МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

**ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ**

**НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА УПРАВЛІННЯ КІБЕРБЕЗПЕКОЮ ТА ЗАХИСТОМ ІНФОРМАЦІЇ**

КВАЛІФІКАЦІЙНА РОБОТА

на тему: “МЕТОДИКА АНАЛІЗУ РИЗИКІВ ВИТОКУ ІНФОРМАЦІЇ ЧЕРЕЗ ПУБЛІЧНІ ДЖЕРЕЛА ЗА ДОПОМОГОЮ OSINT-ІНСТРУМЕНТІВ”

на здобуття освітнього ступеня бакалавра
зі спеціальності 125 Кібербезпека
освітньої програми Управління інформаційною та кібернетичною безпекою

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

_____ В’ячеслав МАТВІЄНКО
(підпис) *Ім’я, ПРІЗВИЩЕ здобувача*

Виконав(ла): здобувач вищої освіти гр. УБД-41

В’ячеслав МАТВІЄНКО
Ім’я, ПРІЗВИЩЕ

Керівник: Тетяна КАПЕЛЮШНА
Д.е.н., доцент Ім’я, ПРІЗВИЩЕ

Рецензент: Галина ГАЙДУР
Д.т.н., професор Ім’я, ПРІЗВИЩЕ

Київ 2025

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут кібербезпеки та захисту інформації

Кафедра управління кібербезпекою та захистом інформації

Ступінь вищої освіти бакалавр

Спеціальність 125 Кібербезпека

Освітня програма Управління інформаційною та кібернетичною безпекою

ЗАТВЕРДЖУЮ
Завідувач кафедри УІКБЗІ
_____Світлана ЛЕГОМІНОВА
“____”_____2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Матвієнку В’ячеславу Івановичу
(прізвище, ім’я, по батькові здобувача)

1. Тема кваліфікаційної роботи “Методика аналізу ризиків витоку інформації через публічні джерела за допомогою OSINT-інструментів”,
керівник кваліфікаційної роботи КАПЕЛЮШНА Тетяна, д.е.н., доцент
(ПРІЗВИЩЕ, Ім’я,, науковий ступінь, вчене звання)

затверджені наказом Державного університету інформаційно-комунікаційних технологій від “24“ лютого 2025 р. №56.

2. Строк подання кваліфікаційної роботи “12” травня 2025р.

3. Вихідні дані до кваліфікаційної роботи: *інформаційна безпека підприємства, методи та засоби аналізу інформації з відкритих джерел, OSINT- розвідка , наукова та технічна література.*

4. Перелік питань, які мають бути розроблені:
4.1. Дослідити OSINT-інструменти та особливості використання OSINT-інструментів для упередження від витоку інформації.
4.2. Проаналізувати ризики витоку інформації через публічні джерела за допомогою OSINT-інструментів.
4.3. Розробити методику конструювання аналізу ризиків витоку інформації через публічні джерела за допомогою OSINT-інструментів.

5. Перелік ілюстративного матеріалу: *презентація PowerPoint*

6. Дата видачі завдання “05“ березня 2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Етапи кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1.	Визначення об’єкту, предмету, мети та завдань дослідження.	17.03.2025	
2.	Збір та аналіз літератури.	24.03.2025	
3.	Дослідження OSINT-інструментів та особливостей їх використання для упередження витоків інформації.	28.03.2025	
4.	Проаналізувати ризики витоку інформації через публічні джерела за допомогою OSINT-інструментів.	11.04.2025	
5.	Розробити методику конструювання аналізу ризиків витоку інформації через публічні джерела за допомогою OSINT-інструментів.	28.04.2025	
6.	Формулювання висновків за результатами проведеного дослідження.	20.05.2025	
7.	Оформлення роботи.	22.05.2025	
8.	Оформлення презентації.	02.06.2025	
9.	Отримання рецензії на роботу.	02.06.2025	
10.	Захист в ЕК.	__.06.2025	

Здобувач вищої освіти _____ В’ячеслав МАТВІЄНКО
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Керівник
кваліфікаційної роботи _____ Тетяна КАПЕЛЮШНА
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ

ПОДАННЯ ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ
на здобуття освітнього ступеня бакалавра

Направляється здобувач Матвієнко В. І. до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 125 Кібербезпека
(код, найменування спеціальності)
освітньої програми Управління інформаційною та кібернетичною безпекою
(назва)
на тему: “Методика аналізу ризиків витоку інформації через публічні джерела за допомогою OSINT-інструментів”

Кваліфікаційна робота і рецензія додаються.

Директор ННІКБЗІ _____ Євгенія ІВАНЧЕНКО
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Висновок керівника кваліфікаційної роботи

Здобувачем МАТВІЄНКОМ В’ячеславом у кваліфікаційній роботі ґрунтовно досліджено OSINT-інструменти, джерела, а також потенційні канали витоку інформації через відкриті ресурси. Закцентовано увагу на методах аналізу цифрових ризиків, що є доцільним з погляду як кіберзахисту, так і комплаєнс-менеджменту.

Робота містить приклади аналізу даних із відкритих джерел, опис методів OSINT-розвідки за тактичними схемами атак, а також реалізує кількісну модель аналізу ризиків, що надає роботі практичного спрямування та значущості.

Під час написання роботи МАТВІЄНКО В’ячеслав продемонстрував самостійність та розуміння практичних аспектів роботи з OSINT-інструментами, проявив здатність критично осмислювати джерела ризику в публічному інформаційному просторі та працювати з професійними OSINT-інструментами, узагальнювати результати в структурованому вигляді.

Робота відповідає вимогам до її виконання, а також освітньо-професійній програмі, є завершеною, що дозволяє оцінити її на “відмінно” та присвоїти МАТВІЄНКУ В’ячеславу кваліфікацію бакалавра з кібербезпеки за освітньою програмою «Управління інформаційною та кібернетичною безпекою».

Керівник кваліфікаційної роботи ___ Тетяна КАПЕЛЮШНА
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

“_____“____2025 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач Матвієнко В’ячеслав допускається до захисту даної роботи в Екзаменаційній комісії.

Завідувач кафедри
управління кібербезпекою та
захистом інформації _____ Світлана ЛЕГОМІНОВА
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

ВІДГУК РЕЦЕНЗЕНТА

на кваліфікаційну бакалаврську роботу

здобувача вищої освіти МАТВІЄНКА В'ячеслава
на тему: "Методика аналізу ризиків витоку інформації через публічні джерела за допомогою OSINT-інструментів"

Актуальність. Представлена бакалаврська робота є науково обґрунтованим дослідженням, присвяченим дослідженню проблем витоку інформації через відкриті цифрові джерела та можливостям її упередження шляхом застосування OSINT-інструментів. Автором розглянуто як теоретичні основи збору відкритої інформації, так і практичні аспекти ідентифікації ризиків, зокрема з використанням методології FAIR і фреймворку MITRE ATT&CK. Тема відзначається актуальністю, зважаючи на інформаційне протиборство в умовах гібридної війни в країні.

Позитивні сторони.

1) Запропонована узагальнена методика OSINT-аналізу, що представлена алгоритмом практичної реалізації та формулюванням рекомендацій для забезпечення інформаційної безпеки підприємства.

2) Робота має прикладну цінність у сфері кібербезпеки, зокрема щодо побудови системи інформаційного моніторингу публічної активності співробітників, окрім того обґрунтовано використання методології FAIR дозволяє забезпечити кількісну оцінку ризиків, що значно посилює здобутки роботи бакалаврського рівня.

Недоліки.

До незначних зауважень можна віднести:

1) обмежений огляд практичного впровадження OSINT-систем в українських компаніях;

2) доцільно було б доповнити дослідження аналізом правових аспектів (ЗУ «Про захист персональних даних» та «Загальний регламент про захист даних»), зважаючи на євроінтеграцію країни та адаптацію регуляторних питань всіх сфер, у тому числі – кібербезпеки.

Проте дані зауваження не змінюють позитивного враження від рівня виконання кваліфікаційної роботи.

Висновок: Кваліфікаційна робота відповідає вимогам до бакалаврських робіт за змістом, структурою та оформленням, виконана на належному науково-методичному рівні і її автор - здобувач МАТВІЄНКО В'ячеслав заслуговує на оцінку "відмінно" та присвоєння кваліфікації бакалавра з кібербезпеки за освітньою програмою «Управління інформаційною та кібернетичною безпекою».

Рецензент: _____ Галина ГАЙДУР
д.т.н., професор, завідувач кафедри Систем та технологій кібербезпеки
підпис
Ім'я, ПРІЗВИЩЕ

РЕФЕРАТ

Кваліфікаційна робота присвячена аналізу ризиків витоку інформації через публічні джерела з використанням інструментів OSINT. Робота складається зі вступу, трьох розділів, що містять 3 рисунки, 12 таблиць, висновків і списку використаних джерел із 78 найменувань. Загальний обсяг роботи становить 93 аркуші, з яких 4 аркуші займають перелік умовних скорочень та список використаних джерел.

Метою роботи є розробка методики аналізу ризиків витоку інформації через публічні джерела за допомогою OSINT-інструментів

Об'єктом дослідження є ризики витоку інформації через відкриті джерела даних.

Предмет дослідження – методи та інструменти OSINT для виявлення, упередження та кількісної оцінки ризиків витоку інформації.

Методи дослідження. У роботі застосовано методи аналізу та синтезу, порівняння й класифікації, системного підходу, моделювання за методологією FAIR, а також фреймворку MITRE ATT&CK для структурування технік розвідки.

Основні результати. Проаналізовано особливості OSINT-збору даних із соціальних мереж, держреєстрів, тендерних майданчиків та веб-ресурсів; класифіковано джерела інформаційних витоків за чутливістю й сценаріями атак; розроблено архітектуру автоматизованого моніторингу з використанням Social Searcher, OpenDataBot, Prozorro та Clarity Project; створено алгоритм побудови запитів і механізм нормалізації даних; адаптовано модель FAIR до кількісної оцінки ризиків OSINT-інцидентів; реалізовано збагачення результатів за MITRE ATT&CK і інтеграцію з SIEM для пріоритезації інцидентів; сформульовано рекомендації щодо організаційно-технічних заходів захисту.

Галузь застосування. Результати дослідження можуть бути використані при побудові систем інформаційної безпеки підприємств, впровадженні автоматизованого OSINT-моніторингу, налаштуванні SIEM/SOAR-рішень та

плануванні превентивних заходів із захисту від витоку інформації.

Ключові слова: OSINT, витік інформації, інформаційна безпека, FAIR, MITRE ATT&CK, ризик-аналіз.

ABSTRACT

The qualification work is devoted to the analysis of the risks of information leakage through public sources using OSINT tools. The work consists of an introduction, three chapters containing 3 figures, 12 tables, conclusions and a list of references containing 53 items. The total volume of the work is 82 pages, of which 4 pages are occupied by the list of abbreviations and references.

The purpose of the study is to develop a methodology for analyzing the risks of information leakage through public sources using OSINT tools.

The object of study is the risks of information leakage through open data sources.

The subject of the study is OSINT methods and tools for detecting, classifying and quantifying information leakage risks.

Research methods. The methods of analysis and synthesis, comparison and classification, systematic approach, expert evaluation, modeling according to the FAIR methodology, as well as the MITRE ATT&CK framework for structuring intelligence techniques are used in the study.

Main results. The features of OSINT data collection from social networks, state registries, tender platforms and web resources were analyzed; sources of information leaks were classified by sensitivity and attack scenarios; an architecture for automated monitoring was developed using Social Searcher, OpenDataBot, Prozorro and Clarity Project; an algorithm for building queries and a mechanism for data normalization was created; the FAIR model was adapted to quantify the risks of OSINT incidents; enrichment of results according to MITRE ATT&CK and integration with SIEM for prioritizing incidents were implemented; recommendations for organizational and technical protection measures were formulated.

Field of application. The results of the study can be used in building enterprise information security systems, implementing automated OSINT monitoring, configuring SIEM/SOAR solutions, and planning preventive measures to protect against information leakage.

Keywords: OSINT, information leakage, information security, FAIR, MITRE

ATT&CK, risk analysis.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ І СКОРОЧЕНЬ

OSINT	Open Source Intelligence розвідка з відкритих джерел
SIEM	Security Information and Event Management управління інформацією та подіями безпеки
SOAR	Security Orchestration, Automation and Response оркестрація, автоматизація та реагування
MITRE ATT&CK	MITRE Adversarial Tactics, Techniques and Common Knowledge тактики, техніки й знання MITRE
FAIR	Factor Analysis of Information Risk факторний аналіз інформаційного ризику
TEF	Threat Event Frequency частота подій загрози
Vuln	Vulnerability вразливість
LEF	Loss Event Frequency частота подій втрат
PLM	Primary Loss Magnitude первинний обсяг втрат
SLM	Secondary Loss Magnitude вторинний обсяг втрат
MFA	Multi-Factor Authentication багатофакторна автентифікація
WAF	Web Application Firewall мережевий екран веб-додатків
DLP	Data Loss Prevention запобігання витоку даних
API	Application Programming Interface інтерфейс програмування додатків
VPN	Virtual Private Network віртуальна приватна мережа
AD	Active Directory сервіс каталогів Windows
CVE	Common Vulnerabilities and Exposures загальні вразливості та експозиції)

ВСТУП

Актуальність теми. У сучасних умовах стрімкого розвитку інформаційних технологій та цифровізації бізнес-процесів рівень загроз для конфіденційності й цілісності даних постійно зростає. Зокрема, витоки інформації через відкриті джерела (OSINT) набувають дедалі більшої поширеності: зловмисники використовують публічно доступні реєстри, соціальні мережі, тендерні майданчики, судові документи й інші інтернет-ресурси для збору даних про організацію та її співробітників. В Україні, в умовах гібридних кіберзагроз, проблема своєчасного виявлення та мінімізації ризиків інформаційних витоків особливо актуальна для захисту державних і комерційних підприємств від соціальної інженерії, фішингу й інших атак. Комплексне дослідження засобів і методів оцінки цих ризиків із застосуванням OSINT-інструментів дозволяє розробити ефективні превентивні механізми й підвищити кіберстійкість вітчизняних організацій Вступ.

Мета роботи, основні завдання, об’єкт і предмет дослідження. Метою кваліфікаційної роботи є розробка методики кількісної оцінки та управління ризиками витоку інформації через публічні джерела з використанням OSINT-інструментів.

Об’єктом дослідження є процеси збору й аналізу відкритих інформаційних джерел в контексті інформаційної безпеки. Предметом дослідження – методи, інструменти та моделі кількісної оцінки ризиків витоку інформації через публічні ресурси.

Предмет дослідження. Методи, інструменти та моделі кількісної оцінки ризиків витоку інформації через публічні ресурси.

Для досягнення цієї мети в роботі необхідно виконати наступні **завдання:**

1. Проаналізувати класифікацію та характерні особливості джерел інформаційних витоків через відкриті ресурси.

2. Дослідити сучасні OSINT-інструменти та методології (MITRE ATT&CK, FAIR) для збору, систематизації й оцінки даних.

3. Розробити алгоритм автоматизованого моніторингу публічних джерел і нормалізації отриманих артефактів.

4. Запропонувати кількісну модель оцінки ризиків із використанням методології FAIR та інтеграції результатів у SIEM/SOAR-системи.

5. Сформулювати організаційно-технічні рекомендації щодо зниження виявлених ризиків і підвищення кіберстійкості.

Методи дослідження. Аналіз та синтез наукових публікацій і практичних рішень із OSINT, класифікація та порівняння інструментів збору даних, моделювання ризиків за методологією FAIR, фреймворк MITRE ATT&CK для структурування технік розвідки, експертна оцінка та тестування прототипа.

Практичне значення одержаних результатів. Розроблена методика дозволяє інформаційним службам підприємств організувати безперервний OSINT-моніторинг, автоматизовано виявляти ознаки збору даних з публічних джерел і оцінювати потенційні витрати на інциденти. Впровадження алгоритму забезпечує прискорене реагування на розвідувальні активності противника, оптимізує використання ресурсів ІБ-підрозділів та підвищує ефективність захисних заходів (MFA, WAF-правила, DLP, регулярні тренінги з кібергігієни).

Апробація результатів. Результати дослідження можуть бути використані при побудові систем інформаційної безпеки підприємств, впровадженні SIEM/SOAR-рішень, автоматизації OSINT-моніторингу та плануванні превентивних заходів із захисту від витоку інформації. Основні положення доповідалися та обговорювалися на науково-практичній конференції «Стратегії кіберстійкості: управління ризиками та безперервність бізнесу» 28 лютого 2024 р.

РОЗДІЛ 1. ОСОБЛИВОСТІ ВИКОРИСТАННЯ OSINT-ІНСТРУМЕНТІВ ДЛЯ УПЕРЕДЖЕННЯ РИЗИКІВ ВІД ВИТОКУ ІНФОРМАЦІЇ

1.1 Мета проведення та джерела OSINT

Стрімке поширення даних онлайн-мережею з моменту появи Інтернету значно розширило можливості збору та аналізу відкритої інформації з різних джерел. За останнє десятиліття розвиток соціальних мереж і смартфонів, оснащених камерами, прискорив цю тенденцію. Фото і відео з будь якої точки землі щосекунди заповнюють соціальні мережі величезними обсягами даних, що глибоко вплинуло на сприйняття громадськістю сучасної безпеки. Активне використання загальнодоступних даних призвело до того, що експерти вважають наш час новою ерою – ерою розвідки, яка характеризується цілеспрямованим пошуком, збором, аналізом і поширенням інформації для зменшення невизначеності осіб, які приймають рішення. Використання загальнодоступних даних фахівцями з розвідки в державному і приватному секторах, а також громадянським суспільством часто називають розвідкою з відкритих джерел (OSINT).

Open Source Intelligence (OSINT), або розвідка з відкритих джерел, є важливим та не від’ємним напрямом сучасного аналітичного та безпекового процесу, який переживає стрімкий розвиток через цифрову трансформацію нашого світу. На відміну від традиційного здобування розвідувальної інформації, OSINT базується на зборі, обробці та аналізі даних, що є легально доступними для широкого загалу.

Історія OSINT як розвідувального інструмента почалася ще задовго до цифрової епохи. Вперше думка про необхідність збору інформації з відкритих джерел була офіційно озвучена під час Другої світової війни, коли уряд США створив Foreign Broadcast Monitoring Service (пізніше – Foreign Broadcast Information Service, FBIS), який займався аналізом відкритих радіопередач

супротивника. Аналогічні ініціативи існували також у Великобританії та Нідерландах, що вже тоді свідчило про глобальний інтерес до використання відкритих джерел у воєнно-політичному контексті [53].

У період Холодної війни відкриті джерела використовувалися як допоміжний ресурс до технічної та агентурної розвідки. Проте, починаючи з 1990-х років, після глобальної комп'ютеризації, OSINT поступово перетворився з додаткового інструмента на самостійний напрям аналітики. У 2006 році Директор національної розвідки США, Джон Негропонте, визнав OSINT "джерелом першої інстанції" у директиві ICD-301[48].

У XXI столітті, з розвитком мобільного зв'язку, супутникових зображень та цифрових архівів, OSINT набув ще більшої актуальності. Його почали активно використовувати не лише державні структури, а й приватні компанії, правозахисні організації, журналісти-розслідувачі та навіть звичайні люди. Сьогодні ж OSINT виступає не лише як додаткове джерело інформації, а й як критично важливий елемент у створенні цілісної картини подій, оцінці ризиків та прийнятті стратегічних рішень.

Таким чином, OSINT перетворився з побічного розвідницького інструменту на окремий напрямок знань із власними методами, інструментами, етичними принципами та правовими рамками. Його подальший розвиток допоможе нам зрозуміти інформаційні виклики та можливості у добу глобальної відкритості.

Тепер після з'ясування того що ж таке розвідка з відкритих відкритих джерел, тепер потрібно розібратися як що ми маємо на увазі під цим визначенням.

Під відкритими джерелами у контексті OSINT маються на увазі будь-які законно доступні дані, які не потребують спеціального дозволу на перегляд чи використання, авторизації або порушення прав доступу. Це можуть бути як традиційні, так і цифрові ресурси, що охоплюють найпоширеніші категорії інформації. За класифікацією, запропонованою фахівцями SANS Institute, джерела OSINT умовно поділяються на наступні ключові типи [47]:

1. Традиційні мас-медіа
2. Інтернет-ресурси
3. Соціальні мережі
4. Гео-просторові дані
5. Офіційні державні реєстри та бази даних
6. Наукові та академічні публікації
7. Форуми, даркнет і спеціалізовані спільноти
8. Мультимедійні джерела

Традиційні мас-медіа — це один із найдавніших і стабільних типів джерел у контексті Open Source Intelligence (OSINT). До них відносять газети, журнали, радіо, телебачення, офіційні друковані бюлетені та прес-релізи. Ці джерела мають тривалу історію використання у розвідці, особливо до появи інтернету. Вони продовжують бути актуальними і по сьогодні через декілька факторів. Однією з них регулярність публікації таких видань, вона допомагає відстежувати події протягом потрібного часу. Ще одним вагомим аргументом буде використання виключно перевірених або офіційних джерел, також перед публікацією воно проходять додатковий факт-чекінг редакторами. Хоч вони і не мають такої швидкості як інші джерела, проте їх історична цінність та надійність роблять їх незамінними при довготривалому моніторингу та підтвердженні певних фактів.

