кібербезпеки. Аналіз відповідних випадків дозволяє зробити висновок, що проактивне виявлення та моніторинг відкритих джерел повинні стати обов'язковим елементом сучасних систем інформаційної безпеки.

Таким чином, розділ 1 закладає теоретичну основу для подальших досліджень методів протидії атакам на основі OSINT у корпоративному середовищі.

РОЗДІЛ 2
РОЗРОБКА МЕТОДУ ПРОТИДІЇ КІБЕРАТАКАМ З ВИКОРИСТАННЯМ OSINT-ТЕХНОЛОГІЙ

2.1 Оцінка вразливостей корпоративних даних для атак з використанням OSINT-технологій

В умовах цифрової трансформації компанії активно використовують інтернет-сервіси для взаємодії з клієнтами (користувачами), постачальниками, партнерами, співробітниками. Робота в мережі призводить до того, що значна частина інформації про компанію опиняється у відкритому доступі. Звісно, що цю інформацію ніхто не класифікує та не фільтрує. OSINT (Open Source Intelligence) — технологія збору інформації з відкритих джерел - може надати зловмисникам (хакерам) повну та необхідну інформацію про систему для її зламу. Наприклад — потенційні вразливості; характеристики програмного забезпечення; конфіденційну інформацію для входу в систему; інформація про користувачів та іншу. Оцінка таких вразливостей дозволяє визначити рівень ризику та ступінь відкритості організації для OSINT-атак [10].

Основні категорії вразливих даних у корпоративному середовищі

Інфраструктурні метадані

Інфраструктурні дані — одні із найцінніших джерел для OSINT-аналітика є технічні дані про інфраструктуру компанії. IP-адреси, відкриті порти, субдомени та доменні імена визначаються на перших етапах при підготовці до атаки на ціль. Такі метадані дозволяють зловмиснику отримати топологію мережі компанії, виявити вразливості, потенційні точки доступу, непривальну конфігурацію служб чи сервісів, що може бути корисним під час планування і проведення атаки. Наприклад, можна дізнатись і потім експлуатувати вразливість сервісного ПЗ чи протоколу. Як варіант - EternalBlue, вразливість протоколу SMB v1. Наявність публічних IP-адрес з відкритими портами - також

може бути потенційною загрозою, яка завжди є першим етапом у ланцюжку планування кібератак.

Основні інфраструктурні метадані:

– IP-адреси, доменні імена, підмережі, конфігурації DNS;
– Дані, зібрані через ресурси типу Shodan, Censys, ZoomEye;
– Відомості про відкриті порти, версії служб, банери веб-серверів.

Технічна інформація про ПЗ

Ще однією категорією OSINT-інформаціє в корпоративному середовищі є відомості про встановлене ПЗ. Наприклад, сканування веб-сайті компанії відкритими сканерами для отримання даних про CMS (WordPress, Joomla та інші). Проводиться шляхом перегляду коду сайту та пошуку необхідних тегів чи імпортів. Також можна знаходити встановлені плагіни (та їх версії), JavaScript-бібліотеки, API-ендпоінти, фреймворки, мови програмування тощо. Ці дані допомагають ідентифікувати "скелет" сайту та його вразливості за допомогою баз даних CVE чи сервісів типу Exploit-DB. Відсутність оновлень, використання застарілих модулів, плагінів може свідчити про практичну можливість віддаленого виконання коду (RCE), SQL-ін’єкцій або XSS-атак [11].

Основні технічні дані про ПЗ:

– Версії вебсерверів, CMS, плагінів, фреймворків;
– Публічно доступні тестові середовища, бекенди, API-ендпоінти.

Особисті дані співробітників

За допомогою пошуку по соц. мережам, аналізу веб-сайту компанії чи використання методу соціальної інженерії можна легко отримати дані про співробітників. Саме особисті дані робітників компанії становлять найвищу цінність для OSINT-розвідки. Аналіз LinkedIn, Facebook, Twitter, GitHub - хакер отримує інформацію про посаду, досвід роботи, службові пошти, стиль мовлення, інтереси. Після цього, вочевидь, є можливість створення індивідуальних фішингових компаній (саме для кожного користувача окремо). Створення профілю довіри, омани через телефон (vishing), компрометаційного впливу чи шантаж співробітників. Особливо важливо - щоб співробітники не

публікували та не використовували службові дані в мережі. Наприклад - використання службових пошт для логіну в інтернет-ресурсах чи публікування фотографій документації безпосередньо з офісу [12].

Основні дані співробітників:

– Дані зі сторінок у LinkedIn, Facebook, GitHub, Twitter;

– Службові e-mail, посади, номери телефонів, зразки мовлення/поведінки.

Конфіденційні документи та файли

Нерідко конфіденційні документи компанії опиняються у відкритому середовищі через незахищеність хмарних сховищ або несанкціонованого їх витоку у мережу. Неправильного налаштовані Dropbox, Google Drive сховища, FTP-сервери чи приватні репозиторії на GitHub. За допомогою технік типу Google Dorking можна легко шукати такі файли навіть без прямого доступу до систем компаній.

Наприклад: "site:company.com filetype:pdf confidential".

Ще одна вразливість полягає у наявності метаданих у файлах: автори документів, версії ПЗ, дати створення чи редагування, шляхи директорій можуть допомогти дізнатися структуру компанії (користувачів), внутрішні директорії системи, назви використовуваних інструментів. Саме тому очищення метаданих повинно бути впровадженим та автоматизованим [13].

Основні документи, що потрапляють у відкриту мережу:

– Документи, випадково опубліковані через Google Dorking або на відкритих сервісах зберігання (наприклад, Google Drive, Dropbox);

– Службові PDF, DOCX-файли з метаданими, в яких є імена авторів, структури папок, версії офісного ПЗ.

Реєстраційна та юридична інформація

За допомогою OSINT можна отримати інформацію навіть з державних баз даних, публічних реєстрів в інтернеті, реєстрів юридичних осіб, тендерних платформ, судових реєстрів та інші. Така практика дозволяє отримати достовірну інформацію про структуру компанії, наявність філій, контактні особи та їх дані.

Юридичні документи, опубліковані на таких сайтах, можуть містити конфіденційну чи службову інформацію, що не може бути розкритою публічно - внутрішні процедури, IT-структуру або навіть згадку про конкретні програмні рішення. Такі дані розширюють розуміння структуру організації; полегшують формування картини цілей для подальших атак [14].

Наприклад: Дані з офіційних державних реєстрів, реєстраційних документів, тендерних платформ.

Методи ідентифікації вразливостей через OSINT:

– Використання Google Dorking — пошук специфічних документів, конфігураційних файлів, логів або вікон доступу за допомогою спеціальних запитів у Google;

– Використання спеціалізованого ПЗ — Maltego, SpiderFoot, Recon-ng. Дозволяє автоматизувати складання профілю компанії на основі множини відкритих джерел;

– HaveIBeenPwned, Dehashed — перевірка, чи з'явилися службові акаунти чи поштові сервіси співробітників у публічних витоках (базах даних);

– Методи аналізу медіа-профілів користувачів — отримання інформації про їх посаду та можливості в компанії;

– Методи пасивного аналізу мережі — збирання даних WHOIS, DNS, ASN, SSL-сертифікатів.;

– Методи активного аналізу мережі — сканування портів (Nmap, MassScan), визначення ОС, ПЗ та їх версій (наприклад MetaSploit - також використовується для експлуатації вразливостей). Traceroute - дозволяє побачити маршрут, яким трафік проходить до цілі, включачи всі проміжні вузли [15].

Типові вразливості в корпоративному середовищі:

– Використання однакових паролів у службових та особистих акаунтах співробітників;

– Публікація технічної документації (наприклад, API-доків, конфігурацій) на GitHub або корпоративних сайтах;

– Неочищені метадані в службових документах;

– Недостатній (чи відсутній) контроль над персональними акаунтами співробітників;

– Відкриті порти та сервіси, які необхідно закрити чи вимкнути;

– Інформація про версії, наявність ПЗ та служб в системі;

– Невиправлені вразливості програм;

– Використання неліцензованих програм;

– Публічно доступні API, API-ключі;

– Доступні конфігурації DNS;

– Використання застарілих протоколів;

– "Відкритість" хмарних сервісів;

– Зберігання конфіденційної, службової інформації на відкритих хмарних сховищах;

– Публічне розголошення через соц. мережі.

Критерії оцінки рівня вразливості

"Відкритість" даних можна оцінити наступним шляхом, проаналізувавши:

– **Рівень відкритості даних —** наскільки легко їх знайти (відкриті пошукові системи/спеціалізовані сервіси);

– **Ступінь чутливості —** чи може ця інформація бути використана для компрометації;

– **Можливість автоматизації збору —** чи можна створити скрипт або бот для збору подібних даних;

– **Потенційний вплив —** наскільки великої шкоди може завдати доступ до цих даних (фішинг, доступ до інфраструктури, шантаж).

2.2 Обмеження доступу до чутливої інформації у відкритих джерелах

Ідентифікувавши наявність та варіанти доступу до чутливої інформації в мережі інтернет, логічним кроком буде спробувати обмежити доступ до таких даних чи зробити їх використання неможливим. Знання про вразливості та способи доступу до системи може дозволити зловмисникам отримати доступ до внутрішніх ресурсів компанії, що збільшує ризик кібератак. Тому необхідно вживати заходів для контролю та обмеження поширення чутливої інформації в публічних джерелах [16].

Робота з метаданими документів

Як було вказано вище, по метаданим певного файлу можна отримати багато інформації про внутрішні процеси організації. Це може бути використано зловмисниками для планування майбутніх атак. Найчастіше це стосується офісних файлів, таких як документи DOCX, PDF, XLSX, PTX, що були опубліковані або збережені без належного захисту. Інструментів для виявлення метаданих купа - наприклад сервіс ExifTool, що досліджує файли на вміст метаданих та показує їх.

Для мінімізації ризиків потрібно впровадити інструменти для автоматизованого очищення метаданих перед публікацією або розповсюдженням. Потрібно навчити співробітників перевіряти, чи може певний документ потрапити до відкритого доступу і чи має він метадані чи шкідливий вміст.

Контроль за інформацією, що було розміщено в соціальних мережах

Невелика кількість компаній контролює дані, які співробітники публікують у соц. мережах. Це може бути як професійна інформація (вакансії, події, івенти, зустрічі, зв'язки з іншими компаніями), так і особисті дані (адреси, телефони, посади, пошти). Ці дані можуть бути використані для подальших атак методом соціальної інженерії [17].

Співробітники повинні бути обізнаними щодо того, що робочі дані не повинні контактувати з особистими. На особистих сторінках, як і на робочих, не

повинно бути жодної конфіденційної інформації. Дані, що опубліковані у особистих профілях користувачів не повинні бути пов'язані з робочими профілями, адресами, доменами. Можна використовувати інструменти моніторингу, такі як Social Search або LinkedIn для виявлення випадків розкриття чутливої інформації.

Захист даних через відкриті порти та сервіси

Відкриті порти можуть надати хакерами доступ до внутрішніх ресурсів організації. Інструменти по типу Shodan чи Censys дозволяють публічно і автоматизовано моніторити публічно доступні сервери, пристрої та мережі; показують можливі вразливості та помилки. Це включає порти для FTP, SSH, Telnet, HTTP/HTTPS, які можуть бути використані для атаки. Сервіси також мають пошук по ключовим запитам (аналог Google Dorking).

Компаніям потрібно регулярно перевіряти відкриті порти за допомогою інструментів для сканування мереж. Важливо налаштовувати брандмауери та VPN так, щоб тільки авторизовані користувачі з відповідних IP-адрес мали доступ до внутрішньої мережі компанії.

Інформація з відкритих реєстраційних та юридичних документів

Хакери можуть отримати конфіденційну чи службову інформацію використовуючи відкриті реєстрі, каталоги, бази даних. Таким чином можна отримати організаційно-штатну структуру компанії, імена керівників, дані про активи, статуси працівників і так далі. Багато з таких реєстрів доступні у мережі інтернет навіть без ідентифікації користувача [18].

Недостатній рівень контролю за публічними API

API, які надаються чи використовуються компаніями для розробників чи підключення до інших сервісів, можуть бути відкритими та не мати достатнього рівня безпеки. Поширена практика — знаходити API ключі на GitHub у відкритих репозиторіях. Через такі інтерфейси хакер потенційно може отримати доступ до даних або сервісів організації.

Потрібно налаштовувати автентифікацію через, наприклад, OAuth, обмежувати доступ до API (використання брандмауерів та WAF) та API-ключів. Перевіряти API на наявність вразливостей (Burp Suite, OWASP ZAP).

Політика безпеки у хмарних сервісах

Майже кожна компанія користується хмарними послугами для зберігання, передачі чи обробки даних. Такі сервіси також повинні бути коректо налаштовані. Неправильні налаштування AWS, Google Cloud, Google Disk, Azure, DropBox та інших можуть надати доступ хакерам до всіх файлових об'єктів організації. Доступ до таких ресурсів також можливо автоматизовано шукати в інтернеті.

Налаштована політика безпеки використання і налаштування хмарних сервісів. Використання контролю доступу на основі ролей (RBAC), налаштування IAM в AWS. Проводити регулярну перевірку та оцінку налаштувань безпеки через такі інструменти, як AWS Inspector чи Cloud Security Posture Management (CSPM).

