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: “СИСТЕМА ПІДТРИМКИ ВИБОРУ OSINT-ІНСТРУМЕНТІВ ДЛЯ ВИРІШЕННЯ ЗАВДАНЬ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ”

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

_____ Анна КЛОПОВА
(підпис) *Ім’я, ПРІЗВИЩЕ здобувача*

Виконала: здобувачка вищої освіти гр. УБД-42
Анна КЛОПОВА
Ім’я, ПРІЗВИЩЕ

Керівник: Ірина ЛОЗОВА
к.т.н. Ім’я, ПРІЗВИЩЕ

Рецензент: Сергій ГАХОВ
к.військ.н., доцент Ім’я, ПРІЗВИЩЕ

Київ 2026

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 УКБЗІ
_____ Світлана ЛЕГОМІНОВА
“____ ”_____2026 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Клоповій Анні Андріївні
(прізвище, ім’я, по батькові здобувача)

1. Тема кваліфікаційної роботи “Система підтримки вибору OSINT-інструментів для вирішення завдань інформаційної безпеки”,
керівник кваліфікаційної роботи ЛОЗОВА Ірина, к.т.н
(ІПРІЗВИЩЕ, Ім’я,, науковий ступінь, вчене звання)

затверджені наказом Державного університету інформаційно-комунікаційних технологій від “20“ лютого 2026 р. №51

2. Строк подання кваліфікаційної роботи “11” травня 2026р.
3. Вихідні дані до кваліфікаційної роботи: *OSINT-інструменти, задачі інформаційної безпеки, класифікація OSINT-інструментів, система підтримки прийняття рішень, наукова та технічна література.*
4. Перелік питань, які мають бути розроблені:
   4.1. Проаналізувати основні методи, критерії та підходи до вибору OSINT-інструментів залежно від типу завдань інформаційної безпеки.
   4.2. Дослідити роль OSINT у процесах підтримки прийняття рішень та розробити систему вибору OSINT-інструментів залежно від типу завдань інформаційної безпеки..
   4.3. Провести експериментальну перевірку ефективності запропонованої системи підтримки вибору OSINT-інструментів та порівняти її з існуючими підходами.
5. Перелік ілюстративного матеріалу: *презентація PowerPoint*
6. Дата видачі завдання “15“ квітня 2026 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Етапи кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1.	Визначення об’єкту, предмету, мети та завдань дослідження.	19.04.2026	
2.	Збір та аналіз літератури.	26.04.2026	
3.	Аналіз систем підтримки вибору OSINT-інструментів	06.05.2026	
4.	Розробка системи підтримки вибору OSINT-інструментів	12.05.2026	
5.	Реалізація системи підтримки вибору OSINT-інструментів	17.05.2026	
6.	Формулювання висновків за результатами проведеного дослідження.	20.05.2026	
7.	Оформлення роботи.	21.05.2026	
8.	Оформлення презентації.	24.05.2026	
9.	Отримання рецензії на роботу.	26.05.2026	
10.	Захист в ЕК.	10.06.2026	

Здобувачка вищої освіти _____ Анна КЛОПОВА
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Керівник
кваліфікаційної роботи _____ Ірина ЛОЗОВА
(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 здобувачка Клопова А.А. до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 125 Кібербезпека
(код, найменування спеціальності)
освітньої програми Управління інформаційною та кібернетичною безпекою
(назва)
на тему: "Система підтримки вибору OSINT-інструментів для вирішення завдань інформаційної безпеки "

Кваліфікаційна робота і рецензія додаються.

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

Висновок керівника кваліфікаційної роботи

Здобувачка КЛОПОВА Анна у кваліфікаційній роботі дослідила сучасні підходи до використання OSINT у сфері інформаційної безпеки, проаналізувала класифікацію та функціональні можливості OSINT-інструментів, а також визначила проблеми їх вибору залежно від поставлених завдань. У процесі виконання роботи здобувачкою було розроблено систему підтримки вибору OSINT-інструментів на основі критеріїв оцінювання та механізму ранжування засобів відкритої розвідки.

У межах кваліфікаційної роботи реалізовано програмний модуль системи підтримки вибору OSINT-інструментів, сформовано базу знань інструментів та реалізовано механізм оцінювання ефективності інструментів. Також проведено тестування системи на практичних кейсах інформаційної безпеки та проаналізовано отримані результати.

Все це дозволяє оцінити кваліфікаційну роботу здобувачки КЛОПОВОЇ Анни на оцінку "відмінно" та присвоїти їй кваліфікацію бакалавра з кібербезпеки за освітньою програмою Управління інформаційною та кібернетичною безпекою.

Керівник кваліфікаційної роботи _____ Ірина ЛОЗОВА
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

"____"_____2026 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувачка Клопова А.А. 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

здобувачки вищої освіти КЛОПОВОЇ Анни
на тему “Система підтримки вибору OSINT-інструментів для вирішення завдань інформаційної безпеки”

Актуальність. В умовах постійного зростання кількості кіберзагроз, поширення фішингових атак, витоків даних та інформаційних операцій особливої актуальності набуває використання OSINT-інструментів для забезпечення інформаційної безпеки. Значна кількість доступних засобів відкритої розвідки ускладнює процес вибору найбільш ефективних інструментів для конкретних задач, що потребує застосування систем підтримки прийняття рішень.