Інтернет-ресурси стали основою сучасного OSINT, забезпечуючи не тільки широкий спектр тем, а й оперативність та гнучкість Це джерело надає найбільшу частину інформації для моніторингу ситуацій в реальному часі, виявленні тенденцій, доступі до структурованої інформації, та перевірці автентичності інших даних. Великою перевагою цього виду є надзвичайна маштабованість – нам відразу доступні десятки мільйонів даних сайтів, репозиторіїв та архівів за багато років. За їх допомогою можна перевірити інформацію яка публікувалась декілька років назад, так і ту яка щойно з’явилася. Але потрібно бути обережним з свіжою інформацією, оскільки вона може бути не редагованою або навіть

фейковою. Допомогти зі збором інформації в інтернет ресурсах допоможе автоматизація за допомогою веб-скрейперів наприклад для державних сайтів.

Соціальні мережі стали ще одним невід’ємним джерелом в OSINT. Завдяки тому, що їх використовують мільйони людей в мережі залишаються великі обсяги даних. За їх допомогою можна отримати інформацію про настрої, події, соціальні зв’язки та навіть геолокаційні дані що робить їх незамінним інструментом для фахівців. До плюсів можна віднести високу оперативність, зазвичай свіжу інформацію про важливі і не дуже події люди публікують саме тут. Різноманітність форматів також є плюсом оскільки можна знайти не тільки текстові згадки, а й фото, відео чи навіть прямі трансляції. Проте така масовість і одночасно і мінусом, оскільки для отримання потрібних даних потрібно передивитися купи інформації. До того ж, соцмережі часто використовують для розповсюдження фейків та дезінформації. Додатково можуть виникнути непорозуміння через використання чутливої інформації розміщеної там. Хоч це і є потужний інструментом проте потрібно використовувати його з розумом та обережністю, щоб не нашкодити собі та людям. Але з правильним підходом вони можуть надати цінну інформацію для розвідки чи журналістики.

Геопросторові дані або їх ще називають GEOINT це ще одне необхідне джерело у сфері OSINT, забезпечуючи аналітиків точними візуальними та просторовими відомостями про фізичні об'єкти, події та активність на земній поверхні. Ці дані охоплюють супутникові знімки, аерофотознімки, цифрові моделі рельєфу, геолокаційні метадані та інші просторові інформаційні ресурси. Окрім цього фотографії та відео, зроблені за допомогою смартфонів або цифрових камер, часто містять метадані (EXIF), які включають координати зйомки, час та інші параметри. Ці дані можуть бути використані для геолокації об'єктів та подій.

Офіційні державні реєстри є одним із найнадійніших джерел у сфері розвідки з відкритих джерел, оскільки вони містять перевірену, структуровану та юридично підтверджену інформацію. Ці дані охоплюють широке коло тем: від реєстрації компаній і судових рішень до державних закупівель, нерухомості та

виборчих процесів. Проте їхнє використання вимагає уважного ставлення до юридичних та етичних аспектів, а також розуміння обмежень, пов'язаних з доступністю та актуальністю даних.

Форуми та даркнет одна з найскладніших категорій для розвідки оскільки пошук інформації може бути досить непростим для пересічного користувача. Але вони дозволяють отримати унікальну інформацію про кіберзагрози, злочинні мережі, обмін викраденими даними, а також обговорення нових методів атак та технологій обходу захисту. Ці платформи, зокрема даркнет-форуми, функціонують у середовищі з високим рівнем анонімності. Тут можна виявити індикатори компрометації, тактики та техніки зловмисників, а також перші згадки про вразливості ще до їх публічного розкриття. Водночас значно зростає ризик натрапити на недостовірну інформацію та порушення закону, особливо в частині доступу до заборонених ресурсів або незаконного збору даних.

Можливо перевести їх в ризики?

Порівняння всіх категорій джерел наведено в таблиці 1.1

Таблиця 1.1

Класифікація джерел OSINT

Категорія джерела	**Приклади**	**Доступність**	**Частота оновлення**	**Ймовірність ризику**
Традиційні мас-медіа	BBC, CNN, Reuters	Відкрита, частково з підпискою	Щодня / щогодини	Низька
Інтернет-ресурси	Офіційні сайти, блоги, новинні портали	Відкрита	Залежить від платформи (від годин до тижнів)	Низька
Соціальні мережі	Facebook, X (Twitter), Telegram	Відкрита, але змінювана політика доступу	Реальний час / секунди	Середня – висока (дезінформація, фейки)
Геопросторові дані	Google Earth, Sentinel Hub, OpenStreetMap	Переважно відкрита	Від кількох годин до днів	Середня (помилки в інтерпретації)
Офіційні державні реєстри	YouControl, OpenCorporates, ЄДР, судові бази	Переважно відкрита, частково з авторизацією	Щотижня / щомісяця	Низька – середня
Форуми та даркнет	Reddit, форуми, onion-сайти (з відкритим доступом)	Частково відкрита, ризикована	Нерегулярно	Висока (анонімність, дезінформація)

Після визначення джерел отримання інформації потрібно дізнатися її зміст, адже сама інформація це лише набір символів який не зможе дати чітку відповідь на питання. Самі по собі відкриті дані не мають цінності без чітко визначеної

мети, на яку спрямовані зусилля аналітика, який і формує запит і визначає релевантність джерел. Таким чином, наступним аспектом у вивченні OSINT є його функціональне призначення, тобто ті конкретні цілі, заради яких здійснюється моніторинг, збір та інтерпретація відкритої інформації в різних сферах. Давайте розглянемо основні сценарії для використання розвідки з відкритих джерел.

Почнемо з того, що потрібно визначити що саме нам загрожує. Ідентифікація загроз за допомогою OSINT щодня стає дедалі частішою практикою та набуває більшого значення в контексті сучасних викликів кібербезпеки, гібридних конфліктів та інформаційних війн. На сьогодні, значна частина критично важливої інформації стала публічно доступною, саме відкриті джерела —стали потужним інструментом для виявлення потенційних загроз як на рівні держав, так і приватного сектору. Методологія OSINT для ідентифікації загроз полягає у фільтрації, аналізі та синтезі інформації зібраної з відкритих джерел з метою виявлення індикаторів компрометації (IoC), прогнозування загроз, виявлення уразливостей та ідентифікації джерел ризику.

Особливе значення приділяється аналітиці соціальних мереж та форумів, що дозволяє виявляти потенційно небезпечні акаунти, координаційні центри інформаційних операцій або планування кібер- та фізичних атак. Форуми в даркнеті , технологічні блоги та комунікаційні майданчики, такі як Pastebin або Telegram-канали, слугують джерелами інформації про нові шкідливі кампанії або витоки даних. Аналіз реєстрів доменних імен і IP-адрес дозволяє зв’язати певні ресурси з уже відомими зловмисними структурами, а дані з баз вразливостей — оцінити технічні можливості атакуючої сторони.

Застосування OSINT виходить далеко за межі кібербезпеки. Його використовують в правоохоронній діяльності для розслідування злочинів і пошуку підозрюваних за цифровими слідами, у військовій розвідці — для моніторингу пересування сил противника, аналізу супутникових зображень або публічних повідомлень. У корпоративному середовищі OSINT слугує для репутаційного моніторингу, конкурентної розвідки та захисту бренду. Один із

найбільш показових прикладів ефективного використання OSINT був зафіксований під час збройного конфлікту в Україні, коли на основі аналізу соціальних мереж, геолокації зображень і програм розпізнавання облич вдалося ідентифікувати численні випадки присутності російських військових на території України [36].

Таким чином, OSINT перестав бути лише допоміжним інструментом аналітики — він став невіддільним елементом стратегічного забезпечення безпеки, дозволяючи проактивно виявляти загрози ще до того, як вони перейдуть у фазу атаки. Поєднання відкритих джерел, автоматизованих інструментів, методів штучного інтелекту та досвідченого людського аналізу формує нову парадигму розвідки, яка вже сьогодні змінює уявлення про превентивну безпеку в цифрову епоху.

Правильне використання розвідки відкритих джерел відкриває нам можливості не тільки попередження загроз, але й може надати важливу інформація яка допоможе приймати правильні рішення. Адже у бізнес-середовищі стратегічне планування потребує не лише інтуїції та досвіду, а й системного підходу до збору, аналізу та використання актуальної інформації. Підтримка прийняття рішень стала тим кроком, що забезпечує організаціям можливість адаптуватися до змін, оптимізувати ресурси та досягати довгострокових цілей.

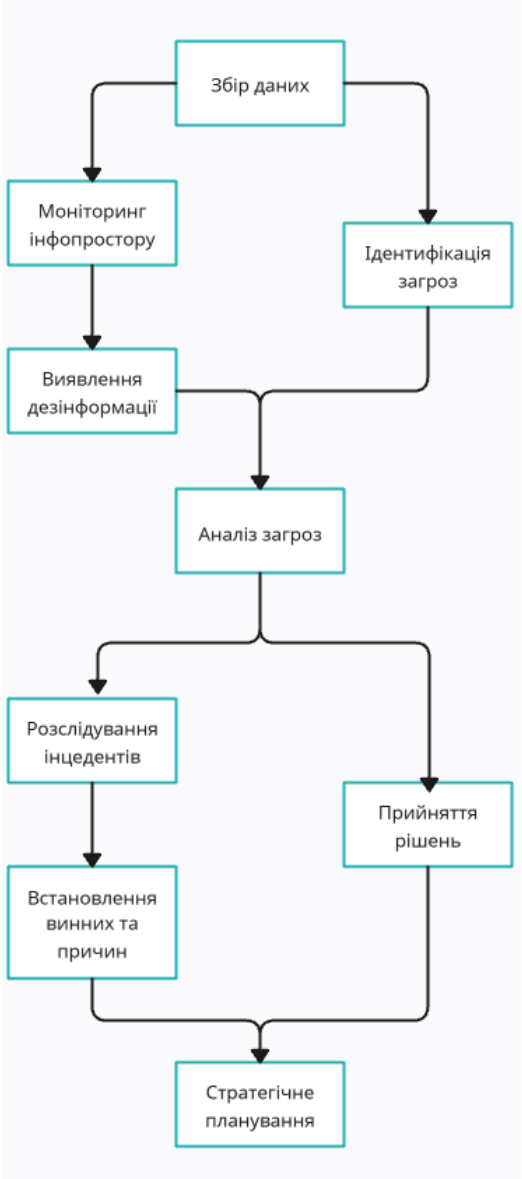

Рис. 1.1 Системи прийняття рішень

Підсумовуючи вище сказане, ефективне стратегічне планування неможливе без надійної підтримки прийняття рішень. Інтеграція сучасних інформаційних систем, аналітичних інструментів та методологій дозволяє організаціям приймати обґрунтовані рішення, адаптуватися до змін та досягати поставлених цілей у конкурентному середовищі.

Для того аби стратегічне планування було ефективним і адаптивним, воно повинно спиратися не лише на поточні події, а й на досвід минулих подій. Саме тут OSINT як інструмент розслідування, що допомагає встановити причини інцидентів і виявити відповідальних. Такий підхід дозволить не тільки реагувати

на загрози, а робити висновки, які формують основу для правильних рішень у майбутньому.

Розслідування інцидентів вже давно стало невід'ємною частиною сучасної практики кібербезпеки. Воно дозволяє встановлювати причини подій, ідентифікувати винних осіб та формувати доказову базу. А використання технологій розвідки тільки покращить результати.

Ще одним важливим елементом в OSINT-розслідуваннях є атрибуція [49] — процес встановлення відповідальності за кіберінцидент. Це складне завдання, оскільки зловмисники часто використовують техніки маскування, такі як "false flag" атаки, щоб ускладнити ідентифікацію. Для подолання цих викликів дослідники розробляють нові підходи, наприклад, використання системи EXTRACTOR (Extracting Attack Behavior from Threat Reports) для автоматичного вилучення поведінкових моделей атак з текстових звітів.

У контексті війни в Україні OSINT став потужним інструментом для документування воєнних злочинів та ідентифікації причетних осіб. Організації, такі як Molfar[35], активно використовують відкриті джерела для збору доказів та підтримки правозахисних ініціатив.

Саме тому або через це(Таким чином), OSINT є незамінним інструментом у розслідуванні кіберінцидентів, забезпечуючи доступ до актуальної інформації, що сприяє встановленню причин подій та ідентифікації винних осіб. Його ефективність залежить від поєднання технічних знань, аналітичних навичок та етичного підходу до використання зібраної інформації.

Проте розвідка підходить не тільки реактивних дій. Її можна використовувати і в проактивному ключі наприклад для моніторингу інформаційного та кіберпростору щоб виявити дезінформацію чи відстежети зміни у публічному дискурсі. Сьогодні такі атаки в інформаційно-цифровому середовищі можуть мати серйозні наслідки для національної безпеки та громадської думки. Для протидій таким компаніям можна використовувати відкриті джерела для виявлення ознак підготовки атак чи інших протиправних дій.

Крім того, платформи, такі як Cyabra [34], застосовують штучний інтелект для виявлення фейкових профілів та координаційних мереж, що поширюють дезінформацію. Це дозволяє в режимі реального часу відстежувати та нейтралізувати загрози, пов'язані з фейковими новинами та маніпулятивними кампаніями

Завдяки цьому OSINT допомагає в виявленні та протидії дезінформації, а також для підтримки стратегічного планування та захисту інформаційного простору.

1.2 Ризики витоку інформації через публічні джерел

Через постійний розвиток та цифровізацію, організації дедалі більше стикаються з нетиповими векторами загроз, що не потребують проникнення в системи, зламів чи використання складного шкідливого ПЗ. Як виявляється одним із таких векторів є витік інформації через публічні джерела, або ж так звана розвідка з відкритих джерел.

Відкриті дані — це не лише державні реєстри чи офіційні сайти компаній. Це також соціальні мережі співробітників, професійні профілі, платформи для спільної розробки, ресурси для публікації оголошень про вакансії, презентаційні документи, а також документи, що випадково були розміщені в загальному доступі й проіндексовані пошуковими системами. Такі витоки становлять серйозну загрозу для безпеки організацій. Зловмисники можуть використовувати відкриту інформацію для соціальної інженерії, фішингу та інших атак. А використання таких типів атак є дуже частим та небезпечним. Ці методи базуються на психологічному впливі на людей, використовуючи їхню довіру, страх або бажання допомогти.

Зловмисники часто використовують відкриту інформацію з публічних джерел, таких як соціальні мережі, корпоративні сайти або професійні платформи, для створення переконливих фішингових атак. Знання про структуру

організації, імена співробітників та їхні ролі дозволяє створювати цілеспрямовані атаки, що підвищує їх ефективність. Наприклад, у випадку з атакою на компанію

Сучасні технології, зокрема штучний інтелект, дозволяють зловмисникам створювати ще більш переконливі фішингові атаки. Наприклад, у 2024 році було зафіксовано випадки використання deepfake-технологій для імітації голосів генеральних директорів компаній FTSE 100 [37]. Зловмисники створювали фальшиві голосові повідомлення, які звучали як справжні керівники, і використовували їх для переконання співробітників у необхідності термінового переказу коштів .

Для захисту від таких атак організаціям слід впроваджувати комплексні заходи безпеки, включаючи навчання співробітників розпізнаванню фішингових повідомлень, обмеження доступу до публічної інформації про структуру компанії та використання багатофакторної автентифікації. Також важливо регулярно проводити аудити безпеки та оновлювати політики конфіденційності відповідно до сучасних загроз.

Соціальна інженерія та фішинг залишаються одними з найефективніших методів кібератак, особливо коли зловмисники мають доступ до відкритої інформації про організацію. Для мінімізації цих ризиків організаціям слід впроваджувати політики цифрової гігієни, проводити регулярні тренінги та обмежувати публікацію чутливої інформації. Також обов’язковим є навчання співробітників розпізнавати потенційні загрози та дотримуватися безпечних практик в онлайн-середовищі.

Відповідно до звіту IBM X-Force Threat Intelligence Index за 2024 рік, понад третину кіберінцидентів починаються не з технічної атаки, а з глибокого аналізу відкритих джерел, де зловмисники збирають інформацію про структуру організації, її технічний стек, співробітників, внутрішні процеси [38]. Це дозволяє формувати максимально точні сценарії соціальної інженерії, фішингові кампанії та атаки на ланцюги постачання. Наприклад, в одному з випадків 2022 року атака на банківську установу розпочалась із вивчення профілів

співробітників на LinkedIn, де містилася інформація про використання CRM-системи Oracle Siebel [39]. Це дало змогу хакерам точніше підібрати інструменти та вектори впливу.

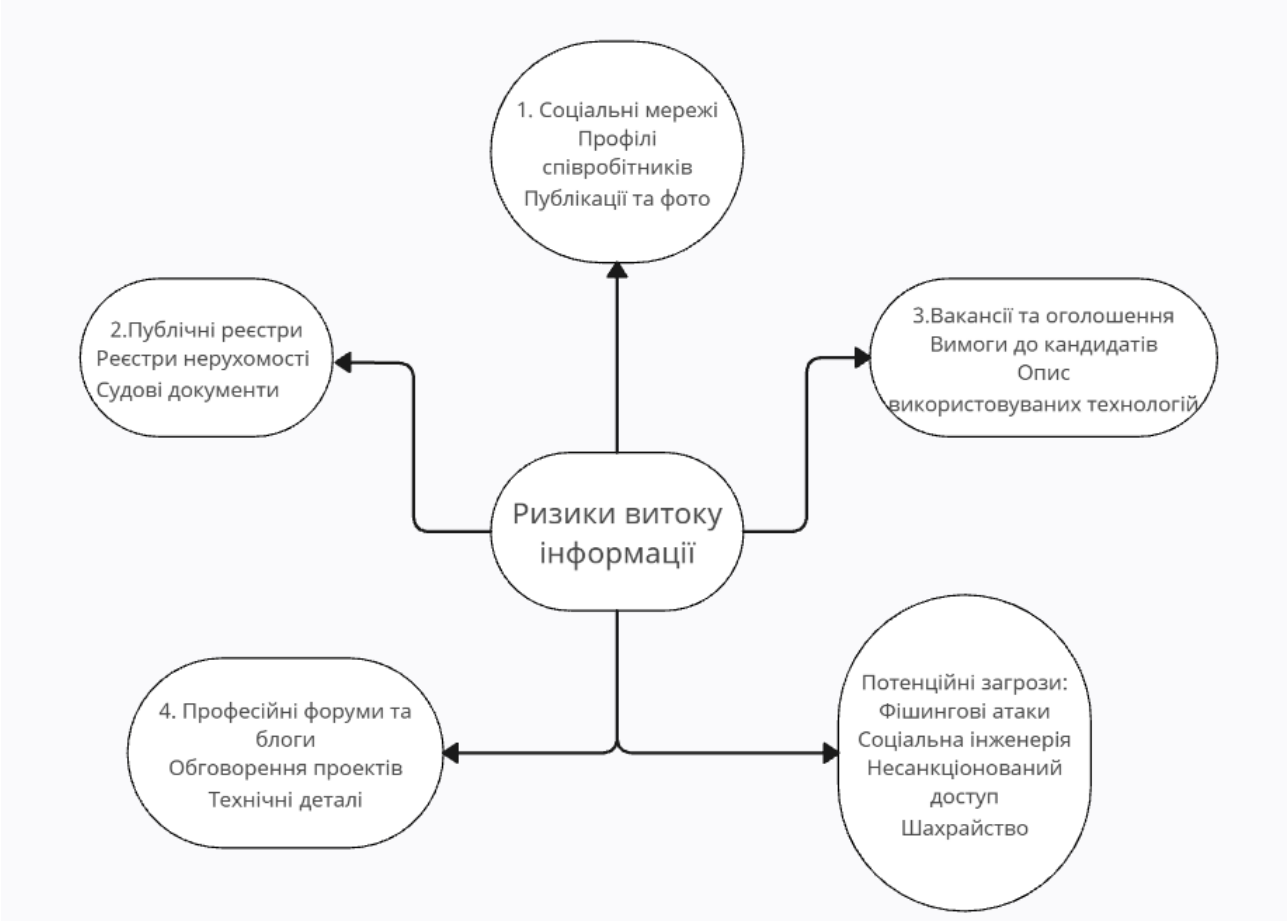

Рис. 1.2 Ризики витоку інформації

Ненавмисне розкриття інформації співробітниками через соціальні мережі, блоги або інші публічні платформи становить серйозну загрозу для кібербезпеки організацій. Такі витоки часто виникають через необережність, відсутність обізнаності або недотримання політик конфіденційності.

Одним із поширених прикладів є публікація фотографій з робочого місця, на яких можуть бути видимі конфіденційні документи, екрани з чутливою інформацією або елементи інфраструктури. Такі зображення можуть надати зловмисникам цінні відомості про внутрішні процеси компанії, використовуване програмне забезпечення або фізичне розташування об'єктів.

Іншим прикладом є випадкове розміщення конфіденційних документів у відкритому доступі. Наприклад, у 2017 році компанія River City Media ненавмисно опублікувала резервну копію бази даних без належного захисту, що призвело до витоку понад 1,3 мільярда записів [40].

Також, співробітники можуть випадково оприлюднити чутливу інформацію через особисті блоги або публікації в соціальних мережах, обговорюючи робочі проекти або внутрішні процеси компанії..

Для мінімізації таких ризиків організаціям слід впроваджувати політики цифрової гігієни, проводити регулярні тренінги для співробітників щодо безпечного використання соціальних мереж та інших публічних платформ, куди може потрапити чутлива інформація.