Перевірка даних перед публікацією

Якщо файл потрапляє у відкритий доступ, потрібно переконатися, що всі чутливі дані (паролі, пошти та логіни користувачів) були видалені з файлу.

Використання інструментів для очищення метаданих, а також інструментів, що дозволяють перевірити вміст документів на наявність конфіденційної інформації.

Захист інформації від витоку через соціальну інженерію

Використовуючи майже будь-які дані про організацію, хакер може використати методи соціальної інженерії для того, щоб отримати ще більше інформації від співробітника або змусити його зробити певні дії. Взагалі, така практика не є поширеною. Якщо планується атака - невдалий фішинг чи інша спроба соціальної інженерії викриває плани хакерів. Найчастіше, такі методи використовують зі 99% впевненістю, що атака буде вдалою [19].

Навчання співробітників протистояти методам соціальної інженерії, розуміти "джерело" розуміння певної інформації незнайомими особами;

тренінги з безпеки, внутрішні політики для виявлення потенційних спроб соціальної інженерії.

2.3 Захист персональних даних співробітників у відкритих інтернет-джерелах

Отримання персональних даних співробітників є пріоритетною ціллю хакерів. Така інформація збирається та аналізується як можливий вектор для побудови атаки. Дані можуть бути використані для фішингових атак, соціальної інженерії, компрометації внутрішніх систем, створення фальшивих акаунтів тощо. Тому потрібно належно захищати дані співробітників у мережі Інтернет [20].

Перелік персональних даних, які можуть потрапити у відкритий доступ та підлягають захисту чи хоча б розуміння того, що вони можуть бути використані для подальших атак:

– Ім’я, прізвище, по батькові — доступні через соцмережі, корпоративні сайти, соціальні мережі, LinkedIn, GitHub;

– Посада, підрозділ, місце роботи — часто вказується в професійних профілях;

– E-mail-адреса (особливо службова) — часто публікується у відкритих презентаціях, форумах, технічній документації;

– Номер телефону — можна знайти в оголошеннях, профілях або витягнути з витоків;

– Фото — використовується для ідентифікації особи або генерації фейкових акаунтів;

– Графік роботи, пересування, відпустки — може бути відомим з публікацій у соцмережах.

Наявність навіть мінімальної кількості даних у мережі 100% стовідсотково буде використана для зламу систем компанії.

Потенційні загрози, пов'язані з наявністю персональних даних у мережі:

– Spear phishing — атаки на конкретного співробітника з використанням персоналізованих листів;

– Social engineering — маніпуляція через довіру (наприклад, атака від імені “керівника”);

– Імперсоналізація — створення фейкових акаунтів для отримання доступу до внутрішніх систем або партнерів;

– Доступ до внутрішніх систем через компрометацію облікового запису – часто починається з OSINT-збору;

– Фішинг - виманювання особистих даних. Зазвичай поєднує кілька атак вище.

Методи захисту персональних даних у відкритому доступі

Політика інформаційної гігієни

Потрібно розробити чіткі правила для співробітників щодо публікації особистої та службової інформації в мережі. Заборонити публікацію службової інформації (наприклад внутрішні номери, пошти, IP-адреси, фото з робочих місць, наявне апаратне і програмне забезпечення) [21].

Навчання персоналу

Навчання персоналу правилам інформаційної гігієни. Проведення тренінгів для розуміння, яка інформація не повинна бути публічною і як її знаходять та використовують зловмисники. Безпекові інструкції з використання та налаштування приватності в соц. мережах, GitHub, LinkedIn, Medium та іінші.

Періодичний OSINT-аудит

Хоча практика OSINT-аудиту не є загальноприйнятою, в аудиті нерідко використовуються OSINT-інструменти. Провести OSINT-дослідження компанії завжди корисно, наприклад для пентесту (робиться завжди) чи оцінки ризиків (майже не робиться). Розуміючи, які дані можна зібрати про компанію, можна побудувати ефективний план захисту. Спеціальні допоміжні інструменти - Maltego, Skopenow, Spiderfoot, сервіси для перевірки витоків паролів та інші.

Видалення або ірраціоналізація (унеможливлення) використання даних

Спроби видалити певну інформацію з певного ресурсу може ускладнити її отримання. Зазвичай подають запити до веб-сайтів чи їх хостерів на видалення певної інформації. Також є варіант маскування (приховування від загального доступу в пошуковій мережі) інформації на публічних видимих сайтах.

2.4 Використання псевдонімів та анонімізації в публічних профілях

Гарна практика — використання псевдонімів та анонімізації в публічних профілях. Особливо для працівників, що займають головні посади в IT-відділах, безпеки або керівництва. Саме вони є об'єктами цілеспрямованої розвідки [22].

Псевдонімізація — метод заміни справжніх імен, ніків та інших ідентифікаторів на вигаданий псевдонім (не повинен бути прямолінійно пов'язаний з посадою), не повинен бути прямо пов'язаний з особою, її реальною ідентичністю, не повинен містити додаткової інформації, не повинен дублюватися у інших сервісах.

Анонімізація — повне або часткове приховування будь-яких особистих даних, за якими можна ідентифікувати особу в цифровому просторі.

Конкретні методи псевдонімізації та анонімізації

Використання вигаданих імен в особистих акаунтах

Наприклад, замість "Koval Dmytro" — KDSec. Особисто актуально для публікацій у форумах, GitHub, Medium та інших веб-сайтах.

Розмежування службових і особистих профілів

Службовий акаунт, як і службова інформація не повинні перетинатися з особистими даними та профілями співробітника. На службовому акаунті - мінімально потрібний набір контактної інформації для роботи. На особистому акаунті - бажана відсутність згадок про компанію чи посаду. Відсутність службової інформації. Приховування або обмеження видимості конфіденційної інформації на веб-ресурсах та соц. мережах. Приватні профілі у LinkedIn,

Facebook, Instagram та інші. Сховані друзІ, цифрова активність, прихований список контактів, геолокація. Використання аватарів замість реальних фото в робочих профілях.

Малюнки, абстракції чи символи замість власного обличчя. Такий метод анонімізації ускладнює ідентифікацію особи через пошук зображень (наприклад Google Image Search).

Заміна службових e-mail на загальні. Наприклад пошта kovald@company.com може бути замінена на it.support@company.com.

2.5 Захист корпоративних доменів від освітлення відкритими джерелами (OSINT)

Розвідка корпоративних доменів цілі робиться в першу чергу. Аналізуються реєстраційні дані головного домену, структура піддоменів, пов'язані IP-адреси, поштові сервери, DNS-записи та інші. Ці дані можуть бути використані для підготовки атак різного типу - від фішингу до складних цільових вторгнень (APT) [23].

Основні канали отримання інформації про корпоративні домені організації:

WHOIS-інформація - база реєстраційних даних, що містить:

- ПІБ реєстратора;
- Контактну особу (реальну людину, співробтіника);
- E-mail, номери телефонів, фізичну адресу;
- Дати створення/завершення реєстрації;
- DNS-розвідка

За допомогою спеціалізованих сервісів (наприклад DNSDumpster) можна отримати наступну інформацію:

- IP-адресу основного сервера;
- MX-записи (поштові сервери);

– SPF, DKIM, DMARC — налаштування захисту пошти;

– CNAME, TXT-записи.

Наприклад, аналізуючи DNS запити, можна виявити погано налаштований субдомен test.company.com, який веде на тестове середовище без автентифікації.

Виявлення субдоменів

За допомогою інструментів (Sublist3r, Amass, crt.sh) зловмисники знаходять всі наявні субдомени організації. Потім перевіряють кожен окремо.

Перегляд цифрових сертифікатів (SSL/TLS)

Сервіси типу crt.sh дозволяють переглядати видані сертифікати з усіма субдоменами.

Метадані сайтів і банери сервісів

Через HTTP-запити або сканери типу Shodan можна отримати веб-версію сервера, назву та версію CMS, структуру URL, хедери.

Методи захисту корпоративних доменів від OSINT-аналізу

Приватність WHOIS-даних

Потрібно використовувати функцію WHOIS Privacy Protection, яка приховує ваші дані від звичайних користувачів. Реєстрацію домену краще робити на спеціальну (цільову) захищену (MFA) пошту, яка не буде використовуватися для інших речей.

Регулярний моніторинг субдоменів

Потрібно використовувати сканери (Amass, Subfinder, DNSdumpster) для виявлення несанкціонованих субдоменів. Видаляти або закривати тестові середовища чи середовища для розробки. Впроваджувати WAF (Web Application Firewall) для внутрішніх субдоменів, якщо вони публічні [24].

Захист DNS-записів

Потрібно мінімізувати публічність TXT-записів. Свідомо налаштовувати SPF, DKIM, DMARC записи, щоб унеможливити підробку e-mail адрес. Сегментувати сервіси — поштові, веб, CRM на окремих IP-адресах.

Використання та контроль SSL-сертифікатів

Потрібна наявність SSL-сертифікату на сайті, що забезпечує шифрування трафіку між веб-сайтов та кінцевим користувачем, використовуючи протокол HTTPS. Змінювати застарілі сертифікати.

Захист тегів та серверних повідомлень

Потрібно приховувати банери сервісів (Apache/Nginx), не залишати версію у відповідях. Мінімізувати наявність HTTP-хедерів (X-Powered-By, Server), не залишати небезпечну інформацію у файлах /robots.txt, /sitemap.xml.

Також, можна використовувати:

Техніку "Honeypots" для субдоменів. Суть техніки у тому, що створюється додаткова, потенційна ціль, яка приваблює хакерів. Вони сканують, вивчають її. Хоча по факту там нічого немає.

DNSSEC — набір безпекових розширень до протоколу DNS, які забезпечують автентичність і цілісність DNS-відповідей.

2.6 Політика безпеки для співробітників: правила використання соціальних мереж і інтернету

Створення політики безпеки для співробітників — конкретні правила використання соціальних мереж та мережі інтернет. На меті — унеможливлення отримання хакерами чутливої інформації про компанію з соціальних мереж.

Вразливість соціальних мереж

Як показує практика досліджень, наступна інформація, що може допомогти хакерам, береться саме з соціальних мереж:

– Реальне місце роботи;

– Службову електронну адресу;

– Внутрішню корпоративну термінологію;

– Деталі про поточні проєкти або технології, що використовуються в компанії;

– фото з офісу, конференцій, презентацій, які можуть містити конфіденційну інформацію (наприклад, логотипи, адреси, ID-бейджі, діаграми, імена колег).

Наприклад: на селфі знімку видно бейдж з повним ім'ям, посадою та компанію працівника. Використовуючи ці інформацію, зловмисник може знайти його профілі у GitHub, LinkedIn на інших сайтах, а потім скласти фішинговий лист із персоналізованим зверненням [25].

Рекомендована політика безпеки щодо соцмереж

Для зниження ризиків, потрібно додати наступні пункти до політики використання соціальних мереж та мережі Інтернет співробітниками:

Оцінка рівня публічності профілів

Працівникам бажано рекомендувати встановлювати приватність профілів на рівні "тільки для друзів" чи "обмежений доступ". Хакер не зможе знайти і проаналізувати такий профіль. Рекомендовано не вказувати повну назву компанії в описі профілю. Уникати прив'язок службових даних (пошта, номери) до соц. мереж.

Заборона публікації службової інформації

Заборонити розміщення фото з внутрішніх приміщень офісу. Заборонити публікувати робочі моменти, листування, скріншоти, аудіо- та відеоінформацію, технічну документацію, плани проектів, інформацію про зустрічі офлайн та онлайн. Не використовувати корпоративну IP-адресу для заходження на особисті профілі.

Регулярне навчання персоналу

Щоквартальні тренінги з інформаційної гігієни. Працівники повинні розуміти, що будь-яка їх публікація потенційно може бути проаналізована зловмисником. Потрібно проводити тестування, симуляції соціальної інженерії, інструктажі перед конференціями

Загальні правила корпоративного інтернет-користування

– Заборона входу на підозрілі сайти або використання ненадійних онлайн сервісів;

– Заборона входу на особисті профілі/ресурси з мережі компанії;

– Використання VPN для віддаленого підключення до офісної мережі;

– Блокування трекінгових скриптів і кукі через розширення браузера на робочих ПК;

– Моніторинг корпоративного трафіку з метою виявлення нетипової активності (наприклад за допомогою Wireshark);

– Використання ізольованих середовищ (sandbox) для перевірки підозрілих файлів.

Впровадження перелічених правил значно ускладнить чи навіть унеможливить OSINT-збір інформації про компанію через профілі працівників у соц. мережах. Ускладнить навіть сам пошук таких профілів. Знижує ризик цільових атак методами соціальної інженерії, фішингу і так далі. Ускладнить встановлення точних зв'язків між співробітниками. Зменшить до нуля кількість конфіденційної чи службової інформації про компанію, технічної інформації [26].

2.7 Моніторинг і аналіз відкритих джерел для виявлення можливих загроз/інформації про компанію

Цей пункт присвячено пошуку, моніторингу та аналізу інформації з відкритих джерел для виявлення потенційних загроз; розуміння того, що про компанію знають хакери і подалі розуміння векторів/структури атак, які базуються на отриманій інформації [27].