З огляду на це, тема кваліфікаційної роботи, присвячена розробці системи підтримки вибору OSINT-інструментів для вирішення завдань інформаційної безпеки, є актуальною та має практичне значення для фахівців у сфері кібербезпеки та OSINT-аналітики.

Позитивні сторони.

1. У роботі проведено аналіз основних напрямів використання OSINT у сфері інформаційної безпеки та досліджено сучасні OSINT-інструменти, їх класифікацію і функціональні можливості.
2. Авторкою розроблено систему підтримки прийняття рішень щодо вибору OSINT-інструментів на основі критеріїв оцінювання та механізму ранжування інструментів відповідно до поставлених задач інформаційної безпеки.
3. Практична частина роботи містить реалізацію системи для автоматизованого вибору OSINT-інструментів із використанням сучасних технологій веб-розробки та програмування.
4. Кваліфікаційна робота оформлена відповідно до встановлених вимог. Матеріал викладено логічно та послідовно, а результати дослідження доповнено таблицями, схемами та ілюстраціями.

Недоліки.

Доцільно було б більш детально розглянути можливості подальшого розширення бази знань системи, а також реалізацію інтеграції з реальними API OSINT-сервісів для автоматичного оновлення характеристик інструментів.

Однак зазначені зауваження не впливають на загальну позитивну оцінку кваліфікаційної роботи.

Висновок: Кваліфікаційна робота виконана на належному науково-методичному рівні і заслуговує оцінки “відмінно”, а здобувачка КЛОПОВА Анна заслуговує присвоєння кваліфікації бакалавра з кібербезпеки за освітньою програмою Управління інформаційною та кібернетичною безпекою.

Рецензент:		Сергій ГАХОВ
к.військ.н., доцент	*підпис*	Ім’я, ПРІЗВИЩЕ

РЕФЕРАТ

Кваліфікаційна робота присвячена дослідженню підходів до вибору та застосування OSINT-інструментів для вирішення завдань інформаційної безпеки. Робота складається зі вступу, трьох розділів, що містять 17 рисунків, висновків і списку використаних джерел із 37 найменувань. Загальний обсяг роботи становить 84 аркушів, з яких 5 аркуші займають перелік умовних скорочень і список використаних джерел.

Метою роботи є розроблення системи підтримки вибору OSINT-інструментів для ефективного виконання завдань інформаційної безпеки.

Об'єктом дослідження є процес використання технологій OSINT у сфері інформаційної безпеки.

Предмет дослідження - методи, критерії та підходи до вибору OSINT-інструментів залежно від типу завдань інформаційної безпеки.

Методи дослідження. Для вирішення поставлених завдань у роботі використані методи аналізу та синтезу, порівняння, класифікації, систематизації, експертної оцінки, а також системний підхід до забезпечення інформаційної безпеки.

Як результат у роботі проаналізовано роль OSINT у забезпеченні інформаційної безпеки, досліджено основні типи OSINT-інструментів та їх функціональні можливості; визначено критерії вибору OSINT-засобів залежно від поставлених задач; розроблено систему підтримки вибору OSINT-інструментів і практичні рекомендації щодо її застосування.

Галузь застосування. Розроблені підходи можуть бути використані фахівцями з інформаційної безпеки, аналітиками та спеціалістами SOC/CSIRT під час проведення розслідувань, моніторингу загроз, аналізу інцидентів та оцінки ризиків на основі відкритих джерел інформації.

Ключові слова: OSINT, ІНФОРМАЦІЙНА БЕЗПЕКА, ВІДКРИТІ ДЖЕРЕЛА, АНАЛІЗ ДАНИХ, КІБЕРРОЗВІДКА, СИСТЕМА ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ, ВИБІР ІНСТРУМЕНТІВ, МОНІТОРИНГ ЗАГРОЗ.

ABSTRACT

The qualification work is devoted to the study of approaches to the selection and application of OSINT tools for solving information security tasks. The thesis consists of an introduction, three chapters containing 17 figures, conclusions, and a list of references including 37 sources. The total volume of the thesis is 84 pages, of which 5 pages are devoted to the list of abbreviations and the list of references.

The purpose of the study is to develop a decision support system for selecting OSINT tools to effectively perform information security tasks.

The object of the study is the process of using OSINT technologies in the field of information security.

The subject of the study is methods, criteria, and approaches to selecting OSINT tools depending on the type of information security tasks.

Research methods. To achieve the objectives of the thesis, the following methods were used: analysis and synthesis, comparison, classification, systematization, expert evaluation, as well as a systematic approach to ensuring information security.

As a result, the thesis analyzes the role of OSINT in ensuring information security, investigates the main types of OSINT tools and their functional capabilities, defines criteria for selecting OSINT tools depending on the tasks, develops a decision support system for OSINT tool selection, and provides practical recommendations for its application.

Field of application. The developed approaches can be used by information security specialists, analysts, and SOC/CSIRT professionals during investigations, threat monitoring, incident analysis, and risk assessment based on open-source information.