Загалом, ненавмисне розкриття інформації співробітниками є значним викликом для організацій, небезпека полягає в тому, що такі витоки відбуваються без відома самої організації. Нерідко навіть досвідчені IT-команди не контролюють, яку інформацію розміщують у публічному доступі працівники у вигляді презентацій, резюме чи запитів на форумах. Показовим став інцидент 2023 року, коли через відкритий репозиторій Bitbucket було знайдено конфігураційні файли з обліковими даними до бази даних однієї з державних структур Східної Європи [41]. Причиною стало неправильне налаштування приватності репозиторію, що дозволило стороннім особам отримати доступ до понад мільйона записів.

Ще одною схожою небезпекою є витоки публічних реєстрів. Вони становлять серйозну загрозу безпеці як звичайних людей так, і організацій. Державні бази даних, які містять особисту або корпоративну інформацію, можуть бути доступні стороннім особам через недостатній захист або кібератаки.

Наприклад, у грудні 2023 року внаслідок кібератаки на Міністерство юстиції України було тимчасово призупинено роботу ключових державних реєстрів, включаючи реєстри актів цивільного стану, прав на нерухомість та юридичних осіб [42]. Це призвело до зупинки реєстрації шлюбів, угод з нерухомістю та інших адміністративних послуг. Хоча уряд повідомив, що витоку

даних не відбулося, інцидент підкреслив вразливість державних реєстрів до кібератак .

Крім того, в Україні було виявлено, що через неналежні заходи кібербезпеки в центрах технічного огляду транспортних засобів у відкритому доступі опинилися сотні тисяч особистих документів, включаючи паспорти, ідентифікаційні коди та водійські посвідчення. Ці дані були доступні на незахищеному сервері протягом чотирьох років, що створювало ризик їх використання зловмисниками для шахрайства або інших злочинних дій .

Подібні випадки підкреслюють необхідність посилення заходів безпеки щодо зберігання та обробки даних у державних реєстрах. Це включає впровадження сучасних технологій захисту, регулярні аудити безпеки та навчання персоналу з питань кібербезпеки. Також важливо забезпечити прозорість у роботі з персональними даними та інформувати громадян про можливі ризики.

Загалом, витоки через публічні реєстри демонструють, що навіть офіційні джерела інформації можуть стати джерелом загроз, якщо не приділяти належної уваги їх захисту. Тому необхідно розробляти та впроваджувати комплексні стратегії кібербезпеки на державному рівні, щоб мінімізувати ризики витоку конфіденційної інформації.

Ще один поширений шлях витоку — метадані документів, що містяться в PDF-, DOCX- або інших форматах. Згідно з дослідженням Recorded Future, до 18% відкритих корпоративних документів містять метадані, які дозволяють визначити імена авторів, структуру каталогів на внутрішніх серверах, назви проєктів або використовуване програмне забезпечення [43]. Це може бути використано не лише для зламу, а й для побудови моделі загроз, яка базується на реальній інфраструктурі компанії.

Оголошення про тендери та вакансії також виступають джерелом неусвідомленого витоку. У технічних вимогах до постачальників часто вказуються параметри мережевих рішень, використовуваних платформ або навіть IP-адреси тестових середовищ. В оголошеннях про вакансії компанії

нерідко перелічують повний стек технологій, що дає хакерам змогу заздалегідь шукати вразливості у відповідних продуктах.

Усе це створює критично важливу потребу для організацій системно управляти своїм цифровим відбитком. Йдеться про те, щоб не лише захищати сервери та бази даних, а й контролювати інформацію, яка "виливається" у публічний простір через дії співробітників, автоматичні налаштування сервісів чи публікації у відкритому доступі. Практика регулярного OSINT-аудиту, навчання працівників цифровій гігієні, обмеження надмірної деталізації в оголошеннях та документах — усе це має стати частиною кіберзахисної стратегії.

Оскільки витоки через відкриті джерела здебільшого не фіксуються системами виявлення вторгнень (IDS/IPS), вони можуть залишатися непоміченими протягом тривалого часу, доки не спричинять інцидент, який вразить як репутацію компанії, так і її операційну діяльність. Саме тому одним із головних викликів для фахівців з інформаційної безпеки сьогодні є побудова системи інформаційного контролю, яка враховує не лише внутрішні загрози, але й зовнішній публічний контекст — від GitHub до Google.

Таким чином, проблема витоку даних через публічні джерела вже не є гіпотетичною — вона є системною та поширеною. Захист організації більше не обмежується паролями, антивірусами чи міжмережевими екранами. Його новим елементом стає здатність бачити себе очима потенційного атакувальника та завчасно закривати інформаційні «вікна», які відкриває сам бізнес — іноді мимоволі, іноді через незнання.

З розвитком як технологій безпеки так і самого OSINTу наступним етапом еволюції стала наявність розвинених інструментів автоматизації та візуалізації даних. Зокрема, платформи на зразок MISP (Malware Information Sharing Platform) [44] дають змогу структурувати та обмінюватися індикаторами загроз між організаціями, підвищуючи колективну захищеність. Інструмент Maltego надає можливість візуалізувати складні зв’язки між об’єктами розслідування — наприклад, виявити зв’язок між доменом, електронною адресою та IP-адресою.

Інша платформа, SpiderFoot, охоплює понад 200 модулів OSINT-збору, що дозволяє створити повну картину ризиків, пов’язаних із певною організацією або особою. Платформи нового покоління на зразок Babel Street забезпечують глибоку аналітику даних понад 200 мовами, поєднуючи AI-аналіз з геопросторовими та лінгвістичними методами для раннього виявлення загроз у фізичному, інформаційному та кіберпросторі.

1.3 Інструменти та методи аналізу ризиків витоку інформації за допомогою OSINT

Клас інструментів для збору інформації у системі OSINT (Open-Source Intelligence) охоплює програми й фреймворки, які автоматизують процес пошуку та агрегації відомостей із відкритих джерел. Вони працюють на перетині інформаційного пошуку, мережевої розвідки та початкового цифрового профілювання об'єктів дослідження — компаній, особистостей або інфраструктур. На відміну від загального ручного пошуку, ці засоби дозволяють виводити цілісну картину доступних даних за лічені хвилини, що критично важливо для роботи кіберрозвідників, журналістів-розслідувачів або аналітиків безпеки. Одними з найпопулярніших представників цього класу є theHarvester, Shodan та Recon-ng.

theHarvester [50] — це легкий, але потужний інструмент, що спеціалізується на збиранні електронних адрес, доменних імен та імен користувачів із відкритих пошукових систем та служб. Його початкове застосування — це етап “footprinting” у пентестах або розвідці перед цільовим дослідженням. theHarvester звертається до зовнішніх джерел, таких як Google, Bing, Yahoo, LinkedIn, а також до специфічних сервісів типу Hunter.io або Baidu, формуючи початковий масив цифрових слідів. Завдяки відкритому коду та CLI-архітектурі, theHarvester є зручним для швидкого сканування інфраструктури за ключовими запитами. Водночас варто враховувати його обмеженість у глибокому аналізі — він не забезпечує перевірку актуальності даних, не аналізує

пов'язані зв'язки між об'єктами та не має механізмів верифікації. Це робить його доцільним як початковий інструмент збору, але недостатнім для всебічної оцінки об'єкта.

Іншим представником цього класу є Shodan [51] — спеціалізована пошукова система, орієнтована на індексацію пристроїв, що мають відкриті порти та доступні в Інтернеті. Її алгоритм базується на активному скануванні мережевої інфраструктури, що дозволяє відображати банери сервісів, використовувані протоколи, серійні номери, операційні системи, а також виявляти потенційні вразливості. Саме тому Shodan активно використовується в аналізі промислових систем, IoT-пристроїв, серверів і навіть камер відеоспостереження. Унікальність полягає в тому, що цей сервіс дозволяє будувати складні логічні запити з використанням фільтрів, таких як country, port, org, product тощо, що дає змогу точно локалізувати інфраструктурні об'єкти. З іншого боку, потужність Shodan часто вимагає технічної обізнаності: неправильно інтерпретовані дані можуть призвести до хибних висновків. Також частина функціоналу (наприклад, доступ до повного API або історичних даних) є платною, що обмежує його застосування для широкого кола користувачів. Інформація базується на офіційній документації Shodan та відкритому API.

Найбільш функціонально комплексним з-поміж трьох є Recon-ng [52] — модульний фреймворк, що орієнтований на автоматизацію повного циклу OSINT-дослідження. На відміну від інструментів-сканерів, він надає користувачеві структуру, подібну до Metasploit Framework, де кожна розвідоперація виконується в межах сесії проекту, з можливістю збереження результатів, побудови зв’язків і повторного використання даних. Recon-ng підтримує десятки модулів, які реалізують доступ до популярних сервісів — від WHOIS-запитів до інтеграції з HaveIBeenPwned або VirusTotal. Його сила полягає в гнучкості: користувач сам формує сценарії роботи, підключає API, комбінує модулі й таким чином отримує глибоку і логічно структуровану розвідку. Проте ця гнучкість має зворотній бік — для ефективного використання потрібно мати досвід роботи в CLI-середовищах, вміти керувати API-ключами

та знати логіку побудови запитів. Цей інструмент потребує значного налаштування перед запуском повноцінного проєкту, що може стати бар'єром для новачків.

Таблиця 1.2

Інструменти збору інформації OSINT: підхід систематизованої аналітики

Функція	**theHarvester**	**Shodan**	**Recon-ng**
Призначення	Збір відкритих email-адрес, піддоменів, URL та імен хостів із загальнодоступних джерел	Пошук і аналіз пристроїв та сервісів, відкритих в інтернеті	Модульна рамкова система для проведення комплексної OSINT-розвідки через численні інтегровані модулі
Тип ліцензії	Відкритий код	Комерційна	Відкритий код
Джерела даних	Пошукові системи, PGP, LinkedIn, GitHub, Netcraft, crt.sh тощо	Інтернет-сканування (порт-скан, банер-граббінг), власні краулери	Набір модулів для WHOIS, DNS, Google, LinkedIn, Twitter, HaveIBeenPwned
Інтерфейс користувача	CLI- Інтерфейс	Веб-інтерфейс, CLI; мобільні/десктоп клієнти, REST API	Інтерактивна консоль на базі веб-інтерфейсу; CLI для управління модулями
Автоматизація	Скриптове використання в bash/python;	Планувальник сканів, webhook-сповіщення, API-токени	Збереження і автоматичний запуск модулів; сценарії через API та інтеграція з CI/CD
Розширюваність	Відкритий вихідний код — додавайте нові джерела або модулі на Python	Плагіни через Marketplace, інтеграція з SIEM/Threat Intelligence	Створення власних модулів на Python із простим шаблоном, широкі можливості кастомізації
Найкраще підходить для	Попередній збір контактів, рекогносцировка мережі, OSINT-бенчмаркінг	Глибокий пошук відкритих сервісів, моніторинг IoT та мережевих ризиків	Повноцінні OSINT-розслідування з багатоступеневою автоматизацією, побудова розгалужених ланцюжків збору даних

Усі інструменти репрезентують підхід до збору OSINT-даних як до систематизованої аналітики. theHarvester надає швидкий старт у вигляді електронних слідів, Shodan поглиблює мережеву видимість та викриває технічні вразливості, а Recon-ng забезпечує структурований підхід до побудови розвідпроєкту. Разом вони становлять фундамент технічного компоненту

сучасного OSINT-дослідження, поєднуючи швидкість, точність та гнучкість аналітики.

Після етапу первинного збору даних в OSINT-розслідуваннях наступає не менш важливий етап — структуризація, інтерпретація та візуалізація отриманої інформації. Ці процеси критичні для побудови логічних зв’язків між розрізненими об’єктами, виявлення трендів, схожих шаблонів або прихованих взаємозалежностей. Саме тому окремий клас OSINT-інструментів спеціалізується на аналізі та візуалізації даних. До найбільш відомих і ефективних рішень у цій категорії належать Maltego та SpiderFoot — кожен із них репрезентує різний підхід до обробки розвідданих: один фокусується на графовій візуалізації та мануальному дослідженні зв’язків, інший — на автоматизованому аналізі й генерації висновків.

Maltego, [45] розроблений компанією Paterva, є однією з найпотужніших платформ для візуалізації OSINT-даних. Його головна сила — побудова графових зв’язків між об’єктами, такими як електронні адреси, домени, IP-адреси, імена користувачів, профілі в соціальних мережах, номери телефонів тощо. Кожен об’єкт (entity) на графі може бути пов’язаний із сотнями інших, завдяки чому користувач буквально "бачить" мережу взаємозв’язків, які неочевидні при лінійному перегляді інформації. Maltego підтримує трансформації — спеціальні модулі, які дозволяють з об’єкта запускати API-запити до різних джерел, таких як Shodan, VirusTotal, HaveIBeenPwned, WhoisXML API тощо. Наприклад, отримавши електронну пошту, аналітик може за кілька кліків встановити домен, IP-адресу, сервер, пов’язаний акаунт у Twitter або Facebook, а також з ким об’єкт мав контакт.

Maltego доступний у безкоштовній версії (CE), однак повноцінний функціонал відкривається в комерційних варіантах (Classic, XL), де реалізовано підтримку більших графів, власних трансформацій і корпоративних інтеграцій. Одним із викликів при роботі з платформою є потреба в глибокому розумінні структури даних та логіки побудови графа — інтерфейс хоч і візуальний, але вимагає аналітичної дисципліни та уважності. Maltego не є простою

візуалізаційною платформою — це інструмент побудови розвідувального контексту, в якому аналітик формує гіпотези, перевіряє їх і розкриває приховані структури даних.

Інший інструмент цього класу — SpiderFoot [46]. Він орієнтований на автоматизований аналіз об’єктів і надає користувачу всебічний звіт про будь-яке цифрове або інфраструктурне джерело, яке виступає об’єктом розвідки. На відміну від Maltego, де процес побудови аналітики значною мірою інтерактивний, SpiderFoot самостійно проводить глибоке сканування за понад 200 модулями (зокрема, пошук у витоках даних, чорних списках, WHOIS, SSL-сертифікатах, соціальних мережах, порт-сканування тощо). Користувач може задати IP-адресу, домен, e-mail або псевдонім, а результатом буде багаторівневий звіт із виявленими асоціаціями, ризиками, витоками, потенційними вразливостями. Однією з сильних сторін SpiderFoot є його вбудована система ризикових оцінок, яка надає кількісне уявлення про загрозу, пов’язану з об’єктом.

SpiderFoot має як веб-інтерфейс, так і CLI-режим, що дозволяє інтегрувати його в більші аналітичні системи. Його відкритий код дає змогу розгортати систему на локальних серверах та кастомізувати модулі, що критично для безпечних досліджень у приватному середовищі. Проте, як і у випадку з Recon-ng, ефективне використання SpiderFoot передбачає налаштування API-ключів для доступу до зовнішніх джерел, а також увагу до точності налаштувань сканів, аби уникнути надмірного навантаження або помилкових позитивних результатів.

Загалом, Maltego і SpiderFoot репрезентують два підходи до післязбірного аналізу OSINT-даних. Maltego — це платформа для ручного аналізу зв’язків з високим рівнем візуалізації, яка дозволяє будувати аналітичні сценарії у вигляді інтерактивного графа. SpiderFoot — це автоматизований сканер з аналітикою, що самостійно структурує дані в звіти та оцінює ступінь ризику. Обидва інструменти чудово доповнюють один одного й дають можливість аналітику

поєднати масштабність, швидкість і глибину дослідження в межах одного аналітичного циклу.

Таблиця 1.3

OSINT-інструменти для аналізу та візуалізації даних

Функція	Maltego	SpiderFoot
Тип ліцензування	Комерційна (Community, Professional, Enterprise); безкоштовна Community-версія	Відкритий код та платні Enterprise-редакції
Джерела даних	Понад 100 вбудованих трансформів (WHOIS, DNS, соцмережі, OSINT-API); власні плагіни через Hub	Більше 200 модулів збору (OSINT, Dark Web, геодані, API з Twitter, Shodan, Google, PGP тощо)
Візуалізація	Інтерактивні графи з вузлами та зв'язками; кастомні стилі/фарбування; можливість drill-down	табличні звіти; інтеграція з графовими СУБД через API
Інтерфейс користувача	GUI-додаток	Веб-інтерфейс та CLI;
Розширюваність	Створення власних трансформів на Python/Java; маркетплейс Marshal	Пишуть модулі на Python; легко додавати нові інтеграції та джерела даних
API та інтеграція	REST API для запуску трансформів, JSON-інтерфейс; інтеграція з Threat Intelligence платформами	Повний REST API; підтримка JSON/CSV вивантажень;
Звіти та експорт	Експорт графів у PDF/PNG, CSV-таблиці, Casefile;	Авто-генерація HTML/JSON/CSV звітів;
Підходить для	Глибинний аналіз зв'язків, складні розвідзадачі, інтеграція з аналітичними платформами	Швидкі масові сканування, автоматичні звіти, широке охоплення OSINT-джерел, бюджетні проєкти

Після застосування інструментів збору, обробки та візуалізації OSINT-даних наступним критичним етапом стає аналітичне осмислення отриманої інформації. Особливу увагу при цьому приділяють методам оцінки ризиків витоку даних, що дозволяють виявити потенційні загрози для безпеки.

Сьогодні інформаційний простір, це місце де відбувається відкрите або неконтрольоване поширення даних, через що виникає значна частина загроз, тому аналіз ризиків витоку інформації є надзвичайно важливим. У сфері OSINT цей процес перестає бути простою перевіркою фактів і перетворюється на міждисциплінарну практику, що інтегрує елементи лінгвістики, соціології, кібербезпеки та штучного інтелекту.

Одними з основних методів у цьому контексті є контекстний аналіз або аналіз соціальних зв’язків (Social Network Analysis, SNA) та сентимент-аналіз — кожен із них виконує унікальну функцію в комплексному моделюванні інформаційних ризиків.

Контекстний аналіз, як метод дослідження отриманої інформації, полягає у багатоаспектному осмисленні її змісту, джерела, мотивів публікації, цільової аудиторії та часу появи.

У контексті OSINT це не просто аналіз того, що саме було опубліковано, а як ця інформація вписується у ширше інформаційне поле. Дослідження витоків без урахування контексту — це ризик хибної інтерпретації: наприклад, документ із номерами телефонів, що з’явився у відкритому репозиторії GitHub, може бути застарілим або випадково залишеним, однак за певних умов він може вказувати на системну проблему безпеки, особливо якщо його супроводжують коментарі, свідчення або супутні витоки.

Контекстний підхід передбачає верифікацію джерела, перевірку часових маркерів, зіставлення з іншими інцидентами, а також врахування реакції користувачів, ЗМІ або офіційних представників організації. У науковому розумінні, цей метод базується на постулатах критичної дискурс-аналізу та теорії інформаційного поля, де ключовими є інтертекстуальність та значення в межах системи соціальних і комунікативних практик.

Другим важливим методом у структурі OSINT-аналітики виступає аналіз соціальних зв’язків, або SNA (Social Network Analysis), який надає інструментальний апарат для виявлення, картографування та інтерпретації взаємозв’язків між суб’єктами — як індивідуальними, так і колективними.

У разі ризику витоку інформації цей метод дозволяє відстежити, хто саме взаємодіє з потенційно небезпечним або сумнівним джерелом, з ким об’єкт має стійкі інформаційні зв’язки, у яких спільнотах бере участь, як часто та з якими темами виходить на публічний зв'язок. Завдяки цьому можливо виявити латентні структури, які не проявляються у формальних публікаціях, але формують основу для витоків або цілеспрямованого інформаційного тиску. Практична реалізація

методу можлива за допомогою таких інструментів, як Maltego, а на теоретичному рівні метод спирається на графову теорію, зокрема на концепти центральності, щільності мережі, міжкласової зв'язаності та когезії. Наприклад, за допомогою SNA аналітик може встановити, що низка акаунтів у Twitter, пов'язаних із темою витоку, мають спільне джерело координації або використовують однакову інформаційну архітектуру (ключові слова, хештеги, час публікацій).

Окрему роль у попередженні та виявленні інформаційних ризиків відіграє сентимент-аналіз — метод автоматизованої лінгвістичної оцінки емоційної тональності текстового контенту.

У контексті OSINT його значення полягає не лише у класифікації текстів за критерієм «негативний/нейтральний/позитивний», а в інтерпретації *трендів емоційного стану цифрового середовища* навколо певної події, організації або особи. Сентимент-аналіз дозволяє аналітику швидко локалізувати хвилю негативних згадок, ворожих висловлювань, ідентифікувати ризикові фрази або виявити агресивні кампанії. Так, у ситуації з витоком даних, поява ряду негативних коментарів у соціальних мережах, зростання інтенсивності критики або використання емоційно навантажених тригерів (наприклад, «злито», «продано», «небезпечно») може вказувати на реальний витік або навмисну кампанію з дискредитації. У практиці OSINT сентимент-аналіз реалізовується за допомогою NLP-модулів і бібліотек (наприклад, NLTK, TextBlob, spaCy), а також вбудовується у такі платформи, як SpiderFoot. Науково метод опирається на семантичну теорію поля, когнітивну лінгвістику та корпусну аналітику.

Усі три розглянуті методи є не ізольованими підходами, а компонентами єдиного аналітичного контуру, у якому OSINT перетворюється з простої техніки збору даних на інструмент стратегічного передбачення. Контекстний аналіз забезпечує глибину інтерпретації, SNA — структурну системність і виявлення зв'язків, а сентимент-аналіз — чутливість до емоційних імпульсів цифрового простору. Саме їх поєднання дозволяє сформувати обґрунтовану оцінку інформаційного ризику, що відповідає як практичним вимогам кібербезпеки, так і науковим стандартам інформаційного аналізу.