Моніторинг полягає у систематичному зборі, фільтрації та аналізі інформації про компанію, що знаходиться у публічному доступі. Зазвичай моніторяться відкриті реєстри, сайти-каталоги, веб-архіви; використовуються сервіси, які повідомляють про витоки конфіденційної інформації з баз даних

(наприклад haveibeenpwned). Така діяльність дозволяє проактивно виявляти вразливості та передчасно реагувати на них.

Джерела OSINT, які доцільно моніторити

Соціальні мережі працівників (LinkedIn, Facebook, Instagram, Twitter(X), Telegram, Medium та інші)

Можна виявляти витоки інформації через пости (публікації), фейкові профілі компанії, її працівників та партнерів.

Форуми, Telegram-канали

На спеціалізованих напівзакритих форумах (реєстрація по запрошенню, закрита реєстрація, платна реєстрація) в мережі Інтернет, у Telegram каналах доцільно моніторити інформацію на предмет витоку, продажі та пошуку інформації, що стосується компанії за гроші, обговорення вразливостей/зламаних облікових записів у системі, інформацію про майбутні атаки.

Платформи для розміщення коду (GitHub, GitLab, Bitbucket)

Доцільно перевіряти перелічені вище платформи на наявність розміщення конфіденційних файлів (API-ключі, паролі, токени), відкритих репозиторіїв, документацію з технічною інформацією, внутрішніми IP-адресами, структурами, процесами.

Paste-сайти (Pastebin, Ghostbin)

Такі сайти чудово індексуються пошуковими роботами та можуть бути легко знайдені, використовуючи спеціалізовані запити (Google Dorks). Там можна знайти (за наявності) дампи баз даних, списки паролів, користувачів; оголошення про злам системи.

Пошукові сервіси інфраструктури (Shodan, Censys)

Сервіси дозволяють виявити відкриті порти, вразливі частини мережі. Є пошук сервісів компаній з уразливими конфігураціями.

DNS, WHOIS, Certificate Transparency Logs

Моніторяться з метою виявлення підроблених або новостворених доменів, що схожі на офіційні та в майбутньому будуть використані як складова фішинг-атак.

Інструменти для аналізу та моніторингу такої інформації

– SpiderFoot — автоматизований збір технічної, доменної та персональної інформації;

– Maltego — графічний інструмент для побудови зв'язків між об'єктами (IP, домени, email);

– theHarvester — пошук email-адрес, доменів, користувачів у відкритих джерелах;

– Recon-ng — платформа для комплексної розвідки;

– Google Dorks — спеціалізовані пошукові запити, що дозволяють знаходити уразливу інформацію.

Приклади загроз, що можна виявити:

– Злив корпоративної пошти на Pastebin (Email адреси, паролі - здобуті внаслідок фішингу або витоку даних);

– Поява домену по типу corp-name-support.com - імітація офіційного сайту для фішингових атак;

– Розміщення токенів Slack або AWS у відкритому середовищі GitHub - надає зловмиснику прямий доступ до використання корпоративних ресурсів;

– Обговорення діяльності компаній в Telegram-каналах - можна знайти інформацію про наміри публікації інформації, майбутні протиправні дії тощо;

– Фото працівників з офісу, де видно схеми інфраструктури, скріншоти, документацію - може бути використано для різного виду атак;

– Витік пари email:password від підключеного сервісу - отримання результатів від haveibeenpwned, що до вашої email-адреси наявний пароль у відкритому доступі [28].

План моніторингу відкритих джерел

Визначається політика постійного моніторингу. Визначається перелік об'єктів: домени, пошти, імена ключових осіб, IP-адреси, які необхідно перевірити на витік даних. Регулярно оновлювати ключові слова, інструменти для моніторингу.

Визначаються процедури реагування на виявлені інциденти. Повідомляється голова відповідального відділу (скоріш за все IT-відділ чи відділ кібербезпеки), аналізується ступінь загрози, за можливості усувається витік даних (видалення публікації, ротація паролів, інформування працівників, нові інструктажі та чеклісти з діями).

2.8 Використання приватних реєстраторів і захист dns для корпоративних доменів

Важливість управління корпоративними доменами, включаючи приватних реєстраторів та захист DNS-систем в контексті протидії кібератакам із використанням технологій OSINT було описано вище. Наступні заходи значно знижують ризики витоку конфіденційної інформації та ускладнюють збір технічних даних про компанію хакерами [29].

Використання приватних (анонімних) рєстраторів — способ приховування WHOIS інформації власників доменів (email, телефон, ПІБ, адреси).

Це ускладнює зловмисникам виявлення:

– Осіб, на яких зареєстрований домен і які відповідальні за роботи з доменами;

– Потенційних службових email-адрес;

– Фізичних адрес, що можуть бути використані в соціальній інженерії;

– Інформації про структуру організації (при масовому аналізі WHOIS-запитів).

Стратегія використання ізольованих облікових засобів

– Створення окремого облікового запису для доменної реєстрації, який не пов'язаний з основною інфраструктурою;

– Використання унікальної email-адреси, ціль якої - саме реєстрація та комунікація з доменним реєстратором;

– Реєстрація домену не на фізичну, а на ім'я юридичної особи;

– Не використовувати корпоративні email, які можуть бути скомпрометовані.

Такі дії максимально знижують можливості хакерів щодо отримання інформації про власників домену. Знижують ризик отримання контролю над зареєстрованим акаунтом, що в перспективі може призвести до заволодіння контролю над поштовими серверами, сайтами, DNS- та mail запитами.

DNS захищається наступним чином:

Використання DNSSEC (DNS Security Extensions)

Гарантує захист від підміни відповідей DNS-серверів; забезпечує цілісність інформації, що передається через DNS. Унеможливлює атаки типу "cache poisoning" [30].

Захист панелі управління DNS

Встановлення хоча б 2FA (а краще MFA) для доступу до реєстратора. Обмеження доступу до пулу IP-адрес (за можливості). Регулярне оновлення паролів та аудит логів.

Використання резервних DNS серверів

Гарантує забезпечення стійкості до DDoS-атак і відмов інфраструктури. Також використовується для розподілення навантаження.

Моніторинг змін у DNS-записах

Моніторинг і автоматичне повідомлення при спробах редагування записів. Інтеграція з SIEM-системами для виявлення аномалій.

При некоректному налаштуванні DNS або реєстрації домену, зловмисник може отримати списки субдоменів; конфігурації поштових систем (SPF, DKIM,

DMARC), що можуть бути використані при фішингових атаках (лист від надійного відправника).

2.9 Реагування на основі аналізу загроз і вжиття необхідних заходів безпеки

Після проведення комплексного моніторингу інформації у відкритих джерелах та аналізу потенційних загроз, потрібно розуміти, яким чином реагувати на виявлені загрози і які превентивні заходи безпеки можна впровадити [31].

Етапи реагування на основі OSINT-аналізу

Виявлення індикаторів компрометації (IoC):

– Емейли, домени, IP-адреси, згадки в paste-сервісах або форумах;

– Наприклад, на сайті Pastebin виявлено логін/пароль до корпоративної пошти.

Кореляція з внутрішніми подіями

Перевірка, чи є знайдені облікові записи активними, якщо ні - коли були активні. Порівняти з логами входу в корпоративні системи.

Реакція та нейтралізація

Зміна паролів, облікових записів, відключення або видалення скомпрометованих профілів. Блокування IP-адрес або доменів у фаєрволах. Повідомлення до відповідних безпекових відділів (SOC, IT-відділ).

Повідомлення, інформування, проведення тренінгів

Інформування керівництва про ідентифіковану загрозу, створення тренінгів за необхідності. Розслідування інциденту.

Типові заходи реагування, що базуються на OSINT

З метою ефективного реагування на загрози, пов’язані з OSINT-активністю, необхідно застосовувати типові заходи захисту, залежно від характеру інциденту. Перелік типових заходів реагування на основні загрози, пов’язані з OSINT представлено в табл. 2.1.

Таблиця 2.1

Перелік типових заходів реагування на основні загрози, пов'язані з OSINT

Тип загрози	**Приклад виявлення через OSINT**	**Заходи реагування**
Витік акаунтів співробітників	Бази даних у даркнеті	Зміна паролів, MFA, розслідування
Підготовка фішингової кампанії	Реєстрація схожого домену	Блокування на DNS-рівні, повідомлення співробітникам
DDoS-загроза	Telegram-канали з погрозами	Налаштування rate-limiting, резервні канали
Витік документації	Згадки в pastebin або форумах	Видалення, пошук джерела витоку, обмеження доступів

Приклади інструментів для аналізу загроз і реагування:

– HaveIBeenPwned, LeakCheck — перевірка на витік облікових даних;

– DNSTwist, UrlScan.io — аналіз фішингових доменів;

– Spiderfoot, Maltego — автоматизований OSINT-збір;

– VirusTotal, AbuseIPDB — перевірка підозрілих доменів або IP.

Створення сценаріїв для реагування

Щоб реагування було ефективним, часто створюють сценарії (playbooks) для типових інцидентів ІБ.

Вони складаються з:

– Алгоритму дій для виявлення загрози;

– Відповідальних осіб;

– Допустимих часових рамок на реагування;

– Шаблони повідомлень, звітів.

2.10 Створення методу протидії кібератакам з використанням OSINT-технологій

Проаналізувавши основні кроки для захисту корпоративної інфраструктури від хакерських атак, першим етапом яких зазвичай є розвідка, було сформовано метод (систематизована сукупність кроків для досягнення певної мети) протидії кібератакам з використанням OSINT.

Метод протидії кібератакам з використанням OSINT-технологій

Визначений метод грунтується на комплексному підході до пошуку, виявлення та аналізі відкритої інформації про компанію з метою виявлення потенційних вразливостей системи, які можуть бути потенційно використані хакерами для атак на ціль. Метод включає визначену послідовність взаємопов'язаних кроків, що дозволяють значно знизити ризики атак, які базуються на OSINT-дослідженні і підвищити загальний рівень кібербезпеки в організації.

Етап 1. Пошук інформації. Оцінка вразливостей

Спочатку здійснюється комплексний збір та аналіз усієї наявної інформації про компанію, що доступна у відкритих джерелах за допомогою OSINT. Потрібно виявити потенційні загрози і вразливості системи, які можуть бути використані хакерами [32].

На цьому етапі здійснюється:

1. Використання WHOIS інструментів для отримання даних про доменні ім'я організації, контактну інформацію про власників домену. Адресу, пошту, телефон.

2. Аналіз мережі через Shodan, Censys для виявлення відкритих портів чи серверів. Аналізуються відкриті порти, вразливості протоколів, служб, програмного забезпечення.

3. Аналіз соціальних мереж компанії та співробітників (LinkedIn, Facebook, Twitter, Telegram) для визначення структури компанії, даних про

співробітників (контакти, посади, публікації, службові дані у відкритому доступі).

4. Пошук витоків даних через платформи GitHub, Pastebin, форуми, канали у Telegram.

5. Використання Google Dorks - спеціалізовані техніки для чіткого пошуку інформації у пошуковій системі Google.

В результаті отримуємо проаналізовані дані компанії в відкритому доступі. Розуміємо, чи я інформація, що може бути використана зловмисниками для атак (соц. інженерія, технічні атаки).

На схемі зображена блок-схема першого етапу створеного методу (рис.3.1).

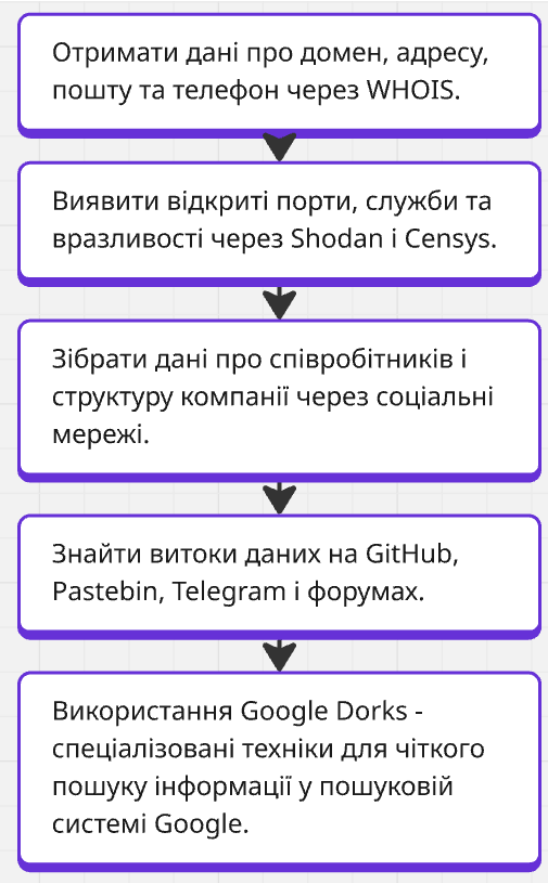

Рисунок 3.1. Блок-схема першого етапу створеного методу.

Етап 2. Обмеження доступу до інформації

На цьому етапі, після виявлення чутливої інформації, аналізу вразливостей, потрібно зменшити ризики, а саме - впровадити контроль та обмеження доступу до інформації [33].

На цьому етапі здійснюється:

1. Видалення з відкритих джерел знайденої раніше службової інформації, видалення наявних метаданих в файлах (PDF, Word, Excel, PowerPoint та інші).