Keywords: OSINT, INFORMATION SECURITY, OPEN SOURCES, DATA ANALYSIS, CYBER THREAT INTELLIGENCE, DECISION SUPPORT SYSTEM, TOOL SELECTION, THREAT MONITORING.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ І СКОРОЧЕНЬ

ІБ	Інформаційна безпека
ПЗ	Програмне забезпечення
СУБД	Система управління базами даних
СУІБ	Система управління інформаційною безпекою
OSINT	Open Source Intelligence
SOC	Security Operations Center
SOCMINT	Social Media Intelligence
EXIF	Exchangeable Image File Format
GEOINT	Geospatial Intelligence
СППР	Системи Підтримки Прийняття Рішень
GUI	Graphical User Interface
CLI	Command-Line Interface
API	Application Programming Interface
DNS	Domain Name System

ВСТУП

Актуальність теми. В умовах повномасштабної війни проти України роль OSINT значно зросла як у державному секторі, так і в діяльності приватних компаній, критичної інфраструктури та медіа. Відкриті джерела стали ключовим інструментом для оперативного виявлення інформаційно-психологічних операцій, фіксації воєнних злочинів, аналізу кібератак і пошуку витоків персональних та корпоративних даних. Використання OSINT дозволяє отримувати актуальну інформацію про загрози, формувати уявлення про потенційні ризики та підтримувати процеси прийняття рішень у сфері інформаційної безпеки.

Сьогодні існує значна кількість OSINT-інструментів, які відрізняються функціональними можливостями, рівнем автоматизації, точністю результатів, умовами доступу, обмеженнями використання та складністю інтеграції у процеси інформаційної безпеки. Через це вибір оптимального інструменту для конкретного завдання часто є складним і потребує значного часу, досвіду та глибокого розуміння специфіки кожного рішення.

У зв’язку з цим виникає необхідність створення системи підтримки прийняття рішень, яка дозволить автоматизувати процес вибору OSINT-інструментів відповідно до конкретних завдань інформаційної безпеки, підвищити ефективність OSINT-досліджень та зменшити ризик помилок під час аналізу відкритих джерел.

Мета роботи полягає у розробці системи підтримки вибору OSINT-інструментів для вирішення завдань інформаційної безпеки.

Об’єкт дослідження - процес використання технологій OSINT у сфері інформаційної безпеки.

Предмет дослідження - методи, критерії та підходи до побудови системи підтримки прийняття рішень щодо вибору OSINT-інструментів залежно від типу завдань інформаційної безпеки.

Новизна одержаних результатів полягає в удосконаленні процесу вибору

OSINT-інструментів за рахунок впровадження системи критеріїв оцінювання (рівень автоматизації, наявність API, зручність використання, точність, швидкість, вартість, можливість експорту та інтеграції) і шкали визначення інтегрального показника ефективності, що дозволило забезпечити раціональний вибір інструментів та скоротити час, необхідний для аналізу доступних засобів OSINT.

Для досягнення поставленої мети необхідно виконати наступні завдання:

1. Проаналізувати основні методи, критерії та підходи до вибору OSINT-інструментів залежно від типу завдань інформаційної безпеки.

2. Дослідити роль OSINT у процесах підтримки прийняття рішень та розробити систему вибору OSINT-інструментів залежно від типу завдань інформаційної безпеки.

3. Провести експериментальну перевірку ефективності запропонованої системи підтримки вибору OSINT-інструментів.

Методи дослідження. Для вирішення означеного вище наукового завдання в роботі використано методи аналізу та узагальнення для дослідження сучасних підходів до застосування OSINT у сфері інформаційної безпеки, методи класифікації для систематизації OSINT-інструментів та їх функціональних характеристик, методи порівняння для визначення переваг і обмежень інструментів, а також елементи системного підходу і моделювання для розробки системи підтримки вибору та її архітектури.

Практичне значення одержаних результатів. Розроблена система підтримки вибору OSINT-інструментів може бути використана фахівцями з інформаційної безпеки, аналітиками SOC/CSIRT та спеціалістами з кіберрозвідки для оптимізації процесу підбору інструментів, скорочення часу проведення OSINT-досліджень.

Апробація результатів кваліфікаційної роботи відбулася на Всеукраїнській науково-практичній конференції “Стратегії кіберстійкості: управління ризиками та безперервність бізнесу” 25 лютого 2026 року.

РОЗДІЛ 1 АНАЛІЗ СИСТЕМ ПІДТРИМКИ ВИБОРУ OSINT-ІНСТРУМЕНТІВ

У першому розділі проводиться комплексний аналіз ролі OSINT-інструментів у сучасній системі забезпечення інформаційної безпеки.

Досліджуються основні напрями застосування інструментарію відкритої розвідки для виявлення загроз та аналізу кібератак. Значна увага приділяється класифікації існуючих OSINT-засобів та детальному вивченню їхніх функціональних можливостей.

1.1 Основні напрями застосування OSINT для вирішення завдань інформаційної безпеки

У сфері інформаційної безпеки OSINT вважається одним із інструментів прогнозування, виявлення та протидії загрозам. Його основною особливістю є те, що інформація отримується з легальних, загальнодоступних джерел, що дозволяє використовувати OSINT не тільки у військовій чи державній сферах, а й у корпоративному секторі: для оцінки ризиків, аналізу репутаційних ризиків, моніторингу витоків інформації та розслідування кіберзлочинів. У наукових публікаціях підкреслюється, що технології OSINT у сфері інформаційної безпеки використовуються для прогнозування, виявлення та відбиття загроз шляхом систематичного збору та аналізу загальнодоступних даних [1].