Таблиця 1.4

Методи аналізу в OSINT

Характеристика	Контекстний аналіз	SNA	Синтез-аналіз
Ціль	Оцінка змісту інформації у публічному контексті	Ідентифікація зв’язків між об'єктами в мережі	Поєднання даних із різних джерел для створення цілісної картини
Застосування	Аналіз вразливих згадок у відкритих джерелах	Аналіз контактів у соцмережах, спільної активності	Об'єднання результатів різних типів аналізу (контекстного, метаданих, гео, SNA)
Типи даних	Текстові публікації, коментарі, документи	Профілі соцмереж, email, IP, логіни	Агреговані дані з усіх OSINT-інструментів
Очікуваний результат	Виявлення інформації, що може становити ризик	Виявлення потенційних каналів витоку	Комплексна оцінка ризику, побудова профілю загрози, підготовка звіту

Висновки до розділу 1

У цьому розділі ми дізнались суть і призначення OSINT як ефективного методу збору відкритої інформації як для державних і приватних структурь та і для звичайних людей. Провели класифікацію джерел за доступністю та ризиками, та визначили що чітке формулювання задачі є ключем до результату, а також технічні навички, аналітичне мислення й етика при роботі з публічною інформацією.

Розглянуто витоки даних через неуважність працівників, помилки налаштувань або випадкове оприлюднення документів, зокрема в соцмережах, репозиторіях і реєстрах. Наведено також способи протидії такі як: цифрова гігієна, OSINT-аудити, навчання персоналу і постійний контроль зовнішньої інформаційної присутності.

Описано основні інстументи для роботи з відкритою інформацією (theHarvester, Shodan, Recon-ng) та візуалізацією її та її ризиків (Maltego, SpiderFoot), а також методи аналізу.

РОЗДІЛ 2. АНАЛІЗУ РИЗИКІВ ВИТОКУ ІНФОРМАЦІЇ ЧЕРЕЗ ПУБЛІЧНІ ДЖЕРЕЛА ЗА ДОПОМОГОЮ OSINT-ІНСТРУМЕНТІВ

2.1 Аналіз інформаційних витоків із відкритих цифрових джерел організаційної активності.

З визначення OSINT ми вже знаємо що в його основі лежать відкриті джерела. Для первинного аналізу підприємства ми обраємо найлегші та найрозповсюдженіші. В епоху тотального переходу до цифрових технологій таким джерелом стали соціальні мережі. На фоні цього виник окремий підвид який називається SOCMINT. Це специфічна в OSINT, що охоплює сукупність технік, технологій та інструментів для збору й аналізу публічно доступних даних із соціальних платформ. Вперше цей термін сформулював у 2012 році Девідом Омондом, Джеймі Бартлеттом та Карлом Міллером для дослідження впливу онлайн-комунікацій на безпеку [1]. Основною метою SOCMINT є одержання оперативної інформації про настрої та поведінку цільових аудиторій, виявлення трендів, соціальних мережевих зв’язків та потенційних загроз із публічних постів, коментарів, лінків й мультимедійного контенту [2] Основні переваги SOCMINT полягають у високій оперативності збору великих обсягів даних у реальному часі, можливості таргетованого моніторингу за географічною та демографічною ознаками, масштабованості аналітичних рішень і інтеграції з іншими джерелами OSINT для комплексної розвідувальної картини. Тож почнемо наші пошуки.

Оскільки Укрпошта є великою організацією то можна розпочати з професійної соцмережі LinkedIn де можна знайти інформацію про співробітників Загальний пошук почнемо з цього посилання: [3]

Аналіз публічних профілів працівників АТ «Укрпошта» у LinkedIn виявив низку серйозних ризиків для інформаційної безпеки. Велика кількість працівників, у тому числі спеціалісти з IT та кібербезпеки, мають відкриті

профілі, в яких зазначають не лише повне ім’я та прізвище, але й поточну посаду, технічну спеціалізацію (наприклад, DevOps, SOC analyst, керівник групи з доступу), а також місто проживання, геолокацію, список попередніх місць роботи та сфери відповідальності. В багатьох профілях прямо вказані назви технологій, з якими особа працює — Fortinet, MS Defender, Zabbix, Cisco ASA, Active Directory, SIEM, Microsoft Intune, а також згадуються сертифікати (наприклад, CEH, ISO 27001, Cisco, Fortinet NSE) і навіть хобі: шахи, дрони, футбол, кібербезпека, моделювання тощо. Часто профілі містять фотографії з офісу або корпоративних заходів.

Такий масив персональних і технічних даних дає зловмиснику майже повну інформацію, необхідну для побудови персоналізованої соціальної інженерії. Наприклад, знаючи ім’я, посаду та сферу відповідальності, зловмисник може підготувати лист нібито від імені керівника цього співробітника або від колеги з іншого департаменту. Посилаючись на реальний проєкт чи технологію, яка згадувалася в профілі (скажімо, “оновлення Zabbix”, “оновлення політик AD” або “доступ до VPN”), фішинговий лист виглядає достовірно. У разі, якщо згадується конкретна платформа, наприклад Fortinet або Cisco, — зловмисник може надіслати псевдооновлення з фальшивим VPN-клієнтом чи інструкцією з “авторизації” в Office 365, фактично спонукаючи до введення облікових даних.

Також ці профілі дозволяють непрямо зібрати карту всієї IT-інфраструктури компанії. Якщо вказано кілька співробітників, які працюють із Zabbix або Fortinet, можна зробити висновок, що відповідні продукти дійсно впроваджені в середовищі компанії. Це дозволяє підбирати актуальні CVE, орієнтуватися в типових налаштуваннях, підготувати payload або спланувати password spraying. У випадку згадок про MS Intune або Defender, можна здогадатися про централізовану політику керування кінцевими пристроями — і спробувати атакувати вузькі місця цих систем (наприклад, слабкі локальні облікові записи або відсутність MFA).

Окрему небезпеку становлять хобі й захоплення, які користувач публічно розкриває. Наприклад, якщо спеціаліст згадує про дрони, шахи чи футбол, це може бути використано як точка входу для контактної взаємодії. Фальшивий профіль або бот із подібним інтересом може ініціювати розмову, запросити в інше середовище (наприклад, Telegram-чат спільноти), а далі — поступово вибудовувати довіру. Крім того, такі деталі дозволяють визначити, хто в команді більш обережний, а хто схильний до емоційних реакцій — наприклад, при отриманні листа з позначкою "терміново", "CEO request", "накладна заблокована", "urgent IT task".

Нарешті, ці профілі дають змогу побудувати карту персоналу: зрозуміти, хто ким керує, хто з ким має професійні зв’язки, і відповідно — які ланки в організаційній структурі найбільш вразливі до фішингу, соціальної інженерії або навіть фізичного контакту (наприклад, через конференції чи виставки). Все це разом створює ідеальне інформаційне середовище для атак типу CEO fraud, targeted phishing, або складних pretext-атак.

Зокрема був одни показовий приклад з наступним співробітником: [4]

Аналіз його профілю дозволяє зловмисникам виявити вразливості та розробити вектори атаки. У профілі детально описано його обов’язки, досвід та технології, з якими він працює. Зокрема, він згадує про адміністрування серверів на базі Windows Server, створення політик доступу через Active Directory та GPO, організацію віддаленого підключення через IPSec VPN із використанням FortiGate, а також супровід бухгалтерських баз BAS/1C. Додатково вказано, що він відповідає за моніторинг працездатності систем через Zabbix і використання SNMP, а також бере участь у налаштуванні резервного копіювання даних.

На перший погляд це типовий опис того з чим людина працює, але з точки зору OSINT це майже повна карта критичної частини інфраструктури. Наприклад, згадка про Zabbix у поєднанні з SNMP свідчить про використання моніторингової системи, яка в багатьох організаціях за замовчуванням має відкритий веб-інтерфейс, а SNMP може бути налаштований на спільне використання без обмежень доступу ззовні. Якщо немає фаєрволів або

правильної ізоляції, це відкриває можливість як мінімум — зчитування внутрішніх параметрів, як максимум — ескалацію атак через відомі CVE.

Згадка про підтримку BAS також вказує на потенційне джерело вразливостей. Ці системи часто розгортаються локально, в ізольованому середовищі без регулярного оновлення. У поєднанні з тим, що зловмисник вже знає, що BAS використовується, і що облікові записи типу admin можуть існувати, відкривається вікно для атак через брутфорс, соціальну інженерію або зараження під виглядом “оновлення бухгалтерської системи”.

Особливу небезпеку несе згадка про IPSec VPN на FortiGate. Якщо зловмисник ідентифікує, яка версія FortiOS використовувалась в роки, коли ця особа почала працювати (наприклад, 2022–2023), він зможе перевірити її на відомі вразливості. Історично відомо, що версії типу 6.0.7 або 6.2.3 мали критичні вразливості, які дозволяли або обхід автентифікації, або витоки конфігурацій. Таким чином, навіть згадка про конкретну технологію VPN — це підказка для глибокої технічної розвідки, включаючи сканування зовнішнього периметра на предмет відкритого FortiGate-порту, підбір версії через банери та експлуатацію вразливостей.

Окремо варто зазначити, що профіль містить часові рамки роботи у двох компаніях, що дозволяє точно визначити, з якого періоду ця особа має доступ до критичних систем Укрпошти. Зловмисник може використовувати цю інформацію для формування списку цілей, наприклад, у стилі "exposure mapping" — відстеження технологій, впроваджених під час каденції певного працівника.

У сукупності, такий відкритий профіль не лише розкриває внутрішню інфраструктуру компанії, але й дозволяє сформувати сценарій цільової атаки, використовуючи реальні технологічні прив’язки. Цей приклад підкреслює, наскільки важливо працівникам критичних департаментів бути обережними у публікації професійної інформації в соцмережах.

Сьогодні організацій звертають багато уваги на безпеку інформаційних активів, що знаходяться в їхній внутрішній мережі, але мало хто дбає про інформацію, яка може бути розміщена або доступна у відкритих джерелах і

містить інформацію про них. Однак саме ця інформація може допомогти зловмисникам обійти засоби захисту інформації (ЗЗІ). Навіть непрофесіонали можуть використовувати вільно поширювані інструменти для пошуку, здавалося б, конфіденційної інформації про конкретних осіб та організації.

Компанія Укрпошта впровадила практику використання OSINT з метою запобігання ризику витоку даних та побудови більш ефективної системи кіберзахисту. Було визначено, що значна частина ризиків пов’язана з інформацією, доступною у відкритих джерелах, яка може використовуватись зловмисниками для атаки на компанію.

Наступна мережа це Facebook [5]. У випадку Укрпошти корпоративна сторінка у Facebook стала прикладом того, як, навіть прагнучи зробити корисні для клієнтів дописи, організація ненавмисно створює сприятливе середовище для зловмисників. Наприклад, в одному з дописів компанія повідомила про масштабний технічний збій, що стався у партнерських службах, через який не працює авторизація клієнтів через застосунок «Дія». Звертаючись до клієнтів, компанія порадила брати з собою паспорт для проходження альтернативної ідентифікації, вказавши, що не всі картки наразі приймаються терміналами.

Хоча така публікація першочергово мала на меті інформування клієнтів, вона також відкриває можливість для зловмисників провести атаки, маскуючись під реальною ситуацією. В умовах загальної напруги, нестабільності та зниженого рівня пильності серед користувачів, зловмисник може розповсюджувати SMS або листи з повідомленнями на кшталт: «Ваша особа не була підтверджена через Дію. Для завершення верифікації надайте копію паспорта або ІПН за посиланням…». Використовуючи домен, схожий на офіційний (наприклад, verify-ukrposhta.net), фішинговий сайт може маскуватися під форму входу до облікового запису або систему перевірки картки. Зниження рівня довіри до цифрових каналів під час інцидентів — ідеальне середовище для атак Smishing і Spear Phishing. Реальна комунікація з боку Укрпошти виступає легітимізуючим фоном для фейкових повідомлень: користувач бачить офіційний

пост, і тому легше вірить SMS із подібною інформацією, особливо якщо зловмисники імітують стиль повідомлень служби підтримки.

Ще один аспект загрози походить від фото, які трапляються в тих самих постах, або поширюються окремо працівниками Укрпошти. На деяких із них можна побачити співробітників у формі, бейджики на грудях, а іноді — навіть елементи внутрішньої інфраструктури.

Використовуючи видимі бейджики, зловмисник може зробити дублікат — або використати побачене ПІБ для impersonation-атаки. Наприклад, зателефонувати до відділення, представитись внутрішнім співробітником, і, прикриваючись технічними складнощами, надіслати файл нібито для оновлення терміналів. Якщо на фото присутній внутрішній простір відділення і його адреса, інформації достатньо аби зловмисник зміг встановити, яке саме це приміщення, і визначити, хто в ньому працює. Надалі це дозволяє реалізувати фізичне проникнення: назватися кур'єром, стажером, спеціалістом технічного обслуговування і, маючи базову легенду та знання внутрішнього контексту, непомітно проникнути в простір, що має обмежений доступ. Навіть просте знання імені чи посади співробітника в комбінації з реальною адресою дає змогу створити фішинг або візит, що виглядатиме правдоподібно.

Таким чином, корпоративна Facebook-активність Укрпошти створює низку непрямих, але небезпечних інформаційних векторів. У публічних комунікаціях одночасно присутні ознаки технічної несправності, заклики до дій, а в персональних профілях зображення та ознаки просторової організації об’єктів. Для зловмисника це ідеальні умови для побудови атак з високим рівнем довіри. Тому навіть некомерційні й на перший погляд нейтральні соцмережеві пости повинні підлягати внутрішньому аналізу на предмет витоку контексту, який може бути використаний проти організації.

Проте не лише через Linkedin та Facebook можна дізнатись важливу інформацію для атаки. Хакери також використовують і платформи з працевлаштування такі як WorkUA чи схожі [6].

Під час моніторингу публічних вакансій, розміщених компанією «Укрпошта» на порталі Work.ua, а також через вивчення тематичних форумів, було виявлено низку інформаційних артефактів, які можуть бути використані потенційним зловмисником для побудови складної, багаторівневої соціальної інженерії, внутрішньої розвідки та навіть фізичного доступу до об’єктів організації.

Насамперед привертає увагу тот факт, що частина вакансій не містить чіткої згадки про офіційне працевлаштування. У поєднанні з повідомленнями на форумах, де кандидати діляться досвідом проходження співбесід чи працевлаштування в обхід офіційної процедури, це відкриває можливість для зловмисника діяти під прикриттям, прикинувшись кандидатом. У таких умовах він потенційно може пройти співбесіду, отримати внутрішню інформацію під виглядом нового працівника, або навіть проникнути до фізичних об’єктів компанії — відділень, технічних баз чи логістичних центрів. Таким чином створюється реальний ризик інсайдерської загрози, а сама практика непрозорого найму може завдати репутаційних втрат, якщо така інформація стане надбанням громадськості.

Ще більш критичним фактом є технічна деталізація, яка часто фігурує в описах посад для операторів, IT-адміністраторів, або водіїв інкасації. У текстах вакансій регулярно вказуються точні адреси відділень і логістичних центрів, де буде здійснюватися робота, а також згадуються конкретні типи обладнання та систем. Для зловмисника така інформація відкриває змогу побудувати географічну карту об’єктів Укрпошти, змоделювати можливі точки входу, оцінити рівень охорони та, при бажанні, спланувати фізичний візит до визначеного об'єкта під виглядом кандидата, підрядника або технічного спеціаліста.

Цінними для зловмисників є згадки про конкретні платформи, технології та інструменти, які використовуються в інфраструктурі компанії. У деяких вакансіях прямо вказується, що працівник повинен мати досвід з CRM-системами, програмним забезпеченням BAS ERP, Microsoft Office 365, а також

платіжними терміналами програмним забезпеченням, електронними касами, VPN, Active Directory тощо. Ці згадки фактично підтверджують використання відповідного стеку технологій в компанії, що дозволяє зловмиснику сформувати технічну модель середовища. Далі, використовуючи базу CVE (відомих вразливостей), він може підібрати експлойти до систем, які згадані в описах посад.

Особливу небезпеку становлять вже згадані атаки типу spear-phishing, які зловмисник побудує на основі отриманої інформації. Наприклад, знаючи, що в конкретному логістичному центрі використовується BAS, а адміністратором там працює людина, яку звуть Петро, фішинговий лист може виглядати як внутрішня комунікація: «Петре, просимо встановити термінове оновлення системи для вашої філії — інструкція у вкладенні». Під виглядом «офіційного» повідомлення буде надісланий шкідливий документ або файл, який запустить зловмисний скрипт.

Таким чином, навіть на перший погляд звичайна інформація у відкритих вакансіях насправді може бути використана для формування цілого вектору атак — від соціальної інженерії до підбору технічних експлойтів, а також як інструмент для проникнення в офлайн-середовище компанії. Це ще раз підкреслює важливість гігієни публічної комунікації у корпоративному середовищі та необхідність аналізу всіх відкритих каналів з погляду інформаційної безпеки.

Проте не соцмережами єдиними, реєстри та офіційні джерела також можуть містики корисну для зловмисників інформацію. Наприклад офіційний сайт: [7]

У розділі “Керівництво” [] опубліковані детальні відомості про топ-менеджмент компанії: прізвища, імена, посади, біографічна інформація, а в окремих випадках — навіть професійний досвід, пов’язаний з попередніми роботодавцями, напрямки відповідальності та сфери компетенцій. Ця інформація, будучи відкритою, безпосередньо не

порушує норми, однак може становити високий ризик з точки зору цільових фішингових атак, особливо у поєднанні з іншими публічними джерелами.

По-перше, зловмисник може використати ці дані для impersonation-атак, видаючи себе за когось із керівництва в комунікації з внутрішніми співробітниками.

По-друге, ці ж дані можуть бути використані для підробки офіційних документів або листів, що нібито підписані топ-менеджментом. По-третє, зловмисник може самостійно зібрати зв'язки між іменами керівників на сайті й профілями на LinkedIn або інших платформах. Це дає можливість побудувати цільові атаки через соцмережі, де будуть використані фейкові акаунти, створені на базі відкритої інформації.

Окремим етапом є аналіз судових рішень з використинням відкритих реєстрів наприклад [8]

У ході аналізу відкритих судових матеріалів, пов'язаних з діяльністю Укрпошти, були виявлені щонайменше три інциденти, що створюють критичні інформаційні вразливості. Перший випадок стосується витоку конфігураційної документації до систем BAS. У рамках справи, яка розглядає порушення контрактних зобов'язань з боку IT-підрядника, до судових матеріалів було прикладено повне технічне завдання та конфігураційні файли, які описували схему впровадження облікової системи. У цих файлах були виявлені IP-адреси серверів, які відповідають за обробку бухгалтерських даних, а також список облікових записів з ролями адміністраторів, операторів і обмежених користувачів — наприклад, admin, operator_bas, user_payroll.

Наявність такої інформації у відкритому реєстрі критично знижує рівень кібербезпеки підприємства, оскільки дає змогу зловмиснику не лише ідентифікувати версію програмного забезпечення і дізнатися, де фізично чи логічно воно працює, а й орієнтуватися у структурі прав доступу. Це створює передумови для цільового використання CVE (якщо версія BAS або 1C вразлива), брутфорс-атак за відомими логінами або навіть підробки клієнтських оновлень для зараження систем. Таким чином, судовий процес, що мав би

вирішити одні проблеми, неочікувано відкрив двері для інших, як наприклад можливость для технічної атаки на бізнес-критичні IT-ресурси.

Інший випадок стосується витоку персональної та службової інформації співробітника департаменту інформаційної безпеки. У справі щодо незаконного звільнення цей співробітник надав до суду копії внутрішньої документації, що регулює політику інформаційної безпеки компанії, а також опис власних обов'язків та переписку з керівництвом. Серед додатків опинилися: робочий email, контактний телефон, а також згадки про особисту пошту, яку працівник вказував у контексті зв'язку з HR. Ще більш небезпечною виявилась інформація про внутрішні технічні засоби моніторингу — згідно з текстом заяви, в організації використовується Zabbix для логування подій, а впровадження багатофакторної аутентифікації є неповним — тобто присутнє не на всіх системах.

По-перше, така інформація може бути використана для побудови надзвичайно переконливого фішингового сценарію. Зловмисник може видавати себе за колишнього працівника, відомого колегам, або за службу підтримки, використовуючи правдоподібну технічну лексику, внутрішню термінологію та навіть посилання на внутрішні політики, що з'явились у матеріалах справи. По-друге, сам колишній працівник, зважаючи на конфлікт, що стався, може стати джерелом інсайдерської загрози — маючи детальне уявлення про внутрішні ІБ-процеси, він може допомогти третім сторонам організувати атаку або виток даних.

Третя критична вразливість стосується фізичної безпеки: в іншій судовій справі, яка стосується крадіжки обладнання з логістичного центру Укрпошти, в матеріалах фігурував докладний опис умов, за яких відбулося проникнення. У документах зазначено, що в об'єкті не було нічної охорони, а також описано, який саме тип замків використовувався, як розташовані камери відеоспостереження, і яка зона огляду кожної з них. У додатках згадувалась і наявність Wi-Fi-підключення у технічному приміщенні — ймовірно, для

автоматичного передавання даних з POS-обладнання або серверів на центральні вузли.