2. Налаштування прав доступу на веб-серверах (файли, сайти, директорії). Налаштування .htaccess файлу (доступ до файлів, директорій, захист об'єктів паролями).

3. Створення регламентів щодо заборони публікації визначених даних у відкритий доступ. Доповнення політики безпеки.

4. Регулярний аудит відкритих ресурсів і пошукових систем на предмет наявності корпоративних даних.

В результаті контролюємо та обмежуємо інформацію з зовнішнього середовища.

На схемі зображена блок-схема другого етапу створеного методу (рис.3.2).

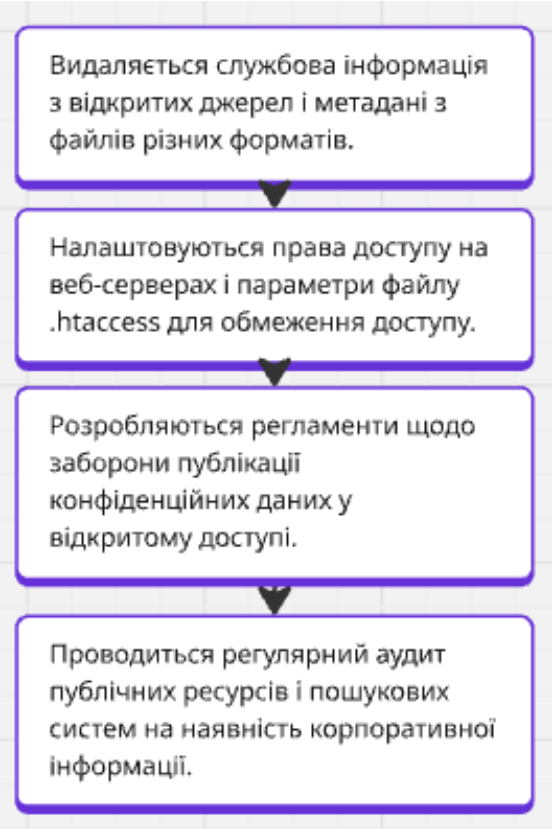

Рисунок 3.2. Блок-схема другого етапу створеного методу.

Етап 3. Захист даних персоналу

На цьому етапі проводиться робота з працівниками щодо захисту інформації, заборони публікації службової інформації в мережі, соц. мережах.

На цьому етапі здійснюється:

1. Аналіз соціальних мереж працівників з метою пошуку службових даних, фото, посад, заходів компанії.
2. Навчання працівників базових правил інформаційної гігієни. Заборона публікувати службову інформацію в соц. мережах.
3. Можлива анонімізація профілів у LinkedIn, Twitter, GitHub, Instagram та інших, видалення зайвої службової інформації, контактів інших співробітників.
4. Налаштування приватності профілів. Статус “для друзів”.

Такі дії зменшують ризик спрямованих атак (наприклад spear phisting або атаки соціальної інженерії). Ускладнюють хакерам варіанти пошуку ключових співробітників та інформації про них.

На схемі зображена блок-схема третього етапу створеного методу (рис.3.3).

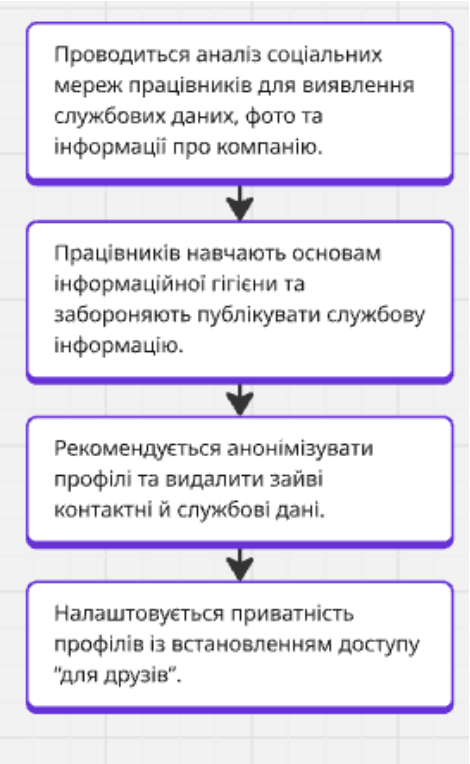

Рисунок 3.3. Блок-схема третього етапу створеного методу.

Етап 4. Захист технічних активів

На цьому етапі необхідно мінімізувати та, по можливості, видалити технічні сліди компанії у відкритих джерелах, що дозволить ускладнити зловмисникам процес збору інформації про систему [34].

На цьому етапі здійснюється:

1. Використання VPN, проксі сервісів, захищеного доступу для приховування реальних IP-адрес серверів.
2. Налаштування функцій приватності на реєстраторі домену, щоб не розкривати персональні дані WHOIS.
3. Захист DNS через DNSSEC для запобігання підробці DNS-записів.
4. Мінімізація інформації у TXT записав DNS, де можуть знаходитися метадані.
5. Видалення тестових доменів, субдоменів, непотрібних DNS-записів.

Впроваджуємо технічний захист від OSINT'у, обмежуємо варіанти отримання технічної інформації.

На схемі зображена блок-схема четвертого етапу створеного методу (рис.3.4).

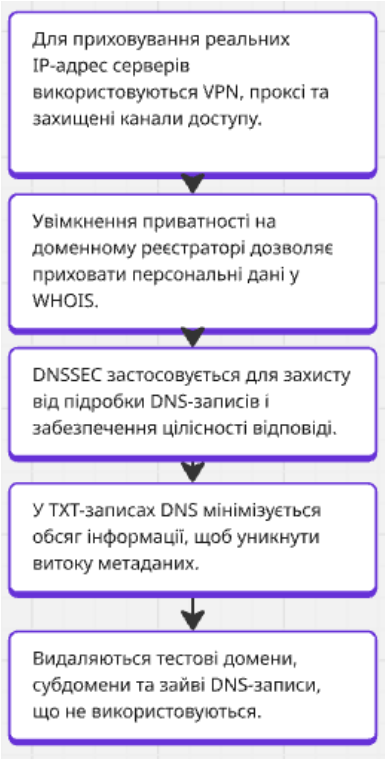

Рисунок 3.4. Блок-схема четвертого етапу створеного методу.

Етап 5. Політика безпеки та навчання персоналу

Формуються вимоги до роботи персоналу в політиці безпеки, проводяться інструктажі та тренінги персоналу.

На цьому етапі здійснюється:

1. Розробка, впровадження, покращення політики ІБ компанії, яка регламентує правила роботи користувачів; їх взаємодію з соц. мережами; зберігання та обробку документів.
2. Проводяться регулярні навчання та тренінги працівників з кібербезпеки, реагування на фішинг, атаки соц. інженерії.
3. Створюються шаблони (сценарії) безпечної поведінки - правила щодо публікації даних у відкритій мережі та у соц. мережах, участі у конференціях.
4. Регулярне тестування персоналу з інформаційної гігієни.

Результатом впровадження таких дій є підвищення обізнаності персоналу у сфері ІБ. Створені правил публікації даних, файлів в відкриту мережі у політиці безпеки.

На схемі наведена блок-схема п’ятого етапу створеного методу (рис. 3.5).

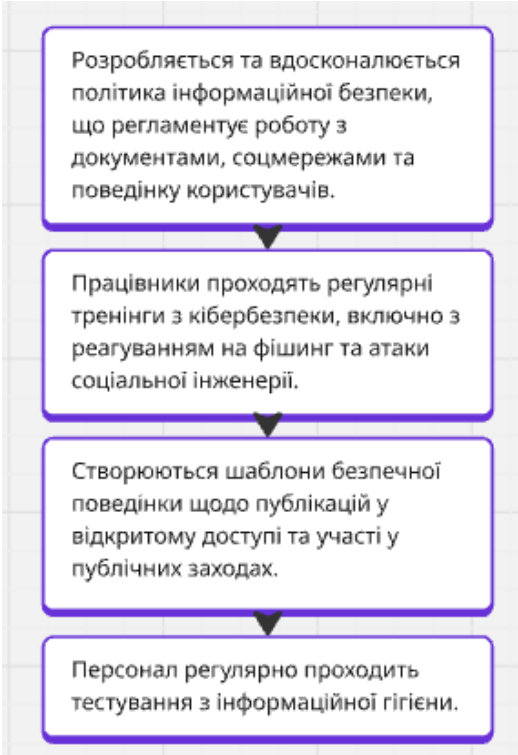

Рисунок 3.5. Блок-схема п’ятого етапу створеного методу.

Етап 6. Постійний моніторинг відкритих джерел

Пасивного захисту зазвичай недостатньо - потрібно регулярно перевіряти інформацію про компанію у відкритих джерелах.

На цьому етапі здійснюється:

1. Автоматизований моніторинг згадок про компанію через сервіси Google Alerts, Mention, Brand24.
2. Пошук та аналіз (здебільшого теж автоматизовано) витоків баз даних, злитих даних (HaveIBeenPwned, IntelligenceX).
3. Перевірка платформ Pastebin, Telegram-каналів та інших на наявність інформації про компанію (логині, паролі, IP-адреси, вразливості).
4. Використання спеціального ПЗ (SpiderFoot, Recon-ng, DarkSearch.io), що полегшує пошук даних.

Мета цього етапу - отримувати регулярне представлення про наявність даних організації в відкритій мережі [35].

На схемі наведена блок-схема шостого етапу створеного методу (рис. 3.6).

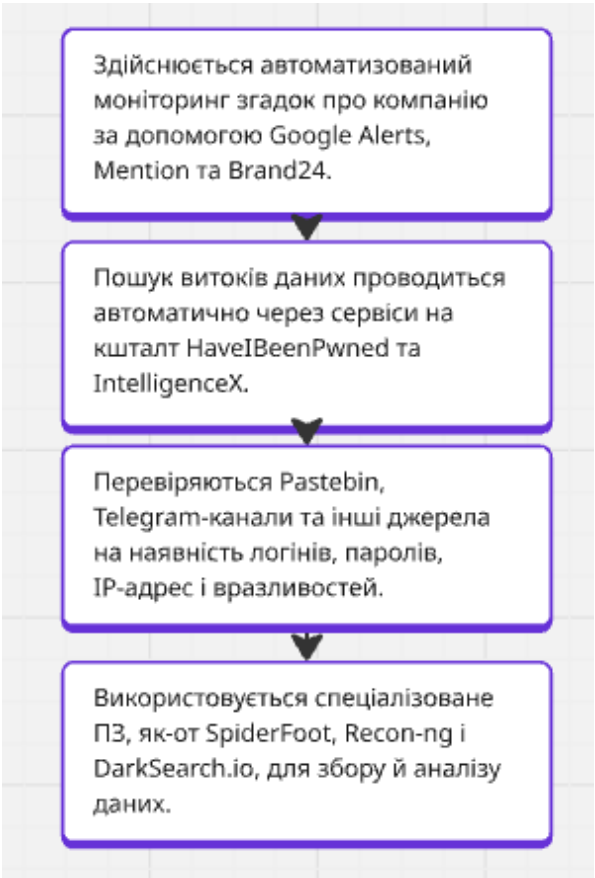

Рисунок 3.6. Блок-схема шостого етапу створеного методу.

Етап 7. Реагування та вдосконалення

На цьому етапі потрібно продумати реагування на ідентифіковані загрози; постійно вдосконалювати план реагування на інциденти ІБ.

На цьому етапі здійснюється:

1. Розробка плану реагування на визначені інциденти ІБ.
2. Використання отриманих даних для аналізу інцидентів, побудови профілів атак.
3. Регулярне оновлення політики безпеки і засобів захисту на основі нових даних.
4. Інтеграція отриманих даних з відділом SOC, SIEM, SOAR системами.

В результаті отримуємо план дій для протидії кібератакам з використанням OSINT технологій, план реагування на інциденти ІБ, можливості для подальшого розвитку.

На схемі наведена блок-схема сьомого етапу створеного методу (рис. 3.7).

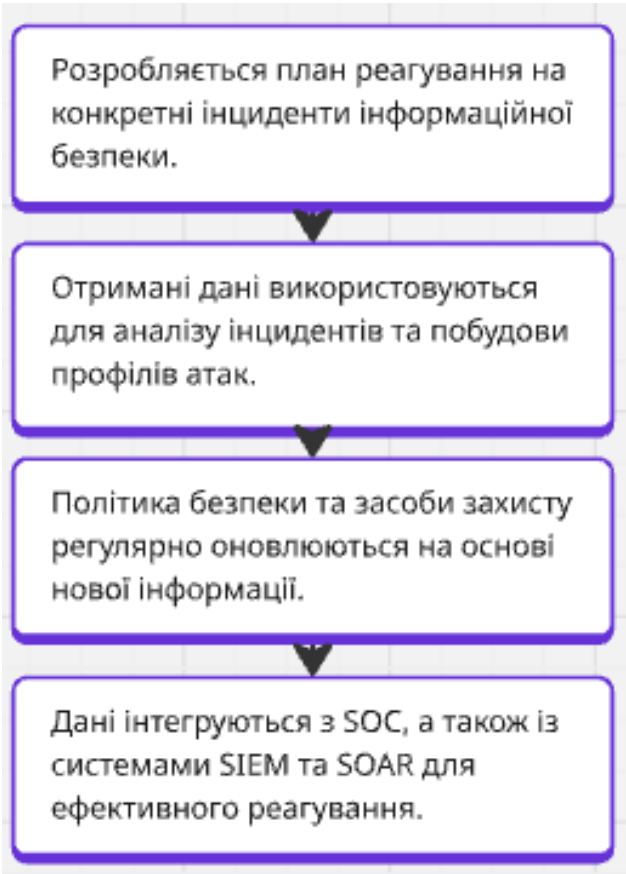

Рисунок 3.7. Блок-схема сьомого етапу створеного методу.