Практичне значення OSINT у сфері інформаційної безпеки полягає в тому, що його можна використовувати для отримання інформації про загрози та вразливості ззовні, не втручаючись безпосередньо в інформаційні системи. Це робить OSINT важливим інструментом для роботи аналітичних центрів, служб корпоративної безпеки, SOC, підрозділів CERT/CSIRT, а також для роботи правоохоронних органів.

Застосування OSINT не обмежується лише збором інформації. Важливою складовою є аналітична обробка даних: кореляція, виявлення закономірностей, оцінка достовірності та формування висновків. У цьому контексті OSINT

виступає як методологія, що включає комплекс етапів: планування, збір, обробка, аналіз, верифікація, представлення результатів. Такий підхід забезпечує можливість використання OSINT у багатьох напрямках інформаційної безпеки.

Згідно з матеріалами досліджень, можна виділити кілька основних напрямів застосування OSINT для вирішення завдань інформаційної безпеки: моніторинг витоків даних, протидія соціальній інженерії та фішингу, виявлення шкідливих ресурсів, кіберрозвідка щодо атакуючих груп, оцінка Attack Surface організацій, протидія дезінформації та підтримка цифрових розслідувань [1–6].

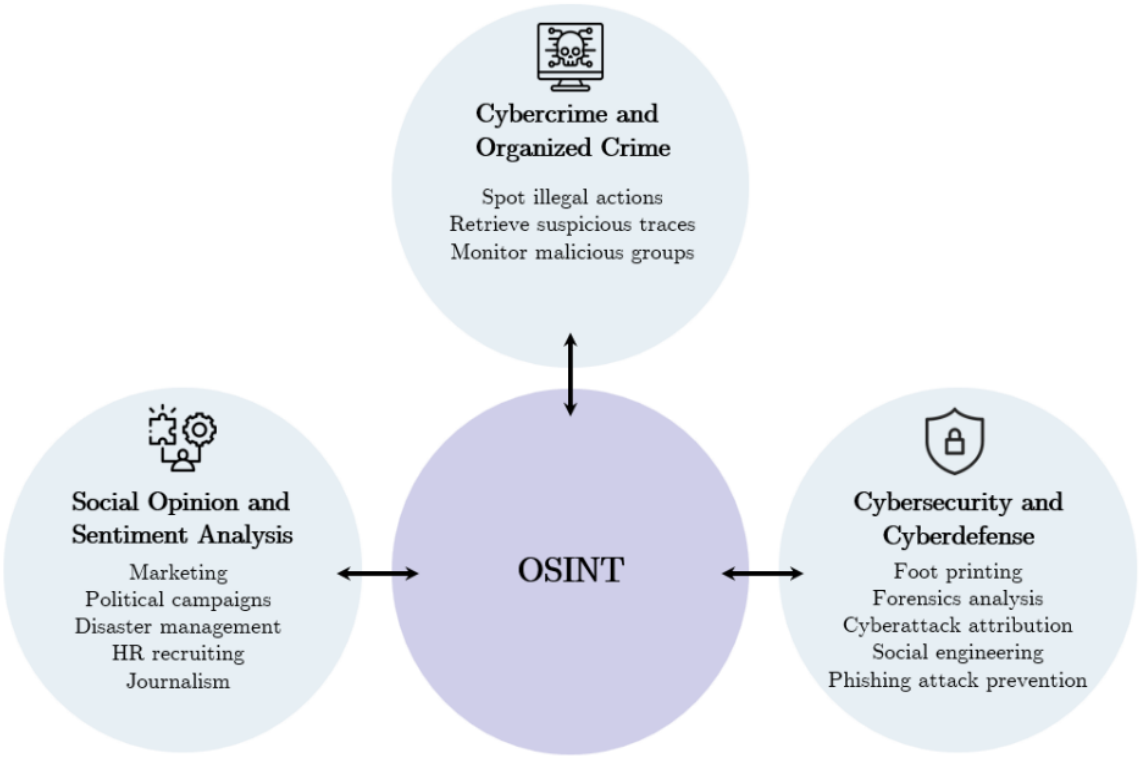


Рис. 1.1.1. Основні сфери застосування OSINT.

1.1.1 Моніторинг витоків інформації

Одним із найважливіших напрямів застосування OSINT у сфері інформаційної безпеки є *моніторинг витоків інформації*. У сучасних умовах витоки конфіденційних даних є однією з найпоширеніших загроз для організацій, оскільки можуть призвести до фінансових втрат, репутаційних ризиків, компрометації внутрішніх систем та порушення законодавства щодо

захисту персональних даних.