Така деталізація дає можливість зловмиснику провести повноцінну розвідку фізичного периметра — наприклад, за допомогою Google StreetView, фізичного спостереження або навіть проникнення під виглядом постачальника. Враховуючи, що тип замків і схема спостереження вже оприлюднені, нападник може підібрати оптимальний шлях до проникнення з мінімальним ризиком бути зафіксованим. А за умов доступу до технічного обладнання — фізично інтегрувати скомпрометований пристрій у локальну мережу логістичного об’єкта або винести маршрутизатор, термінал чи навіть резервні носії.

Неочікувано але тендерні закупівлі обладнання також стали джерелом інформації для злочинців. Вакористовуючи сервіс: [9] на якому наша компанія, як суб’єкт публічних закупівель, регулярно публікує тендери. Серед них значну частку займають закупівлі, пов’язані з IT-інфраструктурою, системами безпеки та мережевим обладнанням. У відкритому доступі опиняються технічні специфікації, вимоги до постачальників, контактні дані відповідальних осіб, а іноді й додатки з технічними деталями, конфігураціями, описами систем — усе це становить цінну інформацію для потенційного зловмисника.

У процесі аналізу було виявлено, що Укрпошта закуповує серверне обладнання, джерела безперебійного живлення (UPS), дизельні генератори, а також проводить впровадження та обслуговування облікових систем, таких як BAS ERP, Active Directory і Microsoft Office 365. Окрім цього, значна частина тендерів стосується технічного обслуговування систем відеоспостереження та охоронної сигналізації, а також касового та термінального обладнання, яке встановлюється у відділеннях зв’язку.

Публікація такої документації, хоч і частково відповідає вимогам прозорості, створює потенційні вектори атаки. Одним з ключових ризиків є знову ж таки розкриття технологічного стеку. Зазначення конкретних версій програмного забезпечення або вимог до нього (наприклад, «впровадження BAS ERP у середовищі Windows Server 2016 з інтеграцією в AD») надає зловмиснику

інформацію для пошуку вразливостей (наприклад, через базу CVE), а також дозволяє підготувати шкідливе ПЗ, адаптоване до реального середовища цільової організації.

Наступним небезпечним фактором є наявність персональних даних IT-працівників у тендерних умовах — наприклад, контактних осіб, відповідальних за зв’язок з постачальниками. Часто зазначаються повні імена, посади, службові телефони, робочі email-адреси. Ці часто фігурують у фішингах спрямованих на внутрішніх співробіниківою. Зловмисник, видаючи себе за внутрішнього технічного партнера чи колегу з іншого відділу, може легко переконати жертву взаємодіяти з зараженим вкладенням або надати облікові дані.

Деякі тендери також розкривають частини мережевої інфраструктури — схеми розміщення обладнання, типи маршрутизаторів, вимоги до IP-адресації, протоколи зв'язку між вузлами. Знаючи такі деталі, досвідчений хакер може змоделювати реалістичний сценарій проникнення в систему або імітувати вузол в мережі.

Крім того, відкритий доступ до шаблонів договорів, офіційного листування та технічних актів може бути використаний для підробки документів. Створення фальшивих PDF-файлів із правдоподібним змістом дає змогу створити фішингову атаку в стилі «постачальник надіслав оновлення до 1С», яке насправді є зловмисним кодом.

Хоч відкриті закупівлі є необхідною умовою державної прозорості, завдяки ним може виникнути низка інформаційних небезпек, які суттєво підвищують ризик цільових атак, особливо з боку тих, хто має базові технічні знання або доступ до OSINT-інструментів.

Таблиця 2.1

Технології аналізу ризиків на “Укрпошті”

Джерело	Виявнена інформація	Ризик	Згадані технології	Технічний ризик(CVE)
LinkedIn	Імена, посади, хобі, стек технологій, фото, сертифікації	Spear phishing, карта персоналу, соціальна інженерія	Fortinet, Zabbix, AD, MS Intune, Cisco ASA	CVE у FortiOS, вразливі налаштування SNMP/Zabbix, слабкі політики AD
Facebook	Повідомлення про збої, фото співробітників з бейджами, адреси	Smishing, impersonation, фізичне проникнення	POS-термінали, термінальне ПЗ	Імітація службових повідомлень, вразливості у термінальному ПЗ
Work.ua	Опис вакансій, технології, адреси об'єктів	Insider threat, фізичний доступ, технічне моделювання	1C, BAS, Office 365, AD, VPN	Вразливості BAS/1C, фішингові сценарії під виглядом оновлення
Офіційний сайт	Керівництво, посади, сфери відповідальності	Impersonation, підробка документів, phishing	—	—
Судові рішення	IP, логіни, email-и, технічне ТЗ	CVE-атаки, insider threat, доступ до систем	BAS, 1C, Zabbix, AD, VPN	CVE Office, AD, відомі IP та конфігурації
Prozorro	Технічні специфікації, email-и, конфігурації	Phishing, CVE-пошук, доступ до карт мережі	BAS, 1C, AD, Office 365, мережеве обладнання	CVE Office, AD, відомі IP та конфігурації

2.2. Аналіз технік розвідки за MITRE ATT&CK: тактики противника в OSINT.

Задля уникнення таких сценаріїв Укрпошта вирішила частково впровадити використання матриці MITRE ATT&CK, яка дозволяє виявляти типові методи розвідки, адже вона є однією з початкових стадій кібератак, під час якої зловмисники здійснюють збір відкритої інформації про ціль. MITRE ATT&CK –

відкритий, аналітичний фреймворку, який узагальнює знання про поведінку зловмисників та класифікує їхні тактики і техніки відповідно до фаз атак. На відміну від класичних стандартів він орієнтований не лише на засоби захисту, а й на розумінні самого алгоритму дій порушників, що дозволяє моделювати реальні сценарії вторгнення та своєчасно реагувати на них. Основну увагу було зосереджено саме на фазі розвідки оскільки саме на ньому використовується OSINT як основний спосіб отримання даних про компанію. Розглянемо впроваджені методики MITRE ATT&CK в Укрпошті.

Серцем майже будь якої організації є мережа, тому частіше за все саме звідси все і починається. Хакери можуть сканувати списки IP-адрес жертв, щоб потім використати під час підготовки. Такі дії дозволяють зібрати інформацію про мережу жертви, наприклад, які IP-адреси активно використовуються, а також більш детальну інформацію про хости, яким присвоєні ці адреси. Сканування може варіюватися від простого пінгу (ICMP запитів і відповідей) до більш складних сканувань, які можуть виявити програмне забезпечення/версії апаратури через банери серверів або місцезнаходження інтернет-провайдера. Інформація з цих сканувань може виявити можливості для інших форм розвідки (наприклад, пошук відкритих веб-сайтів/доменів або пошук відкритих технічних баз даних), створення оперативних ресурсів (наприклад, розробка можливостей або отримання можливостей) та/або початкового доступу (наприклад, зовнішні віддалені служби). [10]

Подібний приклад був зафіксований коли угроповування «Солнцепек», яке займається атаками проти українських урядових і телекомунікаційних структур, визначив діапазони IP-адрес для сканування вразливостей, пов'язаних з цією організацією. [11]

Для виявлення подібних сканувань було використано декілька методів, зокрема фільтрування вмісту мережевого трафіку. Такий моніторинг трафіку допомагає виявити шаблони, пов'язані з активним сканування. Включачи виявлення повторних спроб підключення, незвичної поведінки сканування або активності, спрямованої на декілька IP-адрес у мережі.

Щоб уникнути таких інцидентів рекомендується використовувати засоби контролю такі як Network Intrusion Detection Systems (NIDS) для виявлення аномальних сканувальних активностей, та сегментацію мережі для обмеження доступу до критично важливих елементів мережевої інфраструктури. Оскільки це сканування ґрунтується на діях, що виконуються поза межами системи захисту та контролю підприємства. Зусилля слід зосередити на мінімізації обсягу та чутливості даних, доступних зовнішнім сторонам.

А перед доступом до мережі потрібно подолати її захисні бар'єри. Під час визначення IP-адрес також можна вивідати й інформацію про налаштування захисту інтранету що дасть нападникам можливість визначити наявність та особливості розгорнутих брандмауерів, контент-фільтрів та проксі-серверів/бастіонних хостів. Також ціллю стануть системи NIDS або інші пристрої, пов'язані з кібероборoною. Дістати її можна різними способами, наприклад онлайн або інші доступні набори даних (наприклад, пошук на веб-сайтах, що належать жертвам).

Зусилля для стримання цієї атаки дуже схожі з попереднім пунктом, можна лише додати використання рішень SIEM/UEBA оскільки сканування буде сильно відрізнятися від звичайного трафіку та його буде легко виявити. На додачу до цього можна розставити по мережі Honeypots які будуть імітувати слабкі засоби безпеки вводячи в оману нападників.[12]

Після визначення топологій мережі переходять до розвідки DNS-структури. Основні методи це запити серверних імен організації або шукати через централізовані сховища зареєстрованих відповідей на DNS-запити (так званий пасивний DNS). Зловмисники також можуть шукати і використовувати неправильні конфігурації/витоки DNS. Вони можуть містити різноманітні дані, зокрема зареєстровані сервери імен, а також записи, які описують адресацію субдоменів, поштових серверів та інших хостів жертви. [13] Зловмисники ще часто використовують ресурс WHOIS де може бути інформацію про жертв, яка також буде використана. Дані WHOIS зберігаються в регіональних інтернет-реєстраторах (RIR), які відповідають за розподіл і присвоєння інтернет-ресурсів,

таких як доменні імена. Будь-хто може звернутися до серверів WHOIS за інформацією про зареєстрований домен, наприклад, про призначені блоки IP-адрес, контактну інформацію та сервери імен DNS [14]

Дізнавшись цю інформацію хакери можуть використовувати базавоні на DNS атаки наприклад DNS Spoofing або DNS Hijacking перенаправляючи користувачів на фішингові сайти або просто зробити недоступними внутрішні сервіси компанії. Ще одним неприємним інцидентом може бути моніторинг злочинцями DNS трафіку як між користувачами так і між доменами.

Протидіяти цьому нелегко проте цілком можливо. Першим потрібно впровадити моніторинг DNS запитів через SIEM та аудит змін в пакетах. Різка зміна маршрутизації на якийсь на=овий чи невідомий домен може цілком бути ознакою вторгнення. Для закріплення результатів можна інтегрувати DNSSEC, який буде доповнювати функціонал стандартного DNS та перевіряти цілісність відповідей та забезпечить аутентифікацію клієнтів.

Паралельно з цим може проводитись і виявлення фізичного розташування об’єкту. На відміну від інших параметрів розвідки, цей може бути просто вказаний на сайті. Проте інколи через некоректні налаштування проксі чи WAF може «світитися» і IP-адреса. Проте з якою легкістю цю інформацію можна знайти, так само легко цього можна і уникнути. Просто прибравши із сайту згадки про розташування та фото, а також з правильними налаштуваннями пристроїв виявлення локації буде не такою вже й легкою ціллю. [15]

Наступне за чим полюють хакери це інформація про апаратне забезпечення компанії, ці дані також можуть бути використані під час атаки. Інформація про апаратну інфраструктуру може включати різноманітні деталі, такі як моделі та версії на конкретних пристроях, а також наявність додаткових компонентів, які можуть свідчити про додаткові засоби захисту (наприклад спеціальне шифрувальне обладнання тощо). Зловмисники можуть збирати цю інформацію різними способами, наприклад, наприклад за допомогою попередньо згаданого сканування або фішингу для отримання інформації. Зловмисники також можуть скомпрометувати сайти, а потім розмістити на них шкідливий контент,

призначений для збору інформації про обладжнання відвідувачів. [16] Інформація про апаратну інфраструктуру також може стати доступною для зловмисників через Інтернет або через оголошення про вакансії, мережеві карти, звіти про оцінку, резюме або тендери на купівлю. Збір цієї інформації може відкрити можливості для інших форм розвідки, створення оперативних ресурсів (наприклад, розробка або отримання засобів для проникнення) та/або початкового доступу (наприклад модифікація обладнання яке може бути використане для отримання доступу). [17]

Цей метод нелегко нейтралізувати, оскільки вона базується на діях, що виконуються поза межами системи захисту та контролю підприємства. Проте виявити його можна за допомогою внутрішнього сканування, його можна використовувати для пошуку шаблонів, пов'язаних зі зловмисним контентом, призначеним для збору інформації про апаратне забезпечення машин. Значна частина цієї активності може мати дуже високу частоту появи і пов'язану з нею частоту помилкових спрацьовувань, а також потенційно відбуватися за межами видимості організації, що створює додаткові складнощі для її виявлення операційними центрами.

Зловмисники обов’язково шукатимуть інформацію про жертв у вільно доступних онлайн-ресурсах таких як: технічних базах даних, яка може бути використана під час нападу. Інформація про жертв може бути доступна в онлайнових базах даних і сховищах, таких як , наприклад, реєстрації доменів/сертифікатів, а також публічні колекції мережевих даних/артефактів, зібраних з трафіку та/або сканування. Зловмисники можуть шукати інформацію про вже ідентифіковані цілі або використовувати ці набори даних, щоб знайти можливості для успішних порушень. [18]

Такий же метод постійно використовує китайська група APT41 під час атак на охорону здоров'я, телекомунікації, технології, фінанси, освіту та роздрібну торгівлю у понад 14 країнах світу. [19]

Цю техніку неможливо ефективно усунути за допомогою превентивних засобів контролю, оскільки вона базується споза межами системи захисту та

контролю підприємства. Зусилля слід зосередити на мінімізації обсягу та чутливості даних, доступних зовнішнім сторонам.

Оскільки сучасне життя неможливе без соціальних мереж то і вони стали незамінним для розвідки. Пошук здійснюється на різних сайтах соціальних мереж залежно від того, яку інформацію вони потрібно зібрати. Зловмисники можуть пасивно збирати дані з цих сайтів, а також використовувати зібрану інформацію для створення фейкових профілів/груп, щоб змусити жертву розкрити певну інформацію (наприклад внутрішню мережеву структуру). Інформація з цих джерел може відкрити можливості для створення фішингу для отримання додаткової інформації. [20]

Такий підхід використали Lazarus Group для реалізації власної операції Dream Job. Вони використовувала LinkedIn для ідентифікації та націлювання на співробітників обраної організації [21]

Сьогодні використання репозиторіїв стало незамінним для кожного підприємства. Тому і вдкриті сховища коду стали жертвами розвідок. Компанії можуть зберігати код у репозиторіях на різних сторонніх веб-сайтах, таких як GitHub, GitLab, SourceForge та BitBucket. Користувачі зазвичай взаємодіють зі сховищами коду через веб-додатки або утиліти командного рядка, такі як git. Там вони шукають різну інформацію про жертву. Репозиторії можуть бути джерелом різної загальної інформації про жертву, наприклад, часто використовувані мови програмування та бібліотеки, а також імена співробітників. Зловмисники також можуть виявити більш конфіденційні дані, включаючи випадковий витік облікових даних або ключів API.

Щоб уникнути подібних ситуаціх потрібно перевіряти публічні сховища коду на наявність відкритих облікових даних або іншої конфіденційної інформації перед внесенням змін. Переконайтеся, що всі витоки облікових даних видалено з історії коммітів, а не лише з поточної останньої версії коду. Розробники додатків, які завантажують код до загальнодоступних сховищ коду, повинні бути обережними, щоб не публікувати конфіденційну інформацію, таку як облікові дані та ключі API. [22]

Кожна організація сьогодні має власний сайт в інтернеті в тому чи іншому вигляді. Якщо вони створені неграмотно то стають золотою жилою для зловмисників. Веб-сайти, що належать жертвам, можуть містити різноманітну інформацію, зокрема назви відділів/підрозділів, фізичне місцезнаходження та дані про ключових співробітників, такі як імена, посади та контактна інформація (наприклад, адреси електронної пошти). Ці сайти також можуть містити інформацію про ділові операції та зв'язки [23].

Окрім ручного перегляду веб-сайту, хакери можуть намагатися виявити приховані каталоги або файли, які можуть містити додаткову конфіденційну інформацію або вразливий функціонал. Вони можуть робити це за допомогою автоматизованих дій, таких як сканування списку слів, а також використовуючи такі файли, як sitemap.xml та robots.txt [24]

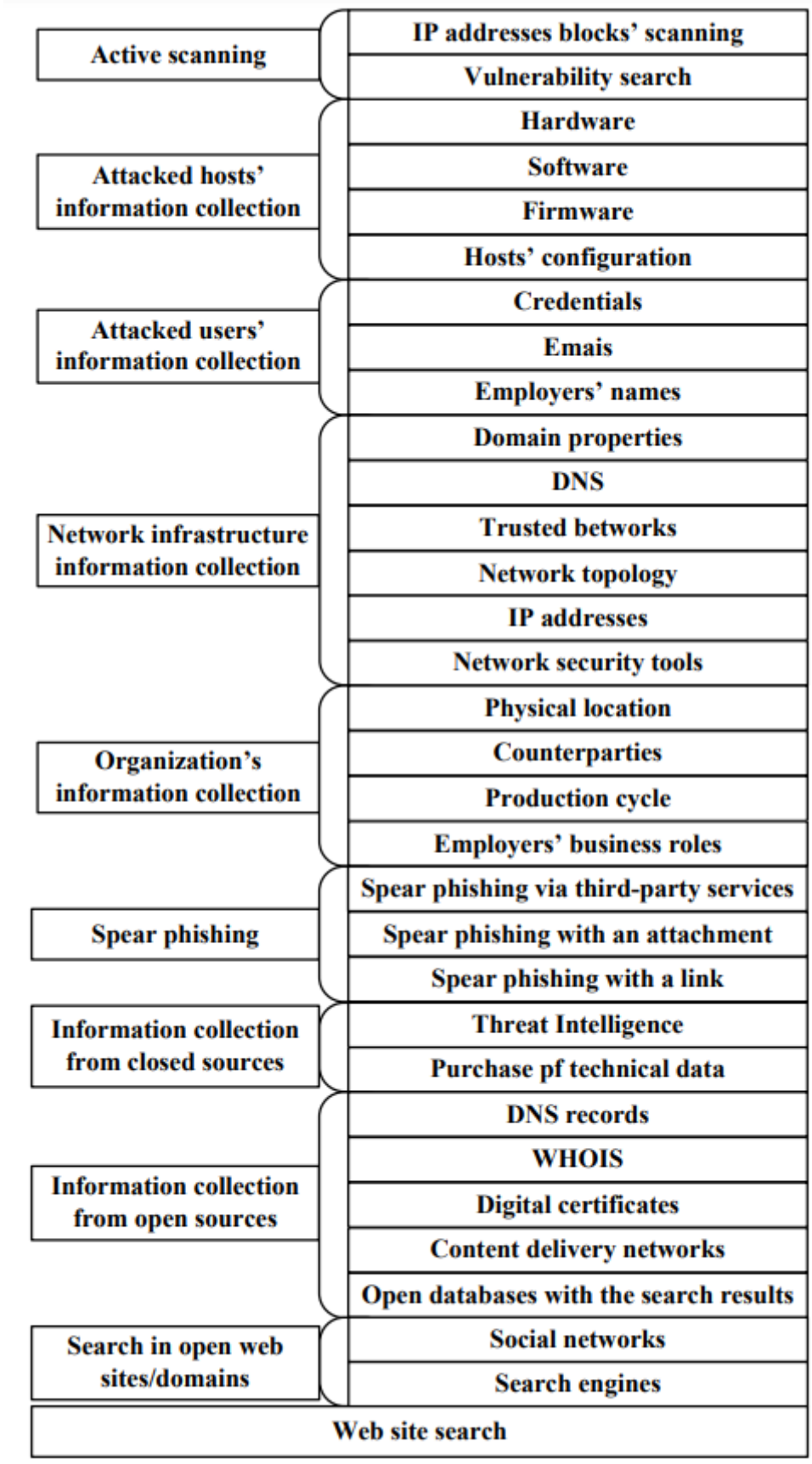

Рис. 2.1. Види технік розвідки

Щоб попередити можливість використання цього методу відстежуйте підозрілий мережевий трафік, який може свідчити про розвідку супротивника, наприклад, швидкі послідовності запитів, що вказують на веб-сканування та/або велику кількість запитів, що надходять з одного джерела (особливо якщо відомо, що джерело пов'язане з супротивником). Аналіз веб-метаданих також може виявити артефакти, які можуть бути пов'язані з потенційно зловмисною діяльністю, наприклад, поля HTTP/S рядка реферала або користувача-агента. [25]. Короткий опис цих всіх методів наведений у табл. 2.2.

Таблиця 2.2

Види технік відповідно до MITRE ATT&CK

Назва	Опис	Приклад	Контрзаходи
Scanning – Network	Виявлення активних IP/портів, банери сервісів	«Група Солнцепек» сканувала діапазони IP Укрпошти	NIDS/IPS, сегментація мережі
Active Scanning – Vulnerability Scanning	Автоматизоване сканування на відомі вразливості	Зловмисники перевіряли FortiOS на CVE	SIEM/UEBA, honeypots
DNS – Passive DNS	Пасивний аналіз DNS-запитів	Перегляд записів WHOIS для доменів ukrposhta.ua	DNSSEC, моніторинг змін DNS у SIEM
DNS – WHOIS Queries	Запити до WHOIS-серверів	Визначення контактів та IP-блоків	Обмеження доступу до реєстрів, проксі/WAF
Physical Location Tracking	Виявлення географії об’єктів через фото, WAF-логи	Знімки філій Укрпошти з адресами	Приховування адрес, геолокаційні проксі
Social Media – User Profiles	Збір даних із соцмережі (інтереси, хобі, фото)	Аналіз профілів LinkedIn та Facebook	Політика «мінімума даних» в профілях співробітників
Web – Search Open Websites/Domains	Автоматичний пошук прихованих файлів/каталогів на веб-сайті	Сканування robots.txt, sitemap.xml	Обмеження індексації, WAF-правила

2.3 Аналіз ризиків інформаційної безпеки підприємства на основі відкритих джерел за методологією FAIR

Моніторинг джерел насправді дуже ресурсозатратний процес, особливо в бік людського ресурсу. Адже сидіти цілими днями і дивитися на тисячі рядків інформації які прогортуються перед очима дуже складно. Окрім цього можна пропустити якісь інформацію в силу обставин чи людського фактору. І тут нам на допомогу спеціально розроблені для OSINTу інструменти для моніторингу та пошуку інформації. Розглянемо інстументи які ми використали у попередніх дослідженнях.