На схемі представлена блок-схема методу протидії кібератакам з використанням OSINT-технологій (рис. 3.8).

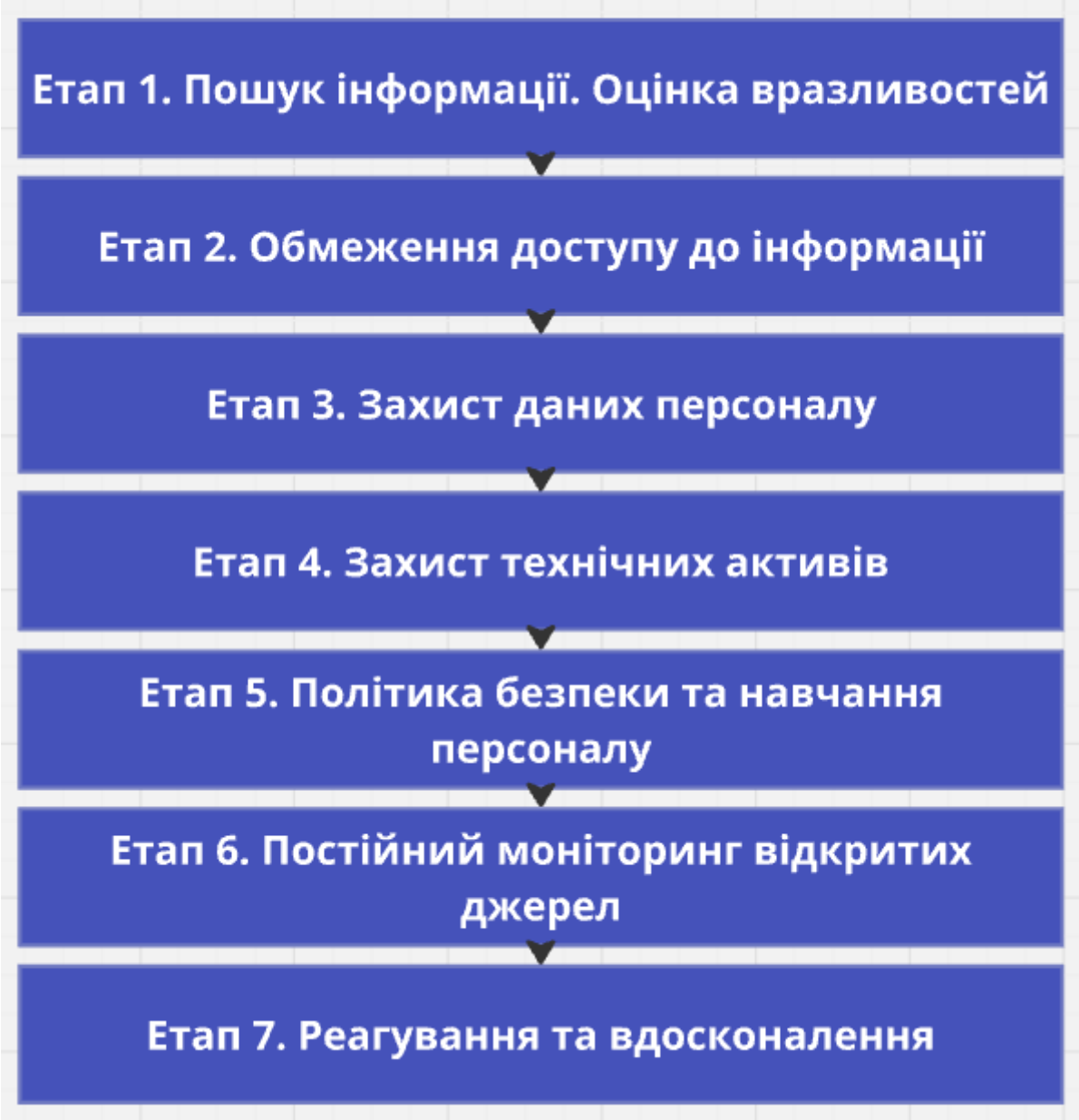

Рисунок 3.8. Блок-схема методу протидії кібератакам з використанням OSINT-технологій.

Використання визначених програм та сервісів на основі створеного методу показано у Додатку А.

Висновок за розділом 2

В рамках другого розділу було визначено та проаналізовано основні заходи протидії кібератакам з використанням OSINT-технологій. Були визначені основні типи вразливостей, характерних для сучасних організацій, включаючи надмірну відкритість технічної інфраструктури, витік корпоративних даних та оприлюднення особистої інформації співробітників у відкритому доступі. Аналіз існуючих підходів до протидії таким загрозам дозволив виділити фундаментальні практики, які виявилися ефективними в умовах зростаючої цифрової відкритості.

На основі отриманих висновків було розроблено метод протидії атакам на основі OSINT. Цей метод побудований на комплексному підході та передбачає інтеграцію технічних, організаційних та поведінкових заходів. Він складається з семи логічно пов'язаних між собою етапів: пошук інформації та оцінка вразливостей, обмеження доступу до конфіденційних даних, захист персоналу, захист технічних активів, впровадження політик безпеки та навчання, постійний моніторинг відкритих джерел та реагування на виявлені загрози.

Кожен етап методу спрямований на зменшення привабливості організації як цілі для зловмисників, що використовують інструменти OSINT. Особлива увага приділяється мінімізації цифрового сліду компанії, обмеженню публічних профілів співробітників, захисту доменів, даних WHOIS та постійному моніторингу даркнету та публічних джерел. Ці дії значно зменшують ризики, пов'язані із соціальним інжинірингом, фішингом та цілеспрямованими атаками.

Таким чином, розділ 2 підтверджує актуальність застосування комплексного підходу до захисту організацій від загроз OSINT, що поєднує як класичні заходи захисту, так і сучасні методи виявлення ризиків за допомогою відкритої інформації. Запропонований метод може бути ефективно впроваджений у корпоративному середовищі для підвищення загальної кіберстійкості та забезпечення цифрової безпеки на етапі, що передує атаці.

РОЗДІЛ 3
ПОРІВНЯЛЬНИЙ АНАЛІЗ ТА ОЦІНКА ЕФЕКТИВНОСТІ СТВОРЕНОГО МЕТОДУ ПРОТИДІЇ КІБЕРАТАКАМ З ВИКОРИСТАННЯМ OSINT-ТЕХНОЛОГІЙ

3.1 Аналіз існуючих методів протидії кібератакам з використанням OSINT-технологій

Threat Intelligence Platforms (TIPs)

Threat Intelligence Platforms — платформи для проактивного пошуку загроз. Ціль їх використання – пошук, збір та фільтрація даних з відкритих джерел про актуальні загрози. Поширення IoC (індикатори компрометації) для детектування загроз.

Можливі інструменти: MISP, IBM X-Force, Recorded Future, ThreatConnect та інші.

Особливості

Такі платформи можуть бути інтегровані в інфраструктурні рішення компанії (SIEM/SOAR) системи, а робота щодо виявлення загроз може бути автоматизованою. Ключовою перевагою використання таким систем є швидке визначення та передача індикаторів компрометації, кореляція даних з внутрішніми логами компанії.

Щодо переваг використання таких систем — робота у пулі реальних загроз для конкретної компанії (фільтрація). Поширення актуальних IoC. Швидке реагування на загрози на основі таких даних.

Із мінусів, можна визначити складність налаштування TIPs для конкретної інфраструктури організації. Високу коштовність таких рішень.

Пасивний OSINT-моніторинг

Метод полягає у систематичному моніторингу інформації про компанії у відкритій мережі. Пошуку підлягає інформація про компанію, співробітників,

структуру підприємства, мережі. Далі, аналізуються загрози, які залежать від знайденої інформації.

Можливі інструменти: Shodan, Google Dorks, Maltego, Social Searcher.

Особливості

Можливо виявити та реагувати на загрози до здійснення атаки. Можна знайти широкий спектр даних — від згадок про компанію на відкритих форумах, до зливу баз даних на спеціалізованих сайтах (Pastebin, Ghostbin, файлообмінники). Для збору даних потрібна людина, яка використовує автоматизовані інструменти для пошуку даних та самотужки аналізує результати. Такі дії називаються пасивним OSINT`ом, їх неможливо викрити.

З переваг можна виділити "безкоштовність" пошуку — Shodan, Google Dorks, Social Searcher – повністю безкоштовні сервіси. В Maltego є платний тариф, але безкоштовного достатньо. Такий пошук даних є безпечним та простим у впроваджені. Потрібно шукати конкретну інформацію з використанням конкретних правил. Для використання перелічених програмних засобів чи сервісів не потрібна серйозна технічна підготовка.

Мінуси — часто не можна повністю зрозуміти, чи достатньо таких дій (пасивного моніторингу) для ефективного захисту від атак. Можна знайти інформацію про компанію, після чого будувати модель загроз (як знайдені дані можуть бути використані для побудови плану атаки на ціль), а можна побудувати модель загроз з інформацією, яку потрібно перевіряти на відкритість. Спосіб потребує постійного моніторингу, ручної роботи. Деякі дані можуть бути упущені внаслідок "людського фактору".

Red Team OSINT Assessment

Послуга замовляється в Red Team. Метою є проведення OSINT-дослідження компанії. Пошук та аналіз наявних даних. Побудови модель загроз на основі знайдених даних; моделювання реальних атак.

Команда імітує дії хакерів — використовують OSINT-інструменти для пошуку даних для атак.

Інструменти: SpiderFoot, Recon-ng, TheHarvester, LinkedIn Scraping та інші. Широкий пул ПЗ.

Особливості

Такий метод дозволяє моделювати реальні хакерські атаки на основі проведеного OSINT-дослідження. Можуть бути використані як технічні навички команди для отримання інформації, так і соціальний вплив (фішинг, соц. інженерія та інші). Можна виявити нестандарті (непередбачувані) шляхи проникнення. Звіт дозволяє зрозуміти, як думає хакер, що шукає, на що орієнтується. Які вектори бачить при аналізі даних.

Переваги - дуже точний та детальний аналіз, бо його робить професійна Red Team (червона команда), яка спеціалізується на хакінгу. Можливість знайти конкретні вразливості та слабкі місця в системі, критичні дані в відкритій мережі.

Недоліки - Такі OSINT-дослідження є одноразовими (нерегулярними) та дуже коштовними. Також, для розуміння та аналізу отриманого звіту, краще мати досвід в роботі Red Team чи додатково консультуватися, як реагувати на виявлені загрози.

Human Risk Intelligence (Аналіз цифрової відкритості персоналу)

Метод полягає у дослідження відкритості персоналу до атак соціальної інженерії на основі відкритих даних в мережі.

Інструменти: Maltego, Google Dorks, соц. мережі.

Особливості

Аналізуються дані про співробітників в мережі. Наскільки важко їх отримати та що взагалі можна отримати. Формуються ризик-профілі для "потрібних, важливих" працівників. Фокус на директорів, керівників відділів (наприклад IT-відділ) для проведення атак типу spear phishing. В пріоритеті інформація про соціальні зв'язки співробітників, їх вразливості, інтереси. Після проведення дослідження можливий реальний тест працівників на протистояння атакам соц. інженерії.

Переваги — посилюється пильність працівників. Можна конкретно визначати ціль, збирати інформацію, тренувати її. Визначення слабких місць

цілі, донесення можливих векторів атак. Створення прикладів можливих атак та тренування на протидію таким.

Недоліки — не є комплексною послугу. Спрямовано саме на роботу з працівниками. Важко зробити для всіх працівників - потрібно багато часу, велика команда, багато зусиль. Обирається чітко визначений пул осіб, які з більшою ймовірністю цікавлять зловмисників.

Інтеграція OSINT-даних у SOC, SIEM, SOAR системи

Схожий до першого з проаналізованих методів, але тут інтегруються дані, зібрані різними шляхами, у внутрішню систему безпеки компанії. Це дає змогу автоматизовано виявляти на загрози, планувати стратегію реагування завчасно.

Інструменти: Splunk, IBM QRadar, Google Chronicles (SOAR) та інші.

Особливості

Метод дозволяє інтегрувати знайдені дані як тригер для автоматичної відповіді. Дані корелюються з внутрішньо зібраними логами в системі. Можливо автоматично отримувати сповіщення про сканування IP, використання певних даних для входу (пара email:password), пошук IoC в листах на пошті та інші. Найголовніше - створюються playbooks (сценарії реагування на згрози).

Переваги — інтеграція даних в безпекову систему компанії дозволяє швидко реагувати на конкретно проаналізовані загрози. Можливо масштабування взаємодії — використання платних сервісів для автоматизованого знаходження даних.