OSINT дозволяє виявляти факти оприлюднення конфіденційної інформації у відкритих джерелах. Зокрема, витоки можуть публікуватися у вигляді файлів або баз даних на форумах, у публічних чатах, на ресурсах для обміну файлами, у репозиторіях з відкритим кодом, а також у месенджерах (особливо в Telegram-каналах). У статті, присвяченій застосуванню OSINT у кібербезпеці, підкреслюється, що моніторинг відкритих джерел дає можливість швидко виявляти компрометацію логінів, паролів, службових документів або внутрішніх інструкцій, які можуть використовуватися зловмисниками для подальших атак [2].

Практичне значення такого моніторингу полягає в можливості оперативного реагування. Наприклад, якщо виявлено витік облікових даних, організація може швидко здійснити зміну паролів, активувати багатофакторну автентифікацію або обмежити доступ до критичних ресурсів. Якщо витік стосується внутрішньої документації чи конфігураційних файлів, можна провести аудит доступів, змінити політики безпеки та усунути першопричину витоку.

Моніторинг витоків інформації за допомогою OSINT також дозволяє оцінити масштаб інциденту. Наприклад, аналіз оприлюднених даних дає змогу визначити, чи стосується витік окремого підрозділу або всієї організації, чи включає він персональні дані, фінансову інформацію або технічні параметри систем. У цьому контексті OSINT використовується як інструмент раннього виявлення загроз, що забезпечує можливість мінімізувати наслідки інциденту.

У матеріалах дослідження також підкреслюється, що відкриті витоки часто є індикатором недостатньої внутрішньої політики захисту інформації, зокрема відсутності контролю доступів, недосконалого управління обліковими записами або слабкої культури інформаційної безпеки серед персоналу [2]. Отже, OSINT у цьому напрямі використовується не лише як реактивний інструмент, але й як механізм оцінки рівня зрілості безпекових процесів організації.

Таким чином, моніторинг витоків інформації є одним із ключових

напрямів застосування OSINT, оскільки забезпечує організації можливість виявляти загрозу на ранньому етапі, реагувати на інциденти та вдосконалювати систему захисту інформації [2].

1.1.2 Аналіз соціальної інженерії та фішингу

Соціальна інженерія є одним із найефективніших способів реалізації кібератак, оскільки вона спрямована на використання людського фактора. Фішинг, підроблені повідомлення, маніпуляції довірою та психологічні методи впливу на працівників організацій часто застосовуються зловмисниками для отримання доступу до конфіденційної інформації або корпоративних систем.

OSINT відіграє важливу роль у дослідженні соціальної інженерії, оскільки дозволяє аналізувати цифрову присутність організації та її співробітників. У відкритих джерелах можуть бути доступні відомості про структуру компанії, посадові обов'язки працівників, корпоративні контакти, адреси електронної пошти, інформація про внутрішні процеси, а також відомості про партнерів та постачальників. Такі дані можуть бути використані зловмисниками для формування переконливих фішингових сценаріїв.

OSINT дозволяє виявляти слабкі місця у публічній інформаційній політиці організації та прогнозувати можливі сценарії соціальної інженерії [1]. Наприклад, якщо у відкритому доступі містяться контакти керівників, відомості про відрядження працівників або внутрішні корпоративні новини, зловмисники можуть використовувати ці дані для створення фальшивих листів чи повідомлень, які виглядатимуть правдоподібно.

Застосування OSINT у сфері протидії фішингу може бути як аналітичним, так і профілактичним. Аналітична складова полягає у виявленні підроблених доменів, сторінок або акаунтів, що імітують офіційні ресурси організації. Профілактична складова включає аналіз того, які дані про співробітників є доступними у відкритому доступі, та визначення рівня ризику використання цих даних для атаки.

Зокрема, OSINT може допомогти виявити:

- інформацію про посади та функції працівників,

- відкриті контактні дані,
- корпоративні адреси електронної пошти,
- зв’язки між працівниками у соціальних мережах,
- згадки про внутрішні проєкти та технічні рішення.

На основі такого аналізу організація може коригувати політики публічної інформації, проводити навчання працівників, а також обмежувати надлишкову публічність даних.

Таким чином, OSINT у напрямі протидії соціальній інженерії виконує функцію виявлення інформаційних ризиків, пов’язаних із людським фактором. Це дозволяє підвищити рівень захищеності організації шляхом усунення джерел даних, які можуть бути використані для фішингових атак.

1.1.3 Виявлення та блокування шкідливих ресурсів

Виявлення шкідливих ресурсів є ще одним важливим напрямом застосування OSINT у сфері інформаційної безпеки. Шкідливі ресурси можуть включати фішингові сайти, підроблені сторінки авторизації, домени-клони, шкідливі скрипти, а також сервіси, що використовуються для розповсюдження шкідливого програмного забезпечення.

OSINT-інструменти дозволяють аналізувати:

- відкриті доменні дані,
- реєстраційну інформацію,
- хостинг-платформи,
- DNS-записи,
- IP-адреси.

Завдяки цьому можна виявляти підозрілі домени, що використовуються для атак, ще до того, як вони спричинять масові інциденти.

У матеріалах, присвячених демонстрації OSINT-методів, зазначається, що OSINT може застосовуватися для пошуку фішингових ресурсів шляхом аналізу доменних імен, схожих на легітимні, а також шляхом перевірки мережевої інфраструктури, пов’язаної з підозрілими сайтами [3]. Наприклад, якщо домен організації має відомий формат (company.ua), зловмисники можуть створити

домен company-login.ua або company-secure.com. OSINT-аналіз дозволяє знаходити такі домени, визначати дату їх реєстрації, географію хостингу та технічні характеристики.