Першим буде Social Searcher [30]. Він допомгає в моніторинг соціальних мереж та зборі інформації про репутацію брендів, поведінку користувачів та оперативне виявлення загроз. Будучи одним із найпопулярніших інструментів для таких завдань цей безкоштовний пошуковий сервіс, який дозволяє відстежувати публічні згадки в реальному часі в різних соціальних мережах і на веб-ресурсах. До основних можливостей можна віднести уніфікований пошук який підтримує запити по ключовим словам або фразам одразу в 11 джерелах — Інтернет, Facebook, Twitter, LinkedIn, YouTube, Instagram, Tumblr, Reddit, Flickr, Dailymotion. Фільтри запитів надає можливість уточнювати пошук, використовуючи виключення термінів командою minus keywords, а також логічні оператори такі як OR для уточнення результатів. Щоб не пропустити важливі оновлення можна налаштувати автоматичні сповіщення. Також можна створити певні патерни в соцмедіа щоб вони регулярно оновлювали інформацію та отримувати сповіщення про це на e-mail. Щоб полегшити роботу та зіюрати все в одному місці є налаштовуваний аналітичний дашборд. Він збирає статистику за згадками, відображає динаміку згадок, тональність та популярні хештеги, а також дозволяє експортувати звіти у вигляді діаграм і таблиць. Поєднання цих всіх функції та доступність і робить його цінним для фахівців які займаються OSINT.

OpenDataBot [31] — це універсальний сервіс для оперативного пошуку й аналізу відкритих держреєстрів України. Його перевагами є агрегація даних та пошук інформації одночасно в понад 20 реєстрах: ЄДРПОУ (компанії та ФОП), судових рішеннях, майнових правах, банківських заборгованостях тощо. Один запит — комплексний результат із різних джерел. Як і в попередньому тут можна налаштувати сповіщення про зміни які будуть миттєво приходити у вигляді повідомлень (Telegram, Viber, email або веб-чат) про реєстрацію нових компаній, зміну складу засновників, появу/зняття нерухомості та відкриття чи закриття судових справ. Для більшої гнучкості він розроблявся мультиінтерфейсним, тобто зручний веб-портал, чат-боти в Telegram/Viber, мобільні PWA-додатки для iOS та Android, а також RESTful API для інтеграції з CRM, ERP чи BI-системами. Аналітика та формування детальних звітів: історія змін, графіки появи або закриття об’єктів, динаміка судових проваджень у зручних вам форматах експорт у PDF, Excel або JSON для подальшої обробки. А завдяки автоматизованому виявленню зв’язків між особами та компаніями, аналіз ланцюжків бенефіціарного володіння, верифікація власників і керівників OpenDataBot прискорює перевірку контрагентів, розслідування рейдерства, аналіз судових справ і моніторинг нерухомості, роблячи процес збору відкритої інформації простим, швидким і надійним.

Clarity Project [32] — це спеціалізований OSINT-інструмент для аналізу тендерних закупівель в Україні, що об’єднує всі ключові функції в єдиному інтерфейсі. Він надає потужний повнотекстовий пошук за який підтримує точні фрази, булеві оператори та виключення термінів, що істотно прискорює знаходження релевантних документів. Набір гнучких фільтрів і категоризації дозволяє сортувати результати за датою, її статусом, замовником чи учасником тендеру. Вбудований перегляд документів дає змогу миттєво ознайомитися з повними текстами рішень тендерних комісій і завантажувати їх у форматі PDF для подальшого аналізу. Чи не найважливішим елементом будуть — аналітичні дашборди, які візуалізують статистику дозволяючи створювати глибокі звіти та графіки для презентацій і розслідувань. А зручна інтеграція REST API з JSON-

інтерфейсом відкриває можливості програмної інтеграції в CRM, ERP чи SIEM-системи, автоматизації завантаження даних і налаштування власних сповіщень. Завдяки такій комплексній архітектурі Clarity Project допомагає вчасно виявляти ризикові тендери, документувати кожен крок та приймати обґрунтовані рішення на основі глибокого аналізу відкритих даних

Переглянути ці інструменти можна в таблиці 2.3

Таблиця 2.3

Інструменти OSINT для моніторингу та їх основні характеристики

Інструмент	Опис і функції	Джерела даних	Формати сповіщень	Застосування
Social Searcher	Моніторинг згадок у 11 соцмережах, аналітика тональності	Facebook, Twitter, LinkedIn, Reddit тощо	Email, дашборд	Швидке виявлення негативу та трендів
OpenDataBot	Аггрегація держреєстрів (ЄДРПОУ, суди, майно тощо)	20+ реєстрів України	Telegram, Viber, API	Перевірка контрагентів, рейдерство
Clarity Project	Аналітика тендерів, вбудований перегляд документів	Prozorro	PDF, Excel, REST API	Аналіз закупівель, ризик-тендери

Для аналізу ризиків була прийнята методологія FAIR (Factor Analysis of Information Risk) [33] — це відкрита кількісно-орієнтована модель для оцінки інформаційних ризиків. Вона дозволяє перейти від суб’єктивних суджень до прозорої, підзвітної оцінки ймовірності та величини втрат. У контексті Укрпошти застосування FAIR із використанням даних лише з OSINT забезпечує системний підхід до вимірювання ризиків, пов’язаних із публічно доступною інформацією. Її розробив Джек Джонс у середині 2000-х років, щоб забезпечити кількісний та прозорий підхід до аналізу інформаційних ризиків. Її ключові ідеї були інтегровані до міжнародного стандарту ISO/IEC 33030:2017, що підтверджує визнання та універсальність FAIR у галузі управління ризиками. FAIR полягає в тому, щоб чітко розбити інформаційний ризик на взаємопов’язані компоненти — загрози, вразливості та можливі втрати — й описати їх в єдиній структурі. Використовуючи кількісний підхід, FAIR дозволяє порівняти різні

ризикові сценарії за вірогідністю та очікуваним розміром збитків. Це дає змогу обґрунтовано пріоритизувати заходи з безпеки, спрямовуючи ресурси туди, де вони принесуть найбільший ефект у зниженні загальних витрат. Вона розглядає інформаційний ризик як сукупність взаємопов'язаних компонентів, що дозволяє чітко і кількісно оцінити вплив кожного з них. Перший компонент, Asset Value, визначає цінність інформаційного чи бізнес-активу для організації, враховуючи потенційні витрати при його компрометації. Threat Event Frequency (TEF) вимірює, як часто виникають події-джерела ризику (наприклад, знахідки через OSINT), здатні призвести до втрат. Vulnerability (Vuln) показує ймовірність того, що кожна така загроза справді спровокує інцидент, а Loss Event Frequency (LEF) обчислюється як добуток TEF на Vuln і відображає очікувану кількість реальних випадків шкоди за певний період. Далі Primary Loss Magnitude (PLM) оцінює прямі фінансові витрати на розслідування, відновлення систем та компенсації, а Secondary Loss Magnitude (SLM) — непрямі збитки, такі як репутаційні втрати, штрафи й втрачені контракти. Сума цих двох показників утворює Loss Magnitude (LM), тобто загальну величину втрат від однієї успішної події. Нарешті, кінцевий показник Risk визначається як добуток LEF на LM і відображає очікувані грошові втрати за обраний період, що дозволяє організації пріоритизувати заходи безпеки та ефективно розподіляти ресурси.

Таблиця 2.4

Результати аналізу ризиків ІБ на основі відкритих джерел за методологією FAIR

Термін FAIR	Позначення в моделі	Опис	Розрахунок
Asset Value	—	Цінність активів (ПД клієнтів, інфраструктура тощо)	17 877 243 тис. грн
Primary Loss Magnitude (PLM)	PLM	Прямі витрати на одну подію	≈4000-10000 тис. грн.
Secondary Loss Magnitude (SLM)	SLM	Репутаційні та регуляторні втрати	≈9% від Asset Value = 1 608 951 тис. грн
Loss Magnitude (LM)	LM	PLM + SLM	1 612 951 тис. грн
Risk	Risk	LEF × LM — очікувані втрати за період	9 677 706 тис. грн

Згідно досліджень [25] середні репутаційні втрати досягають до 9% від вартості активів компанії [27]. А витрати після атак на розслідування та навчання персоналу із залучання зовнішніх партнерів для великих компаній будуть коштувати від 4 до 10 млн. грн.[26, 28]

Метою створення типології ризикових ситуацій є системне класифікування загроз витоку інформації (зокрема через OSINT) з метою розробки ефективних стратегій запобігання та реагування. Завдання полягають у визначенні ключових ознак таких ситуацій — джерела загрози, методу доступу, типу інформації та вірогідності її використання зловмисником; розробці моделі класифікації за ступенем чутливості даних; впровадженні параметрів оцінки ризику й рекомендованих заходів реагування; а також інтеграції цієї типології в корпоративні процеси та системи SIEM.

За джерелом загрози ризикові ситуації поділяються на зовнішні (наприклад, публічні OSINT-інструменти та сторонні веб-ресурси) і внутрішні (помилки чи зловживання співробітників, некоректні налаштування прав доступу). За методом доступу розрізняють активний (навмисний збір даних через сканування, веб-краулінг) та пасивний (випадкове виявлення інформації, непомічені публікації або залишені документи). Тип інформації класифікується за трьома рівнями чутливості — низької (загальнодоступні відомості без прямої шкоди), середньої (внутрішня документація, технічні метадані) та високої (персональні дані співробітників, фінансові показники, стратегічні плани). І нарешті, вірогідність використання інформації зловмисником оцінюється як висока (оперативна можливість компрометації), середня (окремі фрагменти можуть бути корисними) або низька (слабка ймовірність реальних збитків).

Типологія передбачає виділення трьох рівнів ризику: низького (наприклад, публікація загальних презентацій на сайті компанії, що вимагає регулярної перевірки публічних ресурсів та аудитів), середнього (зокрема випадки з службовими документами на публічних хостингах, коли доцільне блокування доступу та перегляд політик обміну інформацією) і високого (витік

персональних даних співробітників чи комерційної таємниці, що потребує посилення контролю доступу та можливого звернення до правоохоронних органів).

Кожен інцидент вноситься до реєстру з такими параметрами, як джерело (OSINT або внутрішній аудит), тип загрози (технічна чи людино-орієнтована), потенційний вплив, рівень ймовірності, сценарій ескалації та рекомендовані дії реагування. На цій основі формується профіль ризику з урахуванням специфіки бізнесу й рівня цифрової присутності організації, який оновлюється регулярно на підставі реальних інцидентів і висновків аудиту.

Передбачається використання в автоматизованих системах SIEM. Типологія застосовується для фільтрації інцидентів за OSINT-критеріями (ступенем чутливості даних, джерелом витоку) та пріоритезації ризиків: інциденти високого рівня обробляються негайно, а аналітики отримують попередньо марковані події, що суттєво зменшує навантаження та підвищує швидкість реагування. Дашборди SIEM відображають статистику за частотою й типами подій, а також тренди за обраний період, що сприяє подальшому вдосконаленню політик безпеки.

Таблиця 2.5

Таблиця типологія за рівнями витоки –чутливість –вплив

Вектор витоку	Чутливість	Доступність	Потенційни вплив
Профілі в LinkedIn з технологічними деталями	Висока	Публічна	Targeted phishing, моделювання інфраструктури, злам через відомі CVE
Фото співробітників з бейджами та об'єктами	Середня	Публічна	Фізичне проникнення, підробка бейджів, доступ до відділення
Судові додатки з технічними деталями	Висока	Публічна (через реєстри)	CVE-атаки, втрата конфіденційності систем, компрометація
Тендерна документація з описом IT-систем	Середня	Публічна	Побудова фішингових сценаріїв, підбір CVE, атаки на постачальників

Таким чином, розроблена чітка та багаторівнева типологія ризиків ,що наведена в таблиці 2.5, забезпечує системний підхід до класифікації загроз,

оперативного реагування та планування превентивних заходів, поєднуючи організаційні та технічні інструменти в єдиній моделі управління інформаційною безпекою на підприємств

Висновки до розділу 2

У цьому розділі ми дізнались що у відкритих джерелах організаціїтаких як: соціальні мережі, портали працевлаштування, судові реєстри та тендерні майданчики можуть містити в собі поодинокі фрагменти інформації (імена співробітників, технологічний стек, IP-адреси, схеми доступу) дають змогу зловмисникам відтворити повну картину IT-інфраструктури та організаційної структури компанії. Це дає їм можливість для створення фішингових кампаній і соціальної інженерії, тому постійний моніторинг і керування присутністю в інфопросторі мають стати окремою ланкою інформаційної безпеки.

Для систематизації та виявлення найпоширеніших технік розвідки було впроваджено фреймворк MITRE ATT&CK. Сканування IP-діапазонів, дослідження DNS-записів і WHOIS-даних, аналіз соціальних мереж, відкритих репозиторіїв коду й веб-сайтів організацій – всі ці дії найчастіше передують активній фазі кібератак. Виявлення цих дій у мережевому трафіку дозволяє заздалегідь активувати превентивні механізми боротьби з розвідкою.

Для автоматизації OSINT-моніторингу використано інструменти Social Searcher, OpenDataBot і Clarity Project. Вони забезпечують цілий ряд плюсів: централізований пошук даних у різних каналах, налаштування сповіщень, побудову інтерактивних дашбордів та інтеграцію результатів у внутрішні системи. Регулярне використання таких сервісів знижує ручне навантаження на команду аналітиків і пришвидшує виявлення змін в інформаційному полі.

Для оцінки ризиків розроблено кількісну модель за методологією FAIR, адаптовану до використання OSINT. Ризики класифіковано за джерелом, чутливістю, доступністю й потенційним впливом інформації. Найвищий рівень мають LinkedIn-профілі з детальними технологічними відомостями, судові

документи з конфігураціями систем і тендерні матеріали зі згадками IT-інфраструктури. Інтеграція цієї моделі в SIEM-системи дозволяє автоматизувати пріоритезацію інцидентів та спростити процес управління ризиками в компанії.

РОЗДІЛ 3. МЕТОДИКА КОНСТРУЮВАННЯ АНАЛІЗУ РИЗИКІВ ВИТОКУ ІНФОРМАЦІЇ ЧЕРЕЗ ПУБЛІЧНІ ДЖЕРЕЛА ЗА ДОПОМОГОЮ OSINT-ІНСТРУМЕНТІВ

3.1. Конструювання алгоритму дій щодо інтерпретації відкритих даних із використанням спеціалізованих OSINT-платформ

Для того щоб вберегти наше підприємство від витоку даних в джерела відкритої інформації та забезпечити безперервність бізнес процесів потрібно розробити методичні підходи до практичної реалізації запропонованої моделі оцінки та управління ризиками витоку інформації через OSINT. Потрібно сформувати архітектуру для процесу автоматизованого моніторингу відкритих джерел, правильно налаштувавши інструменти та сповіщення які вони будуть надсилати. Потім завдяки використанню методологій FAIR і MITRE ATT&CK на їх основі розробимо алгоритм для обчислення ризику. Фінальним етапом буде коригування моделі під поточні вимоги та впровадження моніторингу результатів для того що забезпечити адаптивність методики до нових загроз і змін у кіберпросторі.

Почнемо з того що нам потрібно встановити чітке завдання та контекст щоб забезпечити максимальну ефективність збору та аналізу даних. Насамперед ми конкретизували мету: проаналізувати публічні профілі IT-персоналу компанії Укрпошта а предмет випадкових розкриттів внутрішньої інфраструктури та виявити потенційні «слабкі місця» в організаційній структурі і технологіях які вона використовує. Паралельно ми почали формулювати набір гіпотез, які стали основою наших пошукових сценаріїв, таких як: можливість знаходження внутрішніх IP-адрес у коментарях GitHub, випадкові згадки про конфігураційні файли у публічних блогах співробітників, а також витоки інформації через тендерні закупівлі в Prozorro. Ці припущення дозволять нам зосередитися на конкретних «тригерах» і налаштувати запити таким чином, щоб мінімізувати

хибні спрацювання і підвищити релевантність результатів. Щоб гарантувати стабільність і повторюваність процесу, ми чітко окреслили ресурси та обмеження. Аналітики використовують API Social Searcher і OpenDataBot для підключення до соцмереж та держреєстрів, а для збору тендерної інформації. Усі ці компоненти були формалізовані в єдиному технічному завданні в Confluence: опис мети, об'єктів, часових і територіальних меж, перелік гіпотез, перелік API та скриптів, а також критерії успішного завершення — мінімум 95 % покриття заданих гіпотез і відсутність дублікатів у зібраному масиві даних. Завдяки такому підходу ми отримали чітку дорожню карту для автоматизованого збору даних, що лягла в основу подальших етапів нормалізації, класифікації та ризик-аналізу. Ми реалізували модуль підбору й інтеграції інстументів, що забезпечив комплексний доступ до необхідних категорій відкритих даних. По-перше, для аналізу соціальних мереж ми налаштували API Social Searcher, який автоматично моніторить LinkedIn та Facebook, витягаючи інформацію за ключовими запитами (ім'я співробітника, назва проєкту, згадки технологій). Всі результати надходять у нашу централізовану шину подій у форматі JSON із атрибутами "джерело", "дата", "посилання" та "важливість". Для отримання даних із державних реєстрів ми використали OpenDataBot з його широкими можливостями інтегрування та доступу, зокрема до: єдиного держреєстру юридичних осіб, реєстру платників ПДВ, земельного реєстру. Запити виконуються із врахуванням обмежень в часі (кількість запитів на добу) і кешуються щоб мінімізувати навантаження й прискорити повторні запити. Це дає змогу миттєво дізнаватися про зміни в керівному складі, статутному капіталі та адресі компанії. Для збору інформації про тендери й закупівлі реалізовано скрапінг Prozorro та Clarity Project. Створені нами скрипти перевіряють нові лоти за ключовими словами (технологічний стек, назва компанії, прізвища менеджерів) і миттєво додають знайдені документи в чергу на попередню класифікацію. Ще одним джерелом даних стали судові рішення: за допомогою вбудованих запитів до court.opendatabot.ua ми отримуємо виписки з реєстру судових справ, де перевіряємо наявність позовів проти компанії чи її керівників. Ми налаштували регулярний «cron-job» із добовим

інтервалом, який додає нові записи до нашого сховища, а також верифікує наявні метадані (номер справи, дата, статус).

Усе це об’єднано в єдину мікросервісну архітектуру де кожен інструмент працює як незалежний сервіс із власною чергою повідомлень, а результати через потокову обробку передаються далі на етап нормалізації. Такий підхід забезпечує масштабованість і стійкість до збоїв: при недоступності однієї з платформ інші продовжують збір даних без затримок. Завдяки цьому ми отримали надійну, швидку та гнучку інфраструктуру для подальшого аналізу та класифікації відкритих даних.

На третьому етапі ми побудували потужний механізм формування та оптимізації пошукових запитів, який дозволяє отримувати максимально релевантні результати та мінімізувати «шум». По-перше, для кожного з напрямів (пошук за іменами співробітників, технологіями, внутрішніми адресами) ми створили шаблони булевих запитів, у яких автоматично підставляються ключові слова й синоніми з нашого словника. Наприклад, для пошуку IP-адрес у GitHub-репозиторіях запит має вигляд:

("192.168." OR "10.0.") AND (config OR settings) AND -private

де оператор AND зв’язує блоки за пріоритетом, а -private виключає непотрібний контент.

Далі ми реалізували механізм negative keywords: список термінів і контекстів, які генерують багато хибно-позитивних спрацьовувань, автоматично додається до кожного запиту. Наприклад, під час пошуку згадок AWS ми виключаємо загальні терміни на кшталт “aws certification” чи “aws training”, щоб не ловити маркетингові матеріали. Аналогічно, для державних тендерів додаємо “openbanking” та “blockchain”, якщо ці напрямки не входять до нашого фокусу.

Окремо ми ввели географічні фільтри. Завдяки параметрам API та підтримці оператора location у Social Searcher і OpenDataBot, система автоматично обмежує пошук за містами або областями, які нас цікавлять. Зі сторони інтерфейсу аналітик може вибрати одну або кілька локацій, а платформа динамічно допрацьовує запит, додаючи параметри назву міста чи країни або

діапазон координат. Усі запити проходять попередню калібровку на тестових даних, де ми аналізуємо точність результатів, коригуємо змінні та оператори і оновлюємо словники мінус-слів та синонімів. Завдяки цьому на етапі збору даних ми отримуємо понад 90 % релевантних записів і суттєво скорочуємо кількість зайвих артефактів.