Недоліки — складно інтегрувати великий обсяг даних для різних систем - від SIEM та SOAR до використання SOC-аналітиками. Високі вимоги до працівників - технічне розуміння, можливості роботи з великими обсягами даних. Коштовне використання - від збору даних до їх збереження.

Моніторинг публічної IT-інфраструктури

Один із найлегших перелічених методів. Суть — використання автоматизованих та часто безкоштовних (чи обмежено безкоштовних) сервісів для детектування неправильно налаштованих серверів, відкритих портів (чи серверів), застарілих протоколів в інфраструктурі компанії.

Інструменти: Shodan, Censys, Zoomeye, SSLMate.

Особливості

Отримання інформації про систему у реальному часі або з дуже маленьким інтервалом оновлення. Такий спосіб є ефективним, тому що він імітує дії хакерів. Проводиться розвідка технічних засобів компанії та аналізуються способи атаки на останні. Можна виявляти небезпечні протоколи (FTP, RDP) та інші.

Переваги — використання перелічених сервісів або їх аналогів є безкоштовним. Підхід є проактивним (шукаються не загрози, а вразливості системи).

Недоліки — обмеження в деталізації. Не завжди зрозуміло, яким числом датується перелічена інформація. Потрібна висока технічна підготовка спеціаліста для розуміння, що він взагалі шукає і як це може бути використано зловмисниками. Спосіб є ефективним при умові, що дані, які повинні постійно оновлюватися - постійно моніторяться.

3.2 Критерії оцінки ефективності методів протидії кібератакам з використанням OSINT-технологій

Критерії оцінки ефективності запропонованого методу протидії кібератакам з використанням OSINT-технологій були поділені на 2 групи - технічні характеристики (комплексність захисту, складність реалізації, захист публічної інфраструктури, які вразливості можна знайти) та організаційні, практичні аспекти (витрати на впровадження, вплив на людский фактор, безперервність моніторингу, масштабованість рішення).

Технічні характеристики

Комплексність підходу

Критерій визначає, чи застосовується метод комплексно до системи (враховує різноманітні параметри безпеки) — від технічних до організаційних. Включає порівняння різних інструментів та практик для досягнення комплексного та ефективного захисту системи.

Складність реалізації

Оцінюється складність впровадження методу в реальну систему — необхідність залучення кваліфікованих спеціалістів, складність інтеграції з існуючими системами, технічні та організаційні проблеми.

Захист публічної інфраструктури

Оцінюється, чи впливає метод на захист публічної інфраструктури (сервери, сайти, мережеві ресурси), які знаходяться у відкритому доступі.

На які вразливості орієнтований

Критерій визначає, які вразливості можуть бути знайдені при використанні методу, наприклад — технічні (відкритий доступ, порти, вразливе ПЗ), людські (атаки соц. інженерії) тощо.

Організаційні та практичні аспекти

Витрати на провадження

Критерій оцінює витрати, необхідні для початкової реалізації і підтримки стабільної роботи обраного методу: фінансові затрати, час, технології та людські ресурси. Наприклад — витрати на програмне та апаратне забезпечення, налаштування інфраструктури, навчання персоналу. Методи з низькою вартістю впровадження можуть бути застосовані швидше та простіше, аніж дорогі, на які потрібно більше коштів.

Вплив на людський фактор

Оцінюється, чи впливає метод на поведінку працівників компанії в контексті інформаційної гігієни. Чи змінюється рівень навчання та обізнаності персоналу, зміни в роботі, чи підвищується рівень інформаційної гігієни.

Безперервність моніторингу

Параметр визначає, чи можна застосовувати обраний метод для безперервного моніторингу — стабільний контроль за відкритими джерелами інформації та потенційними загрозами. За допомогою безперервного моніторингу можна швидко знаходити нові ризики та оперативно реагувати на них.

Масштабованість рішення

Критерій визначає, наскільки обране рішення може бути розширене для захисту великих (розподілених) корпоративних систем. Масштабованість повинна охоплювати максимально велику кількість даних, інфраструктури без значного зростання вартості впровадження рішення чи втрати ефективності.

3.3 Порівняльна таблиця запропонованого методу з альтернативними підходами

Для обґрунтування вибору методу протидії кібератакам доцільно провести порівняльний аналіз технічних характеристик існуючих підходів. Технічні характеристики методів протидії кібератак з використанням OSINT-технологій показані в табл. 3.1.

Таблиця 3.1

Технічні характеристики методів протидії кібератак з використанням OSINT-технологій

Метод	**Комплексність підходу**	**Складність реалізації**	**Захист публічної інфраструктури**	**На які вразливості орінєтований**
Створений метод	Висока	Помірна–висока	Так	OSINT, соц. інженерія, технічні
Threat Intelligence Platforms (TIPs)	Помірна	Висока	Частково	Загрози, zero-day

Продовження табл. 3.1

Пасивний OSINT-моніторинг	Низька	Низька	Ні	Витоки, відкриті дані
Red Team OSINT Assessment	Висока	Висока	Ні	Технічні, людські
Human Risk Intelligence (Аналіз цифрової відкритості персоналу)	Помірна	Помірна	Так	Людський фактор
Інтеграція OSINT-даних у SOC, SIEM, SOAR системи	Висока	Висока	Так	Комплексні загрози
Моніторинг публічної IT-інфраструктури	Помірна	Помірна	Так	Технічні вразливості

Створений метод

Комплексність підходу — висока. Включає 7 етапів — пошук інформації та аналіз вразливостей; контроль доступу; навчання персоналу, технічний захист, моніторинг та реагування.

Складність реалізації — помірна чи висока. Включає як організаційні, так і технічні процеси. Тому складність може бути як помірною, так і високою.

Захист публічної інфраструктури — присутній. Рекомендується використання VPN, DNSSEC, обмеження доступу тощо.

На які вразливості орієнтований — вразливості, знайдені у відкритих джерелах - технічні вразливості мережі та обладнання, соц. інженерія.

Threat Intelligence Platforms (TIPs)

Комплексність підходу — помірна. Автоматизований збір та аналіз загроз з різних джерел.

Складність реалізації — висока складність через інтеграцію стороннього сервісу до SIEM/SOAR систем. Робота з великою кількістю даних.

Захист публічної інфраструктури — захист публічної інфраструктури може бути тільки в контексті виявлення загроз.

На які вразливості орієнтований — відомі загрози, zero-day вразливості.

Пасивний OSINT-моніторинг

Комплексність підходу — низька. Моніторинг інформації без активного втручання, пошук потенційних загроз та витоків інформації.

Складність реалізації — низька чи помірна, здебільшого автоматизований процес.

Захист публічної інфраструктури — немає захисту, тільки пошук витоків та загроз.

На які вразливості орієнтований — витоки даних, відкриті відомості про вразливості.

Red Team OSINT Assessment

Комплексність підходу — висока. Активний аналіз вразливостей через проведення OSINT-дослідження.

Складність реалізації — висока складність. Необхідні досвідчені фахівці, симуляція атак.

Захист публічної інфраструктури — можна виявити слабкі місця, але сам по собі захист не відбувається.

На які вразливості орієнтований — вразливості в системах, людський фактор, технічні недоліки.

Human Risk Intelligence (Аналіз цифрової відкритості персоналу)

Комплексність підходу — помірна. Аналіз поведінки співробітників і приватності профілів для виявлення ризиків.

Складність реалізації ─ помірна, потрібен доступ до соц. мереж. Аналіз великого обсягу даних.

Захист публічної інфраструктури — можливий захист через зниження ризику атак, які основані на соц. інженерії.

На які вразливості орієнтований — атаки соц. інженерії, виток інформації в мережу.

Інтеграція OSINT-даних у SOC, SIEM, SOAR системи

Комплексність підходу — висока. Інтеграція даних в автоматизовані системи безпеки для швидкого реагування на інциденти.

Складність реалізації — висока. Потребує інтеграції різних систем, автоматизації за обробки великого обсягу даних.

Захист публічної інфраструктури — проактивний захист, швидке реагування на інциденти.

На які вразливості орієнтований — атаки на інфраструктуру, інциденти безпеки. Технічні атаки.

Моніторинг публічної IT-інфраструктури

Комплексність підходу — помірна. Постійне відстеження інформації про систему в публічних сервісах.

Складність реалізації — помірна. Потрібно налаштувати інструменти моніторингу.

Захист публічної інфраструктури — захист публічної інфраструктури через аналіз вразливостей у мережі.

На які вразливості орієнтований — технічні вразливості — відкриті порти, DDoS атаки, вразливості ПЗ.

Організаційні та практичні аспекти застосування різних методів OSINT-аналізу значною мірою впливають на вибір оптимального рішення для

конкретної компанії. Організаційні та практичні аспекти методів протидії кібератак з використанням OSINT-технологій показані в табл. 3.2.

Таблиця 3.2

Організаційні та практичні аспекти методів протидії кібератак з використанням OSINT-технологій

Метод	**Витрати на впровадження**	**Вплив на людський фактор**	**Безперервність моніторингу**	**Масштабованість рішення**
Створений метод	Помірні	Високий	Постійний	Висока
Threat Intelligence Platforms (TIPs)	Високі	Середній	Безперервний	Висока
Пасивний OSINT-моніторинг	Низькі	Мінімальний	Постійний	Висока
Red Team OSINT Assessment	Високі	Високий	Нерегулярний	Низька
Моніторинг публічної IT-інфраструктури	Помірні	Низький	Постійний	Помірна
Інтеграція OSINT-даних у SOC, SIEM, SOAR системи	Високі	Середній	Безперервний	Висока

Продовження табл 3.2.

Human Risk Intelligence (Аналіз цифрової відкритості персоналу)	Помірні	Дуже високий	Постійний	Помірна

Створений метод

Витрати на впровадження — помірні. Передбачається використання доступних інструментів, потрібна раціональна побудова процесів.

Вплив на людський фактор — високий. Активна участь персоналу у навчанні, тренінги з ІБ, дотримання політики безпеки.

Безперервність моніторингу — постійний. Систематичне спостереження за відкритими джерелами та подіями.

Масштабованість рішення — висока. Можливо адаптувати до будь-якої організації, гнучка структура.

Threat Intelligence Platforms (TIPs)

Витрати на впровадження — високі. Потрібно закупити рішення, оновлювати підписку, інтегрувати з іншими системами.

Вплив на людський фактор — середній. Команда залучена здебільшого для інтерпретації результатів та отримання даних про технічні вразливості.

Безперервність моніторингу — безперервний. Дані постійно оновлюються, автоматизоване рішення.

Масштабованість рішення — висока масштабованість. Підтримка аналізу великого обсягу даних.

Пасивний OSINT-моніторинг

Витрати на впровадження — низькі витрати. Робота з відкритими даними і безкоштовними інструментами.

Вплив на людський фактор — мінімальний вплив. Тільки пошук та збір даних, може бути автоматизованим.

Безперервність моніторингу — постійний. Реалізація через налаштування автоматичного моніторингу.

Масштабованість рішення — висока. Легко масштабувати.

Red Team OSINT Assessment

Витрати на впровадження — високі. Потрібна команда кваліфікованих спеціалістів.

Вплив на людський фактор — високі. Взаємодія з персоналом, тестування атак соц. інженерії.

Безперервність моніторингу — нерегулярний. Послуга проводиться нерегулярно (наприклад раз на квартал).

Масштабованість рішення — низька. Складно адаптувати до постійного використання та у великих масштабах.

Human Risk Intelligence (Аналіз цифрової відкритості персоналу)

Витрати на впровадження — помірні. Інструменти для аналізу соц. мереж і поведінки можуть бути безкоштовними, але для обсягу компаній потрібно PRO-версії. Також потрібне налаштування.

Вплив на людський фактор — високий. Робітники та їх профілі постійно оцінюються на предмет відкритості інформації та її змісту.

Безперервність моніторингу — постійний чи регулярний. Контроль за публікаціями, витоками даних.

Масштабованість рішення — помірна. Залежить від розміну колективу і доступності даних.

Інтеграція OSINT-даних у SOC, SIEM, SOAR системи

Витрати на впровадження — високі. Потрібна технічна інтеграція, автоматизація та багато технічних ресурсів.

Вплив на людський фактор — середній. Фокус на технічних атаках, працює технічний персонал. Мінімальний контакт з іншими співробітниками.

Безперервність моніторингу — безперервний. Інтеграція та автоматизація в системи реагування та моніторингу.

Масштабованість рішення — висока. Такі рішення легко масштабуються (але слід пам'ятати про складність).

Моніторинг публічної IT-інфраструктури

Витрати на впровадження — помірні. Використовуються сканери, відкриті сервіси.

Вплив на людський фактор — низький. Потребує участі і роботи лише технічного персоналу.

Безперервність моніторингу — постійний або регулярний. Постійно скануються доступні компоненти.

Масштабованість рішення — помірна. Зростає складність при масштабуванні рішення.

Таким чином, запропонований метод демонструє високий рівень комплексності при збереженні помірної складності впровадження. Він ефективно захищає інфраструктуру публічної інформації від кібератак, усуваючи як технічні вразливості, так і загрози, пов'язані із соц. інженерією. Метод є економічно ефективним, має значний вплив на людський фактор завдяки підвищенню обізнаності з питань кібербезпеки, забезпечує постійний моніторинг відкритих джерел і легко масштабується. Ці характеристики відрізняють його від існуючих підходів і роблять його практичним та ефективним рішенням для впровадження в корпоративному середовищі.