Після виявлення шкідливого ресурсу можливе застосування практичних заходів реагування: внесення домену або IP-адреси до чорних списків, блокування на рівні корпоративної мережі, інформування користувачів, а також повідомлення відповідним організаціям.

OSINT у цьому напрямі також використовується для моніторингу появи нових шкідливих доменів та ресурсів, пов'язаних з конкретною організацією. Це є важливою складовою превентивного захисту, оскільки дозволяє виявляти загрозу ще до того, як вона стане масштабною. Даний етап є циклічним. Схема наведена на Рис. 1.1.2.

Рис. 1.1.2. Схема виявлення та блокування шкідливих ресурсів за допомогою OSINT

Таким чином, OSINT-методи та інструменти забезпечують можливість

виявлення шкідливих ресурсів у відкритому просторі та формування заходів для їх блокування, що підвищує рівень кіберзахисту організації [3].

1.1.4 Кібер- та інформаційна розвідка щодо атакуючих груп

OSINT активно використовується для збору даних про кіберзлочинні групи, їхню інфраструктуру та методи роботи. Це дозволяє організаціям та фахівцям з інформаційної безпеки формувати уявлення про потенційних противників, прогнозувати можливі сценарії атак та вдосконалювати захист.

У наукових матеріалах зазначається, що OSINT у цьому напрямі включає аналіз відкритих форумів, соціальних мереж, технічних платформ, де обговорюються інструменти атак, витоки даних, продаж доступів до систем або обмін шкідливими програмами [4]. Зібрана інформація може бути використана для ідентифікації тактик, технік і процедур (TTPs), які застосовуються атакуючими групами.

Особливу роль у кіберрозвідці відіграє аналіз інфраструктури зловмисників: доменів, IP-адрес, серверів керування та контролю, CDN-мереж, а також технічних параметрів, що можуть бути пов’язані з певними групами. У багатьох випадках OSINT дозволяє виявити повторювані шаблони використання доменів, хостингів або інструментів, що допомагає здійснювати атрибуцію атак або принаймні визначати тип загрози.

У цьому напрямі OSINT використовується також для аналізу публічних повідомлень про кібератаки. Наприклад, після великого інциденту можуть з’являтися публікації зловмисників або їхніх «заяв» щодо відповідальності. Аналіз таких матеріалів дозволяє встановити контекст подій та оцінити реальний рівень загрози.

Таким чином, кіберрозвідка на основі OSINT є важливим елементом Threat Intelligence та дозволяє організаціям не лише реагувати на атаки, а й здійснювати прогнозування майбутніх загроз на основі аналізу відкритої інформації [4].

1.1.5 Оцінка Attack Surface організацій

Оцінка Attack Surface є важливим напрямом інформаційної безпеки, який передбачає аналіз того, які цифрові об’єкти організації доступні ззовні. До таких

об’єктів належать веб-сайти, домени, піддомени, відкриті IP-адреси, API, хмарні сервіси, сервери електронної пошти, VPN-шлюзи, системи дистанційного доступу та інші компоненти інфраструктури.

OSINT-інструменти дозволяють здійснювати таку оцінку без прямого проникнення в мережу організації. Для цього використовуються інструменти типу WHOIS, Shodan, Censys, пошукові системи, а також аналіз відкритої технічної документації. У навчальних та аналітичних матеріалах зазначається, що OSINT є одним із найбільш ефективних методів попередньої оцінки Attack Surface, оскільки дозволяє виявляти неочевидні ресурси, наприклад тестові сервери або застарілі піддомени [5].

Аналіз Attack Surface може включати виявлення неправильно налаштованих сервісів, відкритих портів, витоків конфігурацій, відкритих директорій або доступних панелей адміністрування [5]. Наприклад, інструменти мережевого пошуку можуть показати, що певний сервер використовує застарілу версію програмного забезпечення або має відкриті служби, які не повинні бути доступними з Інтернету.

Практичне значення OSINT у цьому напрямі полягає в можливості виявлення ризиків ще до того, як ними скористається зловмисник. Це дозволяє організації здійснювати профілактичні заходи: закривати зайві порти, оновлювати програмне забезпечення, змінювати конфігурації, обмежувати доступ до сервісів, впроваджувати захисні механізми.

Отже, оцінка Attack Surface за допомогою OSINT є важливим напрямом, що дозволяє організаціям контролювати власну цифрову присутність та підвищувати рівень кіберстійкості [5].

1.1.6 Протидія дезінформації та інформаційним операціям

Однією з актуальних загроз сучасного інформаційного середовища є поширення дезінформації, маніпулятивного контенту та інформаційних операцій, які можуть впливати на репутацію організацій, формувати паніку або спричиняти соціальні конфлікти. У цьому контексті OSINT є ефективним інструментом для моніторингу інформаційного простору.

У статті, присвяченій використанню OSINT у кібербезпеці, зазначається, що методи OSINT дозволяють виявляти фейкові повідомлення, координовані кампанії, а також групи акаунтів, які діють узгоджено з метою впливу на громадську думку [2]. Аналіз може включати дослідження динаміки поширення контенту, визначення джерел первинної публікації, аналіз мережі репостів та коментарів.