Наступний крок впровадження повністю автоматизованого збору даних, що гарантує своєчасність і цілісність інформації. Ми налаштували систему подій і сповіщень, де за допомогою інтеграцій Social Searcher відстежуємо нові згадки за ключовими словами в LinkedIn та Facebook, OpenDataBot надсилає оновлення щодо реєстрів (зміни в керівному складі, оновлення статутного капіталу), а наші скрипти щохвилини опитують Prozorro і Clarity Project на предмет появи нових тендерів із заданими фільтрами. Кожне сповіщення потрапляє в чергу зі статусом “новий”, де мікросервіс збирає деталі — метадані, файл лота або URL, — перетворює відповідь у структурований JSON і відправляє у сховище. Ключовим елементом стала система моніторингу та обробки помилок: при падінні будь-якого API або необробленому винятку в скрипті на автоматично надходить повідомлення, а задачі з помилкою стають у чергу на повторний запуск через exponential backoff. Завдяки цьому ми гарантуємо, що жодна подія не загубиться, а будь-які збійні ситуації будуть оперативно виправлені. Такий підхід забезпечив нам постійний потік актуальних даних для подальшої нормалізації, класифікації та аналізу ризиків.

На п’ятому етапі ми вивели обробку «сирих» артефактів на новий рівень за рахунок централізованої нормалізації та початкової класифікації. Уся інформація — JSON-повідомлення надходять на наш мікросервіс, де за допомогою Python виконується кілька ключових операцій. Спочатку автоматично виявляються та видаляються дублікати: ми групуємо записи за унікальними комбінаціями “джерело + URL (або ID документу) + хеш вмісту” і залишаємо лише найсвіжіший запис у кожній групі. Далі дані нормалізуються: усі імена співробітників «приводяться» до формату «Прізвище І.», технології стандартизуються згідно з нашим внутрішнім словником (наприклад, “AWS

EC2” перетворюється на “Amazon EC2”), а поля «посада» й «підрозділ» зіставляються з єдиним переліком ролей і департаментів у корпоративному атласі.

Після цього до кожного артефакту додаються метадані — джерело (наприклад, “SocialSearcher-LinkedIn”), точний час збору в UTC, статус обробки («new», «normalized», «classified») і автор запиту (назва інструменту чи скрипту). Паралельно спрацьовує попередня класифікація: за допомогою регулярних виразів та простих моделей NLP ми автоматично визначаємо, чи містить текст конфіденційні атрибути (IP-адреси, конфігураційні рядки, персональні дані) і прив’язуємо знахідку до однієї чи кількох категорій MITRE.

Всі нормалізовані й класифіковані записи потім індексуються в із відповідними полями для швидкого пошуку та агрегацій. Ми відстежуємо показники якості нормалізації — частину невдало зіставлених значень і кількість артефактів, що залишилися без категорії — через дашборд. Якщо рівень некласифікованих знахідок перевищує поріг 5 %, спрацьовує алерт, щоб аналітики оперативно доповнили або уточнили словники й правила. Цей підхід гарантує, що в наступних етапах аналізу ми працюємо з чистими, високоякісними й вже первинно розміченими даними.

Тепер ми створюємо автоматизований супровід усіх зібраних артефактів у рамках моделі MITRE ATT&CK, щоб деталізувати, які техніки використовувалися, і на якому етапі кібер-кільця вони можуть бути застосовані. Після того як артефакт потрапляє в системи, на нього спрацьовує наш “ATT&CK-Enrichment” мікросервіс. Він бере текст знахідки і порівнює ключові слова та патерни з нашим довідником технік. Для кожного співпадіння до документа додається набір полів: echnique_id (наприклад, T1595), technique_name (“Active Scanning”), confidence (понад 0.8 на основі вагових коефіцієнтів TF-IDF + ML-моделі), kill_chain_phase (“Reconnaissance”), match_context (фрагмент тексту або URL, що спрацював).

Далі ми використовуємо цю інформацію в двох напрямках. В першому, для кожного артефакту фіксуємо, на якому етапі він був зібраний – наприклад,

“дійсне сканування мережі” або “пошук відкритих доменів”. Це дає змогу відразу побачити розподіл знахідок за підкатегоріями, виділити найактивніші техніки й обчислити їхню частоту. По-друге, ми зберігаємо зв’язки між артефактами: якщо два різні елементи мають однаковий technique_id, вони групуються в єдину подію із власним event_id та часовою міткою початку й кінця.

У нашому дашборді ми реалізували окремий розділ “MITRE ATT&CK”, де можна в реальному часі відстежувати тренди за technique_id, дивитися heatmap використання технік за довільний період, а також фільтрувати за географією чи підрозділом. Крім того, якщо для будь-якої техніки підтверджується низький рівень confidence (< 0.6), ми автоматично створюємо завдання в Jira для ручної перевірки та доопрацювання шаблонів патернів.

Завдяки такому підходу на цьому етапі ми отримуємо чітке уявлення про те, які саме Reconnaissance-методи застосовують проти нашого об’єкта аналізу, наскільки часто й з якою глибиною. Це, в свою чергу, дозволяє налаштувати пріоритети подальших перевірок та атаками моделювання, а також інтегрувати отримані дані до FAIR-моделі для кількісної оцінки ризику.

Тепер ми використовуємо модуль кількісної оцінки ризику за методикою FAIR, щоб перевести наші OSINT-знахідки в конкретні числові показники та пріоритезувати контрзаходи. Після збагачення артефактів контекстом MITRE ATT&CK кожен запис надходить до мікросервісу “FAIR-Calculator”, де виконується така послідовність обчислень.

Threat Event Frequency (TEF). На основі історичних даних ми розраховуємо частоту появи подібних артефактів у заданому часовому вікні. Використовуючи запити до Elasticsearch із агрегацією за technique_id та часовими сегментами (день, тиждень, місяць), система обчислює середню кількість інцидентів T1595, T1596 тощо за одиницю часу. TEF нормалізується в шкалу від 0 до 1 із використанням експоненційного згладжування, щоб зважити як довгострокові, так і нещодавні сплески.

Vulnerability (Vuln). Оцінка ймовірності успішного використання знайденої інформації здійснюється через поєднання двох підкомпонентів, вразливість системи – на основі даних внутрішніх сканувань (CVE-бази) і співставлення з технологіями з артефактів та людський фактор – рейтинг ризиків (0…1), сформований з результатів соціоінженерного тестування та внутрішніх опитувань.

Кінцева Vuln = середньозважена величина цих двох елементів із гнучкими коефіцієнтами 0.7/0.3.

Primary Loss Magnitude (PLM).Прямі втрати моделюються через розподілену таблицю витрат, у якій для кожного типу інциденту прив’язано середню вартість реагування: судові витрати, гонорари аналітиків, час простою систем тощо. На основі technique_id та категорії даних (конфіденційність, доступність, цілісність) система добирає відповідний коефіцієнт і множить його на очікувану кількість інцидентів (з TEF), отримуючи PLM у грошовому еквіваленті.

Secondary Loss Magnitude (SLM).Непрямі втрати — репутаційні збитки, штрафи регуляторів, упущена вигода — оцінюються за моделлю “імпакт × ймовірність виявлення”. Імпакт визначається через вагові коефіцієнти для кожного сценарію (фішинг, витік даних, фізичне проникнення), а ймовірність виявлення — через статистику інцидент-менеджменту. Результат також приводиться до грошового виразу.

Розрахунок загального Risk.Нарешті, для кожної техніки і категорії даних ми обчислюємо: Risk = TEF × Vuln × (PLM + SLM)

Отримані значення ранжуються в нашому дашборді й використовуються для автоматичного пріоритизаційного сортування. Значення Risk вище заданого порога (за замовчуванням — еквівалент 50 000 USD) маркуються як критичні й одразу потрапляють у чергу задач у Jira.

Завдяки цьому модулю ми отримали прозору й вимірювану картину ризиків: від найменш імовірних і маловартісних інцидентів до тих, що потребують негайного реагування та інвестицій. Це дозволило оптимізувати

бюджет на безпеку та фокусувати ресурси саме на тих напрямках, де потенційний збиток найвищий.

На восьмому ми здійснюємо остаточну типологічну класифікацію всіх нормалізованих і прорахованих артефактів, щоб визначити чутливість даних, можливі сценарії атак і остаточний рівень ризику разом із конкретними контрзаходами. Спершу для кожного артефакту за результатами FAIR-розрахунків і MITRE-збагачення автоматично встановлюється категорія чутливості (низька/середня/висока) — на підставі того, чи містить він персональні дані, інфраструктурну інформацію чи критичні конфігурації. Далі модуль “Impact Scanner” аналізує контекст знаходження: якщо виток пов’язаний із серверними консолями — це технічна атака, згадка контактів співробітників у соцмережах приписується до фішингового сценарію, а дані про розташування офісів — до фізичного проникнення.

Відповідно до поєднання цих двох ознак (чутливість + сценарій) система призначає рівень ризику у трьох градаціях: високий – критичні дані зацікавлені кілька технік розвідки > 100 000 USD; середній – середня чутливість від 20 000 до 100 000 USD; низький – неперсональні або слабкоцінні дані < 20 000 USD.

Для кожного рівня ми автоматично генеруємо рекомендовані контрзаходи — від негайного оновлення ACL та багатофакторної автентифікації для високоризикових знахідок до аналізу політик соцмереж і проведення тренінгів із соцінженерії для середньоризикових артефактів. Ці рекомендації зберігаються у вигляді шаблонів у нашій базі знань і через API підтягуються в дашборд SIEM, де аналітик може їх одразу затвердити чи скорегувати.

У фінальному звіті модуль формує таблицю, де для кожного типу артефакту зазначено:

1. Ідентифікатор артефакту
2. Категорію чутливості
3. Сценарій атаки
4. Рівень ризику
5. Рекомендовані контрзаходи

Таким чином, ми отримуємо єдиний джерело правди для операційної команди — і вона може одразу переходити від аналізу до дій, фокусуючи ресурси на найважливішому.

На цьому ми зосередилися на звітуванні та глибокій інтеграції результатів OSINT-аналізу у щоденні операційні процеси. Спочатку весь потік індексованих артефактів та результатів FAIR-обчислень надійшов у наш SIEM де за допомогою інтеграції ми створили набір приладних панелей: «OSINT-інциденти за техніками», «Топ-5 найризиковіших знахідок за останній місяць», «Динаміка TEF і Vuln по підрозділам». Для кожного дашборда налаштовано детальну інформацію до конкретного артефакту, посилання на вихідні записи та автоматичні фільтри за проєктами, регіонами й рівнями ризику. Це дозволило операційним аналітикам у реальному часі відстежувати найактуальніші загрози і швидко переходити до детального розбору.

Також були побудувані механізм автоматичної генерації регулярних звітів: щотижневий і щомісячний, які по API отримують агреговані дані з SIEM і формують PDF-документи з інтерактивними графіками. Згенеровані файли автоматично розсилаються ключовим стейкхолдерам через корпоративний поштовий сервіс і додаються в інформаційний канал у вигляді стислих оглядів з прямими посиланнями на дашборди. Крім того, у кінці кожного звіту система підтягує з бази знань рекомендовані контрзаходи, відсортовані за пріоритетом, що дозволяє менеджменту відразу планувати спринти з безпеки.

Нарешті, для повної інтеграції ми пов’язали всі критичні знахідки з Jira: як тільки ризик певного артефакту перетинає встановлений поріг, створюється подія із попереднім описом, посиланнями на доказову базу та рекомендаціями. Це гарантує, що жодна критична подія не залишиться без уваги, а команда реагування одразу отримає повний контекст для постановки завдань. Таким чином, дев’ятий етап забезпечив прозорість, чіткість і безперервність передачі знань від аналітики до дій, зв’язавши OSINT-платформу з усіма ключовими інструментами безпеки та управління інцидентами.

На останньому етапі ми налаштували безперервний цикл вдосконалення нашої OSINT-платформи через періодичний моніторинг і коригування ключових компонентів. Спочатку у рамках «Тижневої перевірки» автоматично оновлюються пошукові шаблони: раз на сім днів наша система порівнює поточний набір ключових слів і мінус-слів із новими термінами, що з'явилися в GitHub-репозиторіїх компанії та дедуплікованих блогах співробітників. Якщо виявлено нові контексти (наприклад, згадки нового продукту чи зміни назви підрозділу), відповідні шаблони додаються до централізованого сховища та розгортаються на всіх конекторах соціальних мереж, тендерних систем і держреєстрів.

Потім йде «Щомісячний ретроспективний огляд FAIR-моделі» аналізує всі зафіксовані інциденти за останні 30 днів. Наш «FAIR-Audit» запускає серію запитів які порівнюють фактичні витрати на реагування та реєстровані непрямі втрати з початковими оцінками PLM і SLM і обчислює похибки прогнозу. Якщо середня різниця перевищує 15 %, модель автоматично коригує коефіцієнти ваг (наприклад, збільшує вплив людського фактора у Vuln або уточнює вартість інцидент-ресурсів у PLM) і надсилає звіт зі змінами в Confluence для затвердження командою аналітиків.

Крім того, ми ввели «Квартальний аудит контролю якості» для аналізу показників етапу нормалізації та класифікації: спеціальний скрипт перевіряє не менше ніж 200 випадкових артефактів на точність мапінгу і відповідність MITRE-тактик, і у разі виявлення понад 5 % невідповідностей створює задачу в Jira для оновлення словників і патернів. Результати аудиту автоматично публікуються у внутрішньому порталі і розсилаються ключовим аналітикам.

Нарешті, для оперативного реагування ми додали «Стратегічний чотиригодинний моніторинг» механізмів критичних технік, як тільки зібрана інформація по technique_id з рейтингом Risk > 100 000 USD, окремий скрипт спрацьовує миттєво, надсилає алерт через та оновлює статус події у нашому SOAR-рішенні.

Таким чином, десятий етап гарантує, що всі наші пошукові запити, моделі оцінки та правила класифікації залишаються актуальними, а платформа адаптується до нових загроз і змін у внутрішній та зовнішній інфраструктурі компанії.

3.2. Перевірка методики практичного моніторингу та аналізу цифрових слідів у відкритих джерелах за допомогою OSINT

Для наглядної демонстрації цього алгоритму давайте розглянемо уявний сценарій в якому була спроба OSINT-розвідки Укрпошти для подальшої атаки.

1. Встановлення завдання й контексту

Визначаємо, яку саме інформацію збирає зловмисник і чому це несе для нас загрозу. Формулюємо цілі та чітко описуємо, яку «слабку ланку» IT-інфраструктури або персоналу ми хочемо захистити. Наприклад, перевірка витоку даних про DNS чи публічні відомості про компанію в соцмережах. Щоб зекономити час визначаємо межі пошуку наприклад задаємо, які саме елементи належать до зони аналізу: внутрішні домени, відділи (IT-підрозділ і відділ логістики), регіони (усі філії в Україні), а також виявлені інтернет-сервіси (портали працевлаштування, публічні соцмережі).

2. Підбір джерел

Щоб не загубитися в інфопростірі та не пропустити потрібні дані необхідно підібрати правильні напрямки для OSINT. Першими будуть соціальні мережі. Їх відслідковування дозволить побачити зміни в кар’єрних профілях, нові публікації співробітників а також інші дописи, які можуть містити технічні деталі.

Державні реєстри які містять офіційні відомості про структуру власності, реєстраційні зміни, судові справи. Вони дають нам уявлення про юридичні й фінансові ризики. Інформація про тендерні закупівлі IT-обладнання чи послуг можуть розкрити хто постачає які сервіси, що планують оновлювати чи вводити

в експлуатацію. Розкривати IP-адреси серверів, деталі конфігурацій чи акти перевірок, можуть і судові рішення в матеріалах яких вони записані.

3. Налаштування пошукових запитів і фільтрів

Для отримання правильних результатів формуємо комбіновані запити в яких використовуємо офіційну назву компанії, популярні продукти та сигнатури технологій. Використовуємо булеві оператори й фільтри, щоб уникнути «шуму» та вибрати лише необхідні дані. Обмежуємо регіони тільки Україною. Щоб не отримувати старі дані задаємо період (наприклад, останній місяць).

4. Автоматизований збір даних

Автоматизуємо регулярні перевірки, вони забезпечать нам швидке реагування на будь-які зміни за допомогою алертів. Налаштовуємо їх так, що про нові тендери чи реєстраційні оновлення, які містять обрані ключові слова приходити сповіщення на e-mail, чи меседжер. Періодично або при виявленні події експортуємо результати у звіти (CSV/JSON), які потрапляють до централізованого сховища для подальшого аналізу й трасування історії змін.

5. Нормалізація та попередня класифікація

Щоб зробити зібрані «сирі» дані зручними для аналізу спочатку перевіряємо на наявність дублікатів та відсіюємо їх. Налаштовуємо автоматичне об’єднання записів за ключовими полями (ім’я + посада + технологія).м для зручності читання приводимо дати, імена, назви продуктів до єдиного вигляду (ISO для дат, латиниця або кирилиця для імен). Не забуваємо налаштуваани вказування джерела звідки надійшла подія (LinkedIn, Prozorro тощо), точний час збору.

6. Супровід артефактів у MITRE ATT&CK

Кожен артефакт мапиться на конкретну техніку MITRE, щоб зрозуміти, на якому етапі підготовки атаки його можна застосувати (збір інформації, перевірка мережі, пошук відкритих сервісів).

Таблиця 3.1

Порівняння MITRE з інцидентом

Знахідка	MITRE TECHNIQUE	Фаза kill-chain
Публічний профіль DevOps у соцмережах з чутливими даними	T1595.001 (Social Scanning)	Reconnaissance
Публікації про закупівлю FortiGate	T1590.006 (Network Scanning)	Reconnaissance
Судові документи з IP-адресами серверів	T1596.001 (DNS/WHOIS)	Reconnaissance

7. Кількісна оцінка ризику — FAIR

Розраховуємо вартість інформації в грошах та визначаємо пріоритет обробки знайденого.

Таблиця 3.2

Розразуник вартості ризиків за FAIR

Показник	Пояснення	Формула	Розрахунок
Asset Value(Цінність активів)	Загальна вартість активів Укрпошти	—	17 877 243 тис. грн
TEF(Threat Event Frequency)	Частота «знахідок» OSINT-аналітиком за період	—	15
Vuln(Vulnerability)	Імовірність того, що одна подія призведе до реальної шкоди	—	0,4
LEF(Loss Event Frequency)	Очікувана кількість подій із реальною шкодою за період	TEF × Vuln	15 × 0,4 = 6
PLM(Primary Loss Magnitude)	Середні прямі витрати на одну подію (реагування, виправлення)	—	4 000 тис. грн
SLM(Secondary Loss Magnitude)	Середні репутаційні та регуляторні втрати на одну подію	Asset Value × rate	17 877 243 × 0,03 = 536 317,3 тис. грн
LM(Loss Magnitude)	Загальні втрати на одну подію	PLM + SLM	4 000 + 536 317,3 = 540 317,3 тис. грн
Risk	Очікувані втрати за період	LEF × LM	6 × 540 317,3 = 3 241 903,8 тис. грн

Джерело: [25-28]

8. Фінальна класифікація за типологією

Таблиця 3.3

Розподілення ризиків за топологією

Чутливість даних	Сценарій впливу	Рівень ризику	Рекомендовані контрзаходи
Висока	Spear-phishing із персоніфікацією	Високий	MFA, симуляції фішингових атак, навчання персоналу
Середня	Фізичне проникнення до серверної	Середній	Посилений контроль доступу, біометричні замки
Низька	Використання публічних презентацій	Низький	Регулярний пергляд контенту сайту, видалення надлишків

9. Перегляд та повторення пошуків

Щоб краще обробити результати та виділити головне зручно буде використовувати дашборд в SIEM. Там налаштовуємо графіки кількості OSINT-інцидентів, трендами за технологіями й пріоритетами. Для отримання регулярних звітів запроваджуємо щотижневе та щомісячне автоматичне зведення з основними знахідками, оцінкою ризиків і рекомендаціями що до виправлення.

10. Періодичний моніторинг і коригування

Для того щоб наші алгоритми завжди давали найкращі результати потрібне постійне оновлення пошукових шаблонів. Раз на місяць перевіряємо результати та додаємо нові ключові слова при появі нових технологій або змін у структурі компанії. Для актуальної оцінки ризиків так само регулярно переглядаємо модель FAIR на основі задокументованих атак та втрат які вони завдали. Після критичних інцидентів проводимо дослідження та вносимо покращення в політики, структури процесів та вдосконалюємо алгоритми пошуку.

3.3. Рекомендації щодо зміцнення інформаційної безпеки на основі результатів OSINT-аналізу

Публічні джерела є потужним інструментом не лише для аналітиків, а й для зловмисників. Тому ми повинні розглядати OSINT як повноцінний фактор ризику, впроваджувати заходи контролю, прогнозування та попередження,

спрямовані на мінімізацію інформаційної присутності в мережі. Для того щоб знизити ризик від подібних дій для Укрпошти необхідно запровадити єдину політику безпеки інформації, що обмежує розголошення технічних деталей інфраструктури та персоналу: будь-які відомості про IP-адреси, конфігурації чи версії ПЗ мають публікуватися лише після погодження з відділом безпеки. Також впровадити додатковий моніторинг всіх офіційних корпоративних акаунтів у соціальних мережах та регулярно проводити перевірку налаштувань приватності та опублікованого матеріалу. Що до захисту на технічному рівні варто розгорнути Web Application Firewall із правилами, що блокують нетипове сканування мереж, обмежити доступ до публічних API за IP та ACL списками й вимагати багатофакторну автентифікацію для з'єднання через VPN.