Висновки за розділом 3

У третьому розділі було проведено детальний порівняльний аналіз між запропонованим методом протидії кібератакам з використанням технологій OSINT та існуючими підходами, що застосовуються на даний час у практиці кібербезпеки. Були розглянуті як технічні, так і організаційні аспекти ефективності, що дозволило об'єктивно оцінити сильні та слабкі сторони

кожного методу. Порівняння проводилося на основі таких критеріїв, як комплексність підходу, складність впровадження, захист громадської інфраструктури, фокус на вразливості, витрати на впровадження, вплив на людський фактор, безперервність моніторингу та масштабованість.

Запропонований метод демонструє високий рівень балансу між складністю впровадження та ефективністю. На відміну від більшості альтернативних рішень, він передбачає не тільки виявлення вразливостей, але й формування комплексної стратегії протидії — від організаційних заходів до технічних відповідей. Метод спрямований як на технічні вразливості, так і на загрози соціальної інженерії, що забезпечує багаторівневий захист корпоративного середовища.

У порівнянні з такими підходами, як пасивний моніторинг OSINT або оцінки від Red Team OSINT, розроблений метод виявився більш стійким з точки зору довгострокового моніторингу та масштабованості. Водночас він не вимагає надмірно високих фінансових або кадрових витрат, на відміну від платформ Threat Intelligence Platforms (TIP) або інтегрованих систем на базі SOC/SIEM/SOAR. Крім того, підхід активно залучає людський фактор через навчання персоналу та формування культури інформаційної безпеки, що є особливо актуальним для запобігання атакам на основі соціальної інженерії.

Варто підкреслити, що розроблений метод приділяє особливу увагу захисту публічної інфраструктури — одного з найбільш вразливих сегментів у сучасному середовищі. Впровадження таких політик, як використання VPN, DNSSEC та обмежений доступ до критичних ресурсів, значно зменшує ризики, пов'язані з відкритим доступом до мережевих послуг. Завдяки багатокомпонентній структурі та адаптивності до організацій різного розміру, метод може застосовуватися як в установах державного сектору, так і в приватних підприємствах.

Таким чином, на основі проведеного аналізу можна зробити висновок, що запропонований метод не тільки ефективно інтегрує можливості інструментів OSINT в системи кібербезпеки, але й створює практичний і

універсальний підхід, здатний підвищити кіберстійкість організації в динамічному середовищі загроз.

ВИСНОВКИ

Головною метою цієї дипломної роботи було розроблення ефективного методу протидії кібератакам із використанням технологій OSINT. Протягом дослідження було проведено комплексний аналіз OSINT як інструменту для збору інформації, моделювання загроз та методів кібератак. На основі цього було створено новий метод для зменшення ризиків, пов'язаних із кіберзагрозами на основі OSINT, з акцентом на захист корпоративних даних, особистої інформації співробітників та критичної інфраструктури.

Розроблений метод поєднує технічні та організаційні заходи, включаючи обмеження доступу до конфіденційних даних, використання анонімізації, безпечне управління доменами та постійний моніторинг відкритих джерел на предмет потенційних загроз. Крім того, цей підхід підкреслює важливість людського фактора шляхом впровадження політик безпеки та навчання персоналу, що підвищує загальну стійкість систем.

Було проведено порівняльний аналіз для оцінки ефективності запропонованого методу порівняно з існуючими рішеннями. Цей аналіз продемонстрував, що розроблений метод забезпечує збалансований та масштабований підхід, пропонуючи надійний захист при збереженні розумної складності впровадження та вимог до ресурсів. На відміну від деяких альтернатив, він особливо підходить для довгострокового моніторингу та адаптивного реагування на кіберзагрози, що постійно еволюціонують.

У висновку, дослідження успішно досягло своєї мети, розробивши та перевіривши практичний, комплексний метод протидії на основі OSINT. Цей метод може бути ефективно застосований як у державному, так і в приватному секторах для посилення кібербезпеки в умовах швидко мінливого ландшафту загроз.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Open Source Intelligence 101: From Novice to Expert. — Independently published, 2021. — 200 с.
2. Lloyd J., Wilcox A. Techniques and Tools for OSINT-Based Threat Analysis. — Apress, 2022. — 250 с.
3. Коваль Д., Браіловський М. Метод протидії кібератакам з використанням OSINT-технологій в корпоративній середі // Проблеми кібербезпеки інформаційно-комунікаційних систем (PCSICS): зб. матеріалів доп. та тез VIII Міжнар. наук.-практ. конф. (Київ, 11 квіт. 2025 р.) / редкол.: В.В. Ільченко, С.В. Толюпа, О.А. Лаптєв та ін. – Київ: Київський національний університет імені Тараса Шевченка, 2025. – С. 37–38.
4. Dixon A. The OSINT Handbook: A Practical Guide to Gathering and Analyzing Online Information. 1st ed. — Packt Publishing, 2022. — 320 с.
5. Joseph M. The OSINT Codebook: Cracking Open Source Intelligence Strategies. — Independently published, 2021. — 210 с.
6. Smith J. OSINT Techniques: Resources for Uncovering Online Information. 10th ed. — Independently published, 2023. — 400 с.
7. Wright R. Open Source Intelligence Techniques: Resources for Searching and Analyzing Online Information. — Independently published, 2020. — 450 с.
8. Akhgar B. Open Source Intelligence Investigation. — Springer Nature, 2017. — 350 с. — ISBN 3319476718.
9. Hobbs C. Open Source Intelligence in the Twenty-First Century. — Springer Nature, 2014. — 280 с. — ISBN 1137353325.
10. Layton R., Watters P. A. Automating Open Source Intelligence: Algorithms for OSINT. — Syngress, 2015. — 320 с. — ISBN 0128029161.
11. Da Costa D. T. Osint For The Staffing World!. — Independently Published, 2019. — 200 с. — ISBN 108101380X.

12. Hassan N. A., Hijazi R. Open Source Intelligence Methods and Tools. — Springer Nature, 2018. — 360 с. — ISBN 1484232135.
13. D'Agostino G. Conversations in Cyberspace. — Business Expert Press, 2019. — 250 с. — ISBN 1948976714.
14. Bertram S., Silverleaf P. The Tao of Open Source Intelligence. — IT Governance, 2015. — 230 с. — ISBN 1849287309.
15. Kubecka C. Hack The World With Osint (hackers Gonna Hack). — Chris Kubecka, 2019. — 310 с. — ISBN 0995687595.
16. Troia V. Hunting Cyber Criminals. — Wiley Professional Development, 2021. — 340 с. — ISBN 1119540992.
17. Chauhan S., Panda N. K. Hacking Web Intelligence: Open Source Intelligence and Web Reconnaissance Concepts and Techniques. — Elsevier S&T, 2015. — 350 с. — ISBN 0128018674.
18. Williams H. J., Blum I. Defining Second Generation Open Source Intelligence (OSINT) For The Defense Enterprise. — Rand Corporation, 2018. — 280 с. — ISBN 0833098837.
19. Ickler K. R., Drysdale J. Atomic Purple Teaming. — Defensive Origins LLC, 2021. — 300 с. — ISBN 9780578659794.
20. Kubecka C. Down The Rabbit Hole: An OSINT Journey. — Chris Kubecka, 2017. — 290 с. — ISBN 0995687544.
21. Carment D. Peacekeeping Intelligence. — Taylor & Francis, 2007. — 220 с. — ISBN 1134188404.
22. Black I. S., Fennelly L. J. Investigations and the Art of the Interview. — Elsevier S&T, 2021. — 330 с. — ISBN 0128226625.
23. Gupta R., Brooks H. Using Social Media For Global Security. — Wiley, 2013. — 270 с. — ISBN 1118442318.
24. OSINT Guide. URL: https://osintguide.com/ (дата звернення: 30.04.2025).
25. ITSec Group. OSINT Guide Part 1. URL: https://itsec.group/blog-post-osint-guide-part-1.html (дата звернення: 05.05.2025).

26. OSINT Framework. URL: https://osintframework.com/ (дата звернення: 08.05.2025).
27. Molfar. Useful Apps. URL: https://molfar.com/en/useful-apps (дата звернення: 14.05.2025).
28. Recorded Future. Threat Intelligence 101: OSINT Tools and Technologies. URL: https://www.recordedfuture.com/threat-intelligence-101/tools-and-technologies/osint-tools (дата звернення: 13.05.2025).
29. Talkwalker Blog. Best OSINT Tools. URL: https://www.talkwalker.com/blog/best-osint-tools (дата звернення: 29.04.2025).
30. Cyble Knowledge Hub. Top 15 OSINT Tools for Powerful Intelligence Gathering. URL: https://cyble.com/knowledge-hub/top-15-osint-tools-for-powerful-intelligence-gathering/ (дата звернення: 16.05.2025).
31. freeCodeCamp. What is Nmap and How to Use It: A Tutorial for the Greatest Scanning Tool of All Time. URL: https://www.freecodecamp.org/news/what-is-nmap-and-how-to-use-it-a-tutorial-for-the-greatest-scanning-tool-of-all-time/ (дата звернення: 07.05.2025).
32. Вікіпедія. Розвідка на основі відкритих джерел. URL: https://uk.wikipedia.org/wiki/Розвідка_на_основі_відкритих_джерел (дата звернення: 28.04.2025).
33. Molfar. Що таке OSINT у 2024: гайд від Molfar. URL: https://molfar.com/blog/shcho-take-osint-u-2024-gaid-vid-molfar (дата звернення: 03.05.2025).
34. Unite.AI. Найкращі інструменти OSINT з відкритим вихідним кодом. URL: https://www.unite.ai/uk/найкращі-інструменти-osint-з-відкритим-вихідним-кодом/ (дата звернення: 10.05.2025).
35. The Transmitted. Що таке OSINT (Open Source Intelligence) — розвідка на основі відкритих джерел. URL: https://thetransmitted.com/adlucem/shho-take-osint-open-source-intelligence-rozvidka-na-osnovi-vidkrytyh-dzherel/ (дата звернення: 15.05.2025).

ДОДАТКИ

Додаток А

ВИКОРИСТАННЯ ВИЗНАЧЕНИХ ПРОГРАМ ТА СЕРВІСІВ НА ОСНОВІ СТВОРЕНОГО МЕТОДУ

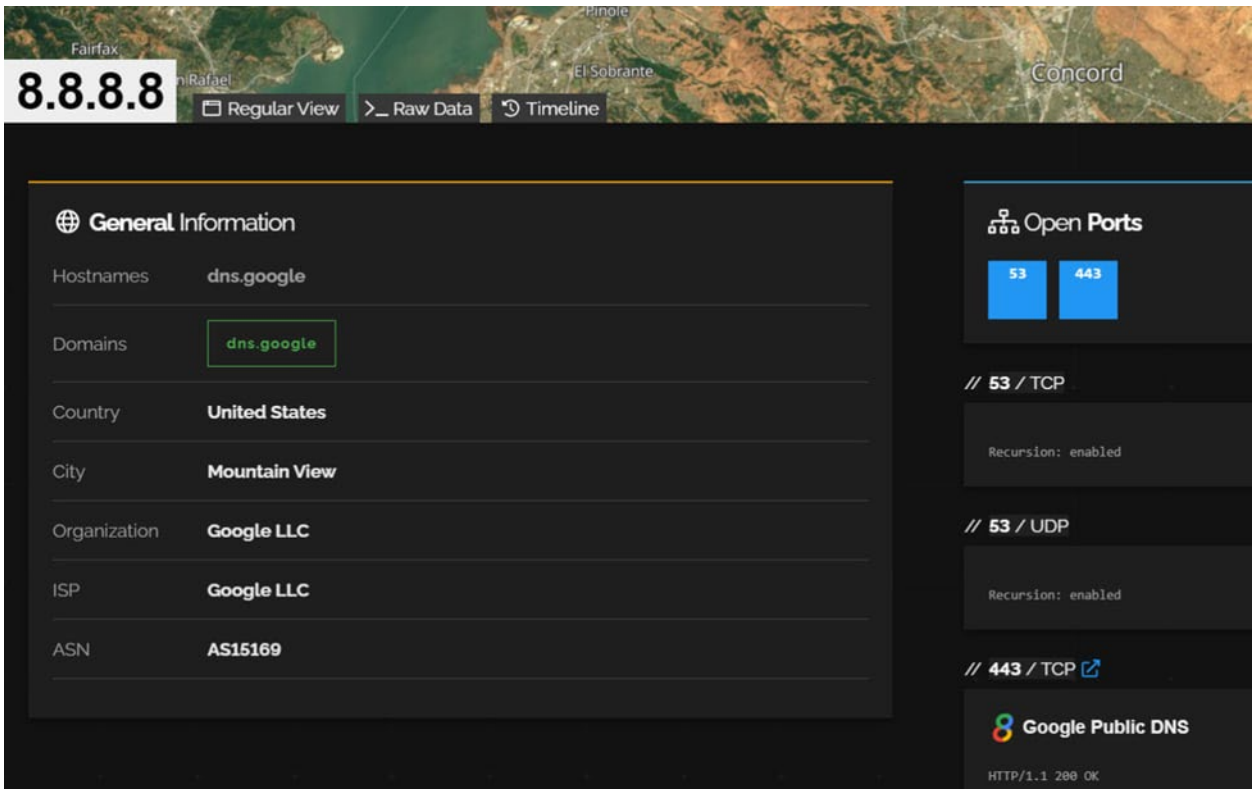

Рисунок А.1. Використання Shodan для отримання даних про мережу організації.