Особливо важливим є виявлення бот-мереж. Бот-мережі можуть створювати ілюзію масової підтримки або навпаки - масового негативу щодо певної організації. OSINT-аналіз дозволяє визначати аномальну активність, наприклад велику кількість однакових повідомлень, синхронність публікацій або підозрілу структуру акаунтів.

Практичне значення OSINT у цьому напрямі полягає в тому, що результати аналізу можуть бути використані для: інформаційного реагування, підготовки спростувань, посилення комунікаційної стратегії, а також для технічного блокування джерел (у межах можливостей платформ чи внутрішніх корпоративних політик). У деяких випадках такі дані можуть передаватися компетентним органам для подальшого реагування.

Таким чином, OSINT виступає інструментом не лише кіберзахисту, а й інформаційної стійкості організації, оскільки дозволяє виявляти загрози у медіасередовищі та протидіяти інформаційним атакам [2].

1.1.7 Підтримка розслідувань та цифрових слідчих дій

OSINT широко застосовується у цифрових розслідуваннях, оскільки відкриті джерела можуть містити важливі дані для встановлення обставин події, авторства, зв’язків між об’єктами та хронології дій. Це актуально як для правоохоронних органів, так і для внутрішніх служб безпеки підприємств.

У наукових матеріалах, присвячених застосуванню OSINT у слідчій діяльності, зазначається, що відкриті джерела дозволяють формувати доказову базу шляхом збору метаданих фото і відео, аналізу історії публікацій, встановлення геолокаційних ознак та зіставлення інформації з різних ресурсів [6]. Наприклад, за допомогою OSINT можна встановити час і місце створення

фото або відео, якщо збережено відповідні метадані, або знайти первинне джерело поширення контенту через веб-архіви чи пошукові механізми.

У межах розслідувань OSINT може використовуватися для:

- пошуку профілів осіб у соціальних мережах;
- встановлення зв'язків між акаунтами;
- аналізу цифрового сліду користувача;
- збору інформації з відкритих державних реєстрів;
- підтвердження або спростування певних фактів через незалежні джерела.

Відкриті джерела можуть бути ефективним інструментом для побудови аналітичної моделі події, встановлення хронології та перевірки достовірності даних [6]. Це особливо важливо в умовах, коли значна частина комунікацій відбувається в цифровому середовищі.

Таким чином, застосування OSINT у цифрових розслідуваннях дозволяє суттєво розширити можливості збору доказів та аналітичної підтримки слідчих дій, що підвищує ефективність роботи служб безпеки та правоохоронних органів.

1.2 Класифікація OSINT-інструментів та аналіз їх функціональних можливостей

Систематизація OSINT-інструментів здійснюється за допомогою класифікації, яка дозволяє впорядкувати наявні рішення та визначити найбільш доцільні напрямки їх застосування. Найбільш поширеними підходами є класифікація за типом джерела інформації та класифікація за функціональним призначенням [5, 7].

Перший підхід дозволяє визначити, з якими інформаційними середовищами працює інструмент (веб, соцмережі, реєстри, архіви). Другий підхід описує роль інструмента у межах OSINT-процесу (збір, обробка, аналіз, кореляція, візуалізація).

У даному розділі розглядаються обидва підходи класифікації, а також

аналізуються функціональні можливості основних груп OSINT-інструментів, що застосовуються у сфері інформаційної безпеки.

1.2.1 Пошукові системи та спеціалізовані OSINT-пошуки

Пошукові системи є базовим інструментом OSINT, оскільки вони забезпечують доступ до значної кількості веб-ресурсів і дозволяють здійснювати пошук за ключовими словами, фразами, файлами та доменами. У задачах інформаційної безпеки пошукові системи використовуються не тільки для загального пошуку, а й для застосування спеціальних операторів пошуку (dorking), що дозволяє виявляти потенційно небезпечну інформацію у відкритому доступі [7].

Пошукові оператори дозволяють знаходити документи, резервні копії, відкриті каталоги, конфігураційні файли, службові сторінки веб-додатків, які можуть бути помилково опубліковані. Це створює ризики витоку конфіденційної інформації, а також сприяє формуванню attack surface організації [7].

Серед інструментарію для проведення розвідки мережевої інфраструктури особливе місце посідає платформа *Shodan.io*. На відміну від традиційних пошукових систем, які орієнтовані на індексацію контенту вебсторінок, Shodan спеціалізується на зборі та аналізі метаданих пристроїв, що безпосередньо підключені до мережі Інтернет. Це дозволяє ідентифікувати не лише вебресурси, а й компоненти критичної інфраструктури, зокрема системи промислового управління, вузли «інтернету речей», маршрутизатори та камери відеоспостереження [5, 7].

Ключові функціональні можливості системи:

- Платформа забезпечує ідентифікацію широкого спектра пристроїв - від побутових «розумних» приладів до складних промислових об’єктів, що функціонують у відкритому цифровому просторі [7, 10].
- Shodan дозволяє здійснювати моніторинг відкритих портів та використовуваних мережевих протоколів, що є критично важливим для виявлення потенційних векторів атак та вразливостей конфігурації [7, 10].
- Інструментарій системи надає можливість проводити глобальний

моніторинг, відстежуючи стан конкретних підмереж, діапазонів IP-адрес або цілих географічних регіонів у режимі реального часу [7, 10].