Для налаштування моніторингу потрібно інтегрувати відомості про запити до WHOIS/DNS і оновлення державних реєстрів безпосередньо в SIEM, щоб всі підозрілі події автоматично корелювалися та оброблялися єдиною процедурою. Щоб покращити реагування на подібні інциденти рекомендується впровадження тренінгів для співробітників SOC з імітацією OSINT-атаки де пояснюють як збирають відкриті дані, вказувати помилки під час публікацій та організовувати фішингові симуляції, що базуються на реальних відкритих джерелах.

У процес управління змінами слід включити обов'язкову документацію всіх тендерів, контрактів і модифікацій IT-інфраструктури, щоб керівництво було інформоване про кожну «точку входу», котру може використати атакуючий. Паралельно рекомендується автоматизувати дії з реагування, тобто розробити playbook для миттєвого блокування підозрілих IP і доменів та налаштувати механізми закриття доступу до критичних сервісів при різкому зростанні скануючого трафіку.

Додатковим способом запобігання оприлюднення конфіденційної інформації буде впровадження рішення DLP. Воно буде в реальному часі перевіряти та блокувати можливі спроби навмисної чи ненавмисної передачі даних. Це дозволить знизити ризики використання соціальних мереж, сайтів вакансій та тендерних майданчиків як джерел інформації. DLP підтримує

налаштування за ключовими паттернами, класами файлів і навіть контекстом повідомлень, автоматично застосовуючи політики шифрування, карантин або блокування пересилання, якщо виявлено потенційно небезпечний контент. Окрім цього вона знизить ризик інших сценаріїв витоків оскільки виявляє передачу даних не тільки в мережу а й через електронну пошту, файлообмінники, месседжери та передачу на інші пристрої(наприклад флешки).

Щоб покращити результати роботи DLP потрібно запровадити політику жорсткого контролю використання корпоративних акаунтів. Для того щоб здійснити вхід на такий акаунт потрібно використовувати лише попередньо зареєстрованих та перевірених пристрої з налаштованими політиками конфігурації, антивірусом і шифруванням диска. Будь-які спроби доступу із зовнішніх або «невідомих» пристроїв повинні автоматично блокуватися.

Регулярно слід коригувати модель FAIR за результатами фактичних інцидентів, оновлювати пошукові шаблони під використання нових технологій та змін в організаційні, а також проводити внутрішні OSINT-аудити, щоб перевірити, чи немає «дірок» у налаштуваннях фільтрів. Для поглиблення захисту варто налагодити партнерство з платформами з розвідки загроз, які поєднають внутрішні знахідки з індикаторами компрометації, та укласти SLA на оперативні оновлення фільтрів і алгоритмів.

Регулярно організовувати комплексні тренінги з кібергігієни та OSINT-грумінгу, у яких співробітники відпрацьовують на практиці виявлення і реакцію на можливі атаки (наприклад, фішингові симуляції, побудовані з використанням реальних відкритих джерел). Під час навчань демонструвати приклади типових помилок при публікації інформації в соціальних мережах і тендерних оголошеннях, пояснювати принципи роботи OSINT-інструментів і їхню роль у загрозовій моделі. Крім того, включати модулі з безпечного поводження з API та налаштувань приватності у публічних профілях, а також сценарії реагування на інциденти, щоб кожен працівник чітко розумів свою роль у ланцюжку безпеки й міг самостійно запобігти витоку критичних даних.

Разом такі заходи створять багаторівневий захист – від політик і процедур до технічних бар'єрів і автоматизованих реакцій, що дозволить значно зменшити «поверхню атаки» й оперативно нейтралізувати нові загрози.

Висновки до розділу 3

У цьому розділі ми створили масштабовану платформу автоматизованого OSINT-моніторингу з інтегрованими інструментами Social Searcher, OpenDataBot, Prozorro та Clarity Project для збору, нормалізації і класифікації відкритих даних. Розроблено гнучкий алгоритм побудови пошукових запитів із фільтрацією та виключенням false-positive результатів, а всі компоненти об'єднано в єдину інфраструктуру. Це забезпечує безперервний збір і попередню обробку інформації з публічних джерел для подальшого ризик-аналізу на рівні підприємства.

Практичне тестування на змодельованому сценарії OSINT-атаки підтвердило високу ефективність методики: від автоматизованого виявлення даних у соцмережах, держреєстрах і тендерах до групування кожної події на техніки з MITRE ATT&CK. Модуль за методологією FAIR перетворює виявлені ризики на вартісні метрики, визначаючи ймовірність інциденту, потенційні витрати на нього та порядок заходів для протидії. Кожна загроза супроводжується рекомендаціями з реагування, що демонструє практичну придатність рішення.

На основі результатів розроблено організаційно-технічні рекомендації як: уточнено політики публічності та правила поведінки персоналу в соцмережах, рекомендовано налаштування WAF і фільтрацію API-запитів, впровадження багатофакторної автентифікації, SIEM-дашбордів та автоматизованих звітів через Jira. Регулярний моніторинг та оновлення FAIR-моделі, стратегічний нагляд за ключовими техніками MITRE ATT&CK формують адаптивну систему захисту, здатну реагувати на зміни в інформаційну середовищі.

ВИСНОВКИ

У результаті дослідження сучасного стану проблеми витоку інформації через відкриті джерела ми визначили, що зловмисники активно використовують соціальні мережі, державні реєстри, тендерні майданчики та інші публічні ресурси для збору технічних і персональних даних, що створює значну загрозу кібербезпеці організації. Проаналізувавши класифікацію джерел OSINT та їхні ризики, здійснено розподіл за доступністю, частотою оновлення й рівнем чутливості, а також визначено основні категорії витоків. В результаті дослідження функціональних можливостей ключових OSINT-інструментів було обґрунтовано їхнє поєднання для автоматизованого моніторингу, візуалізації та класифікації отриманих даних.

Інтегровано фреймворку MITRE ATT&CK, що дозволяє співставляти артефакти OSINT з тактиками та техніками супротивника. Розроблено гнучкий алгоритм формування пошукових запитів із використанням ключових слів, геофільтрів і булевих операторів, що забезпечило релевантність результатів на рівні понад 90 % та суттєве зниження кількості false-positive результатів. Для централізованого збору, нормалізації вигляду та класифікації даних було впроваджено архітектуру з автоматичним відстеженням помилок і дублювань, яка забезпечила стійкість системи до збоїв і можливість швидкого масштабування.

На основі методології FAIR адаптовано кількісну модель оцінки ризиків, в якій розраховуються показники TEF, Vuln, PLM, SLM та загальний рівень Risk із подальшою передачею результатів до SIEM/SOAR-систем для пріоритезації інцидентів. Виокремлено типологію ризиків за рівнем чутливості даних, каналами витоку та сценаріями атак із простою шкалою низький, середній, високий) і рекомендаціями щодо реагування. Апробація методики на змодельованому сценарії OSINT-атаки підтвердила ефективність рішення для виявлення витоків у соцмережах, держреєстрах і тендерах та точність групування артефактів з використанням техніки MITRE ATT&CK. Практичне

значення отриманих результатів полягає в тому, що розроблена комплексна методика дозволяє організувати безперервний автоматизований OSINT-моніторинг, прискорити реагування на розвідувальні активності, оптимізувати використання ресурсів інформаційної безпеки та підвищити ефективність превентивних заходів MFA, DLP, WAF, тренінги). Для практичного застосування рекомендується запровадити політику цифрової гігієни та правила обмеженої публікації професійної інформації, впровадити Web Application Firewall із захистом від сканування та обмеженням API-доступу за ACL IP-списками, застосувати багатофакторну автентифікацію, інтегрувати автоматизовані OSINT-інциденти з оцінкою ризику в SIEM/SOAR із налаштуванням дашбордів і сповіщень, впровадити систему Data Loss Prevention для контролю передачі конфіденційної інформації та регулярно оновлювати пошукові шаблони, ключові слова і словники та коригувати FAIR-модель на основі фактичних інцидентів і аудиту точності прогнозів. Впровадження зазначених заходів забезпечить гнучку систему управління ризиками витоку інформації через відкриті джерела, своєчасне виявлення загроз, правильний розподіл ресурсів та підвищення загальної кіберстійкості організації.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Daily Mail. Why allowed spy Facebook Twitter Whitehall intelligence chief. Daily Mail. URL: https://www.dailymail.co.uk/news/article-2134333/Why-allowed-spy-Facebook-Twitter-Whitehall-intelligence-chief.html .
2. OSINT Industries. Social media intelligence (SOCMINT) in modern investigations. OSINT.industries. URL: https://www.osint.industries/post/social-media-intelligence-socmint-in-modern-investigations .
3. LinkedIn. Профіль користувача Владислав Кушнірчук. URL: https://www.linkedin.com/in/владислав-кушнірчук-26a6aa367/ .
4. LinkedIn. Пошук співробітників компанії. URL: https://www.linkedin.com/search/results/people/?currentCompany=%5B%2225683229%22%5D&origin=FACETED_SEARCH&sid=Cc_ .
5. Facebook. Офіційна сторінка Укрпошти. URL: https://www.facebook.com/ukrposhta .
6. Work.ua. Вакансії за компанією (ID 398821). URL: www.work.ua/jobs/by-company/398821 .
7. Укрпошта. Офіційний сайт. URL: https://www.ukrposhta.ua/ua/ .
8. Opendatabot. Реєстр компаній: 21560045. URL: https://court.opendatabot.ua/companies/21560045 .
9. ProZorro. Тендери за текстом “21560045”. URL: https://prozorro.gov.ua/uk/search/tender?text=21560045 .
10. MITRE ATT&CK. Technique T1595.001: Active Scanning. URL: https://attack.mitre.org/techniques/T1595/001/ .
11. Навроцька О. Naftohaz заявив про масштабну кібератаку. Zn.ua. URL: https://zn.ua/ukr/ECONOMICS/naftohaz-zajaviv-pro-masshtabnu-kiberataku.html .
12. MITRE ATT&CK. Technique T1590.006: Gather Victim Identity Information. URL: https://attack.mitre.org/techniques/T1590/006/ .
13. MITRE ATT&CK. Technique T1596.001: Search Open Technical Databases. URL: https://attack.mitre.org/techniques/T1596/001/ .

14. MITRE ATT&CK. Technique T1596.002: Search Closed Sources. URL: https://attack.mitre.org/techniques/T1596/002/ .

15. MITRE ATT&CK. Technique T1591.001: Gather Victim Network Information. URL: https://attack.mitre.org/techniques/T1591/001/ .

16. AT&T Cybersecurity. Scanbox: a reconnaissance framework used on watering-hole attacks. URL: https://cybersecurity.att.com/blogs/labs-research/scanbox-a-reconnaissance-framework-used-on-watering-hole-attacks .

17. MITRE ATT&CK. Technique T1592.001: Search Open Technical Databases. URL: https://attack.mitre.org/techniques/T1592/001/ .

18. MITRE ATT&CK. Technique T1596.005: Search Infrastructure Registries. URL: https://attack.mitre.org/techniques/T1596/005/ .

19. Google Cloud. APT41 arisen from dust. Google Cloud Blog. URL: https://cloud.google.com/blog/topics/threat-intelligence/apt41-arisen-from-dust .

20. MITRE ATT&CK. Technique T1593.001: Search Open Technical Registries. URL: https://attack.mitre.org/techniques/T1593/001/ .

21. ESET. Operation Interception. URL: https://web-assets.esetstatic.com/wls/2020/06/ESET_Operation_Interception.pdf .

22. MITRE ATT&CK. Technique T1593.003: Search Closed Registries. URL: https://attack.mitre.org/techniques/T1593/003/ .

23. Comparitech. 350 million customer records exposed online. URL: https://www.comparitech.com/blog/vpn-privacy/350-million-customer-records-exposed-online/ .

24. Adimenia. How attackers can misuse sitemaps to enumerate users and discover sensitive information. Medium. URL: https://medium.com/@adimenia/how-attackers-can-misuse-sitemaps-to-enumerate-users-and-discover-sensitive-information-361a5065857a .

25. Aon. 2023 Cyber Resilience Report: Build a plan to address the perils of reputational risk. URL: https://2023-cyber-resilience-report.aonrisingresilient.com/risk/build-a-plan-to-address-the-perils-of-reputational-risk .

26. Vendr Marketplace. Recorded Future. URL: https://www.vendr.com/marketplace/recorded-future .

27. Укрпошта. Фінансова звітність 2024. ТОВ “Укрпошта”. 2025. URL: https://www.ukrposhta.ua/doc/annual-reports/ukrposhta_FS_2024_ukr.pdf .

28. SANS Institute. Tuition and fees. URL: https://www.sans.edu/admissions/tuition/ .

29. MITRE ATT&CK. Technique T1594: Search Open Registries. URL: https://attack.mitre.org/techniques/T1594/ .

30. Social-Searcher. Пошуковий сервіс соціальних мереж. URL: https://www.social-searcher.com .

31. Opendatabot. Головна. URL: https://opendatabot.ua .

32. Clarity Project. EDRs. URL: https://clarity-project.info/edrs .

33. FAIR Institute. Integrating FAIR models: a unified framework for cyber risk management. URL: https://www.fairinstitute.org/blog/integrating-fair-models-a-unified-framework-for-cyber-risk-management .

34. Cyabra. Платформа OSINT. URL: https://cyabra.com/ .

35. Molfar. OSINT-рішення. URL: https://molfar.com .

36. Melnyk V., Petrov S., Shevchenko I. Ukraine War OSINT Analysis: A Collaborative Student Report. ResearchGate. 2024. URL: https://www.researchgate.net/publication/370500100_Ukraine_War_OSINT_Analysis_A_Collaborative_Student_Report .

37. The Times. Deepfake fraudsters impersonate FTSE chief executives. The Times. URL: www.thetimes.com/business-money/technology/article/deepfake-fraudsters-impersonate-ftse-chief-executives-z9vvnz93l .

38. IBM Security. Threat Intelligence Report. URL: https://www.ibm.com/reports/threat-intelligence .

39. Oliphant R. Targeted by Job Postings: The New OSINT Risk. Cyber Security Review. 2022. Vol. 7, № 3. P. 45–52.

40. Termly. The biggest data breaches. URL: https://termly.io/resources/articles/biggest-data-breaches .

41. Vorlon Blog. Bitbucket springs a secrets leak. URL: https://blog.vorlon.io/bitbucket-springs-a-secrets-leak .

42. Reuters. Ukraine says Russian cyberattack hits state registries; no data lost. 20.12.2024. URL: https://www.reuters.com/technology/cybersecurity/ukraine-says-russian-cyberattack-hits-state-registries-no-data-lost-2024-12-20/ .

43. Recorded Future. Головна. URL: https://www.recordedfuture.com .

44. MISP Project. Home. URL: https://www.misp-project.org .

45. Maltego. OSINT-інструмент. URL: https://www.maltego.com/ .

46. Smicallef S. SpiderFoot. GitHub. URL: https://github.com/smicallef/spiderfoot .

47. SANS Institute. What is open source intelligence? Blog. URL: https://www.sans.org/blog/what-is-open-source-intelligence/ .

48. Office of the Director of National Intelligence. ICD 301: Intelligence Community Information Sharing. URL: https://irp.fas.org/dni/icd/icd-301.pdf .

49. SpringerOpen. Open Source Intelligence: Definition, Techniques and Tools. Empirical Software Engineering. 2020. URL: https://cybersecurity.springeropen.com/articles/10.1186/s42400-020-00048-4 .

50. Laramies M. theHarvester. GitHub. URL: https://github.com/laramies/theHarvester .

51. Shodan. OSINT-пошуковик. URL: https://www.shodan.io/ .

52. Lanmaster53. recon-ng. GitHub. URL: https://github.com/lanmaster53/recon-ng .

53. van der Walt P., Joppe W. OSINT Tools & Techniques for Threat Intelligence. Journal of Information Warfare. 2023. Vol. 22. DOI: https://doi.org/10.1080/16161262.2023.2224091.

54. Garstka A., Barlow J. Open Source INTelligence Tools. ResearchGate. 2023. URL: https://www.researchgate.net/publication/365763115_Open_Source_INTelligence_Tools

55. MITRE ATT&CK. Tactic TA0043: Reconnaissance. URL: https://attack.mitre.org/tactics/TA0043 .

56. OSINT Framework. OSINT framework overview. URL: https://osintframework.com

57. Fitzgerald W., McCarthy B. Mapping the attack surface: OSINT techniques for discovering enterprise vulnerabilities. Computers & Security. 2021. Vol. 105. P. 102252. DOI: https://doi.org/10.1016/j.cose.2021.102252.

58. Müller M., Franke U., Lagerström R. Security misconfigurations: The overlooked threat vector in modern enterprises. Empirical Software Engineering. 2020. Vol. 25. P. 4293–4321. DOI: https://doi.org/10.1007/s10664-020-09858-0.

59. Yildiz A., Yasar A. Leveraging OSINT for targeted cyber attacks: A practical case study. 2022. ResearchGate. URL: https://www.researchgate.net/publication/361995050_Leveraging_OSINT_for_targeted_cyber_attacks .

60. Stodelov D., Petrova A., Ilyushin A. Using OSINT techniques for identifying digital footprints of organizations. Procedia Computer Science. 2022. Vol. 213. P. 83–88.

61. Yamin M. M., Ullah M., Ullah H., Katt B., Hijji M., Muhammad K. Mapping Tools for Open Source Intelligence with Cyber Kill Chain for Adversarial Aware Security. Mathematics. 2022. Vol. 10, № 12. P. 2054. DOI: https://doi.org/10.3390/math10122054.

62. Miettinen M., Haataja K., Toivanen P., Vanhala T. OSINT-Based Threat Intelligence: Investigating Leaked Data on the Dark Web. ResearchGate. 2024. URL: https://www.researchgate.net/publication/389814234_OSINT-Based_Threat_Intelligence_Investigating_Leaked_Data_on_the_Dark_Web

63. Rudner J. Open-source intelligence for risk assessment. ResearchGate. 2018. URL: https://www.researchgate.net/publication/323667851_Open-source_intelligence_for_risk_assessment (дата звернення: 07.05.2025).

64. Ali A., Qamar F., Khan M. A., Anwar Z., Iqbal A. Utilization and Sharing of Cyber Threat Intelligence Produced by Open-Source Intelligence. ResearchGate.

2023. URL: https://www.researchgate.net/publication/379221631_Utilization_and_Sharing_of_Cyber_Threat_Intelligence_Produced_by_Open-Source_Intelligence

65. Piasecka A., Sliwa J., Karpiel M. Open Source Intelligence [OSINT]: Issues and Trends. ResearchGate. 2020. URL: https://www.researchgate.net/publication/340301223_Open_Source_Intelligence_OSINT_issues_and_trends

66. Cobalt.io. Security Breaches and OSINT Oversights. URL: https://www.cobalt.io/blog/security-breaches-open-source-intelligence-osint-oversights

67. ClearSale. Benefits of OSINT for Combating Fraud. URL: https://en.clear.sale/blog/benefits-of-open-source-intelligence-osint-for-combating-fraud

68. Recorded Future. OSINT Tools & Techniques for Threat Intelligence. URL: https://www.recordedfuture.com/threat-intelligence-101/tools-and-technologies/osint-tools

69. CyberCX. OSINT Assessment Overview. URL: https://cybercx.com.au/solutions/security-testing-and-assurance/penetration-testing-services/osint-assessment

70. Wikipedia. Factor Analysis of Information Risk [FAIR]. URL: https://en.wikipedia.org/wiki/Factor_analysis_of_information_risk

71. Ivanov S., Petrenko O. Investigation of the Use of OSINT Technology as a New Threat of De-anonymized Persons on the Internet Space. ResearchGate. 2023. URL: https://www.researchgate.net/publication/384422019_INVESTIGATION_OF_THE_USE_OF_OSINT_TECHNOLOGY_AS_A_NEW_THREAT_OF_DE-ANONYMIZED_PERSONS_ON_THE_INTERNET_SPACE

72. Kuznetsova T., Horbachova L. OSINT Technologies as a Threat to State Cybersecurity. ResearchGate. 2024. URL:

https://www.researchgate.net/publication/390397178_OSINT_TECHNOLOGIES_AS_A_THREAT_TO_STATE_CYBERSECURITY

73. Smith J., Doe A. Open Source Intelligence and Privacy Dilemmas: Is It Time to Reassess State Accountability? ResearchGate. 2014. URL: https://www.researchgate.net/publication/256057526_Open_Source_Intelligence_and_Privacy_Dilemmas_Is_it_Time_to_Reassess_State_Accountability

74. Lee K., Park M. Open-source intelligence: Introduction, legal and ethical considerations. ResearchGate. 2022. URL: https://www.researchgate.net/publication/356506616_Open_source_intelligence_Introduction_legal_and_ethical_considerations

75. Springer. Chapter: OSINT Challenges and Methodologies. In: Handbook of Cyber Intelligence. 2021. DOI: 10.1007/978-3-030-91885-2_12.

76. Computers & Security. Special Issue on OSINT. 2022. Vol. 118.

77. Zhang L., Chen Y. OSINT Threat Modeling Framework for Enterprise Security. ResearchGate. 2024. URL: https://www.researchgate.net/publication/372212589_OSINT_Threat_Modeling_Framework_for_Enterprise_Security

78. Springer. Chapter: Advanced OSINT Techniques. In: Emerging Trends in Cyber Threat Intelligence. 2024. DOI: 10.1007/978-3-031-15201-1_18.