Продовження додатку А

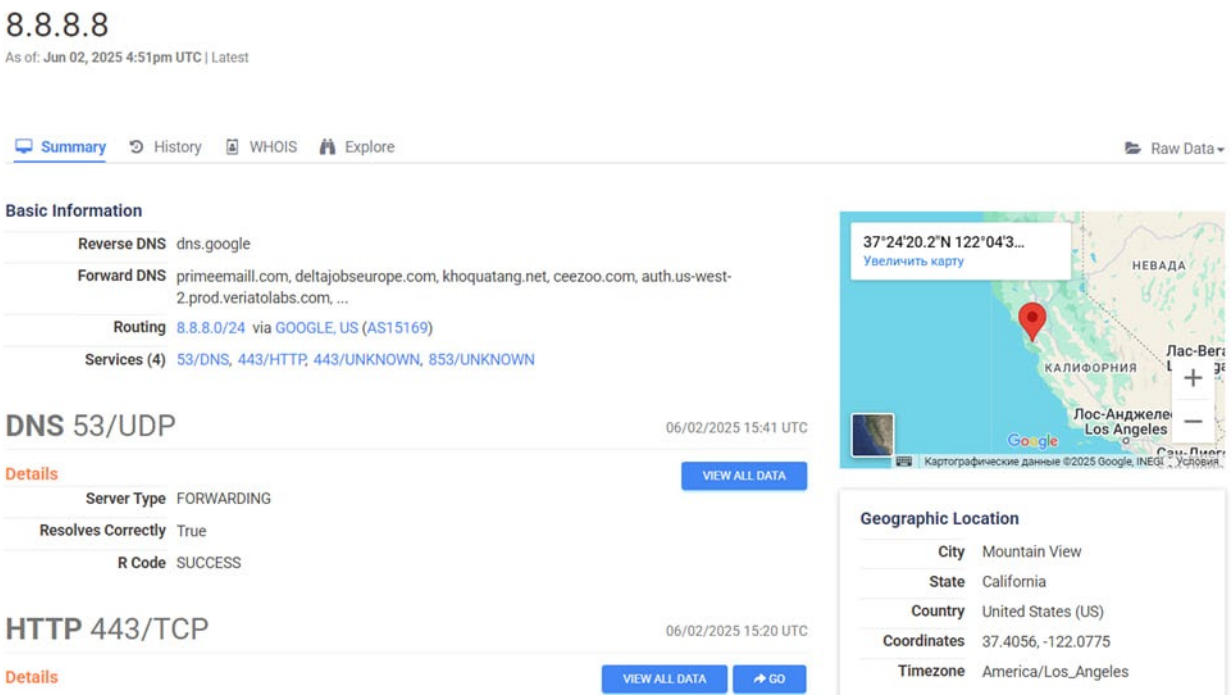

Рисунок А.2. Використання Censys для отримання даних про мережу організації.

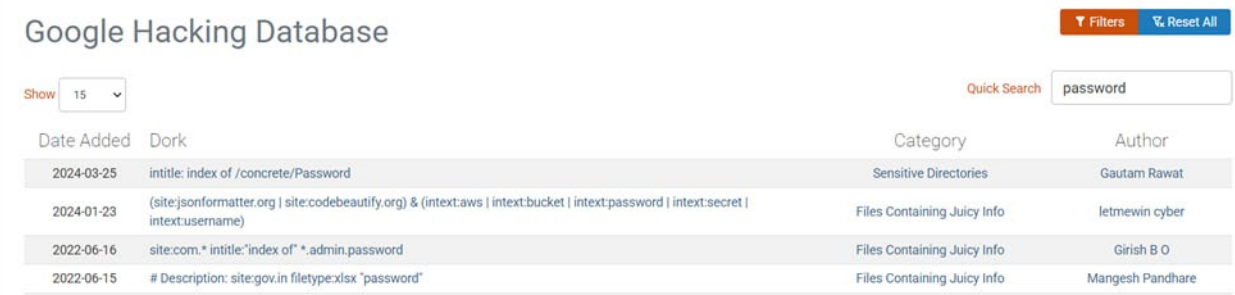

Рисунок А.3. Використання сервісу Google Hacking Database для пошуку оптимальних Google Dorks-технік.

Продовження додатку А

last_modified_by	worka
revision_number	2
create_date	2025:06:03 08:17:00Z
modify_date	2025:06:03 08:17:00Z
template	Normal
total_edit_time	0
pages	1
words	1
characters	10
application	Microsoft Office Word
doc_security	None
lines	1

Рисунок А.4. Використання EXIF-сервісів для аналізу метаданих файлів.

Продовження додатку А

Рисунок А.5. Налаштування приватності в Instagram.

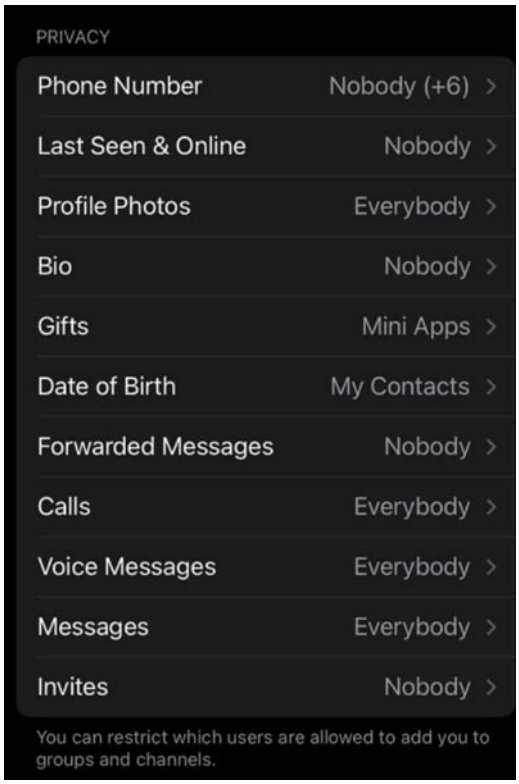

Рисунок А.6. Налаштування приватності в Telegram.

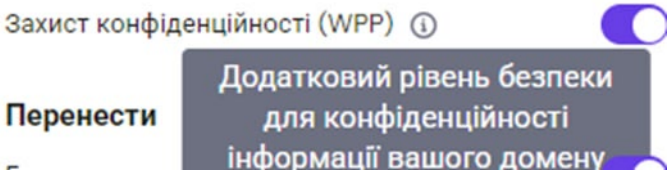

Рисунок А.7. Налаштування конфіденційності для домену.

Продовження додатку А

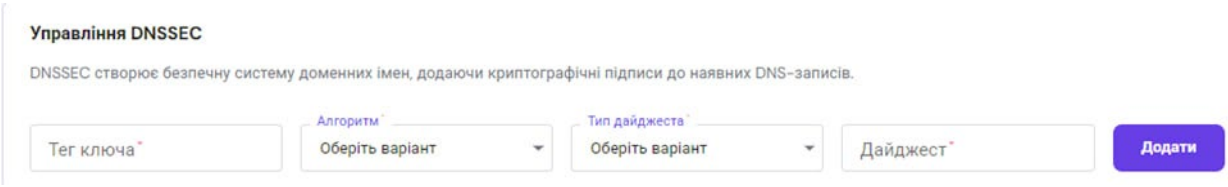

Рисунок А.8. Захист DNS через DNSSEC.

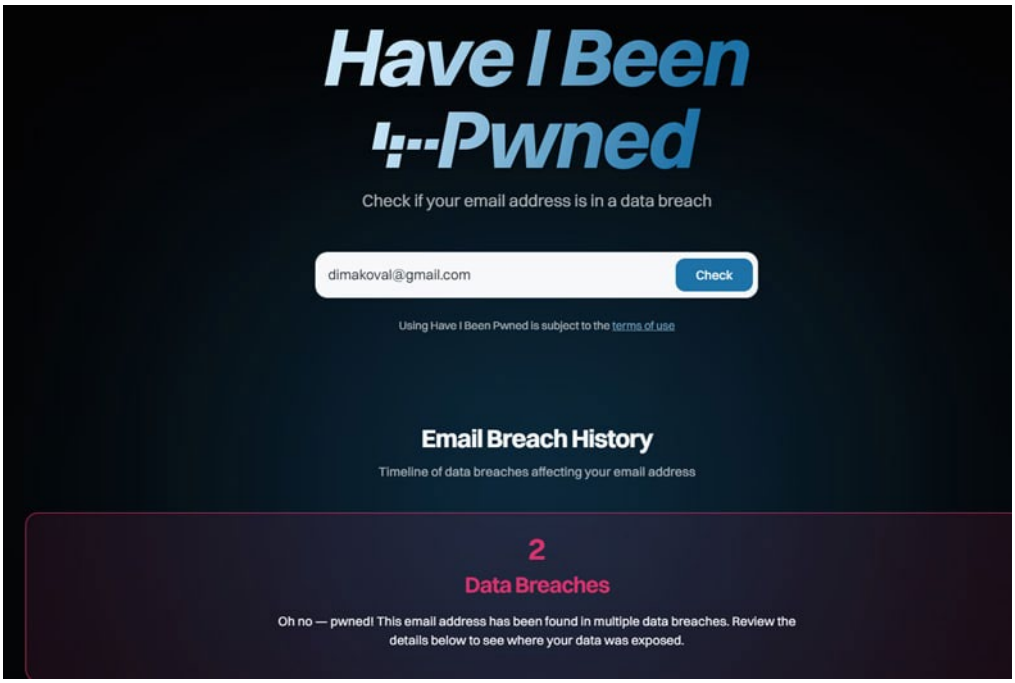

Рисунок А.9. Використання сервісу HaveIBeenPwned для перевірки наявності email у злитих базах даних.

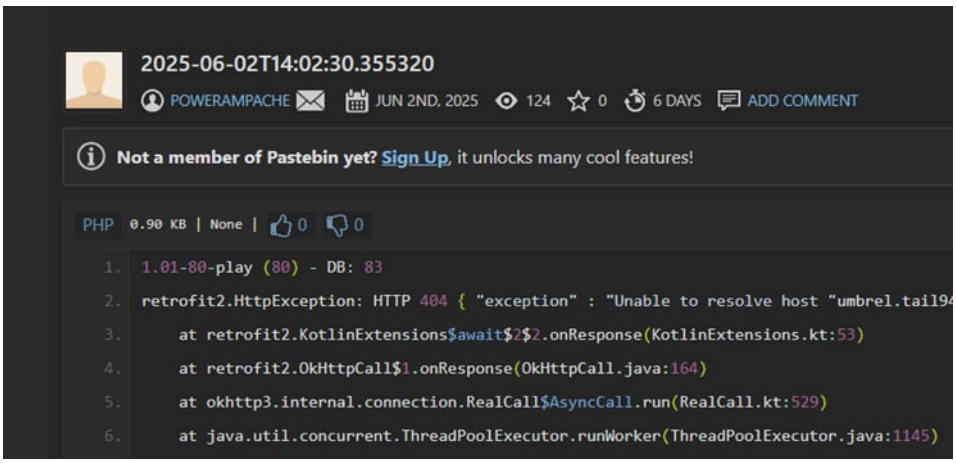

Рисунок А.10. Пошук злитих баз даних/даних у сервісі Pastebin.

Продовження додатку А

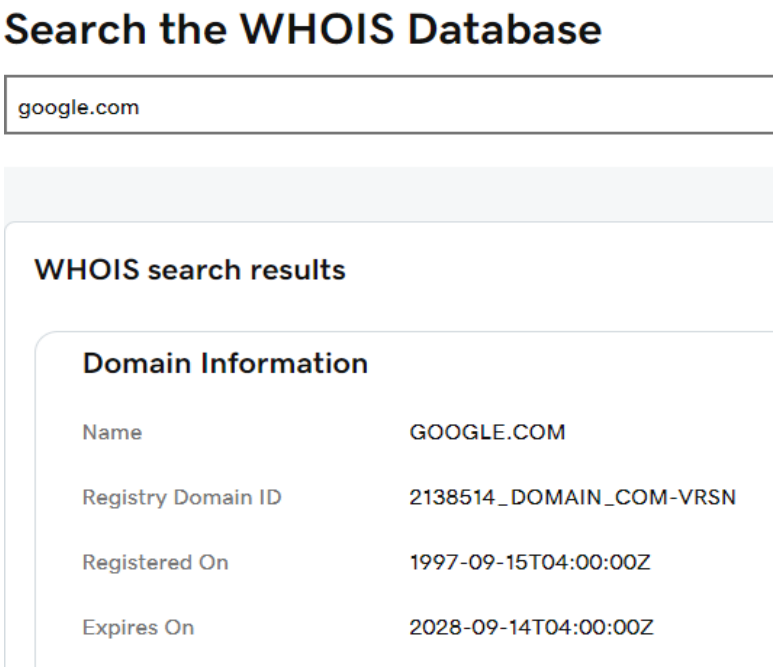

Рисунок А.11. Використання WHOIS-сервісу для отримання даних про доменне ім'я організації.