- Висока точність пошуку досягається шляхом використання складних запитів, що включають фільтрацію за версіями програмного забезпечення, SSL-сертифікатами, заголовками HTTP-запитів та іншими технічними відбитками [7, 10].

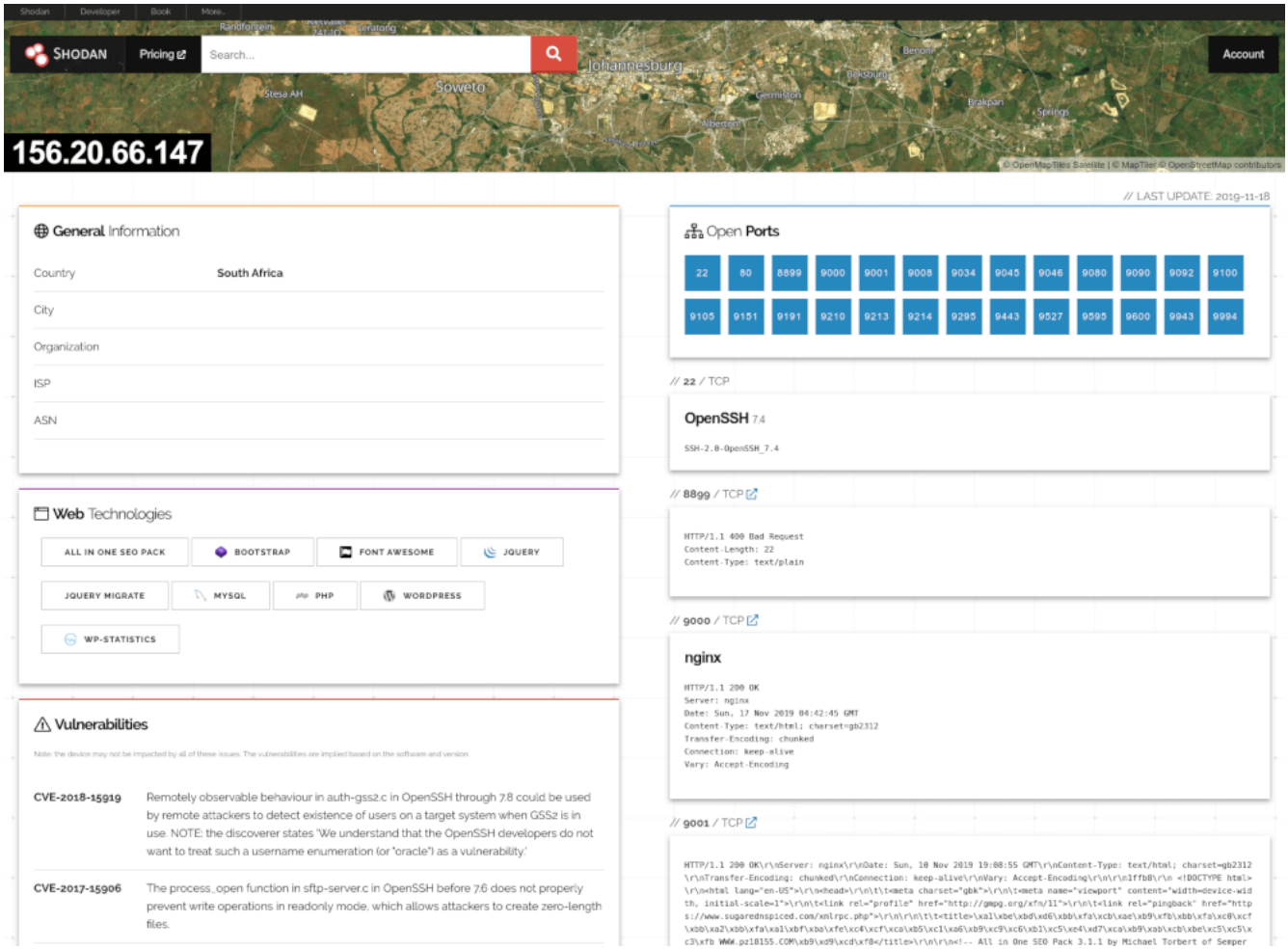


Рис. 1.2.1. Приклад аналізу IP-адреси через пошукову систему Shodan

Ще одним прикладом є сервіси, орієнтовані на витоки даних, наприклад *Have I Been Pwned*. Подібні інструменти дозволяють визначати, чи фігурує певна електронна адреса або домен у базах даних витоків. Такий аналіз застосовується для оцінки ризиків компрометації облікових записів, а також для підготовки заходів реагування на інциденти [5].

Функціональні можливості цієї групи інструментів включають: пошук інформації про організацію, домени, IP-адреси; виявлення відкритих файлів та документів; аналіз інфраструктури та відкритих сервісів; виявлення компрометованих даних у публічному доступі [5, 7].

1.2.1 Соціальні мережі та месенджери

Соціальні мережі та месенджери є джерелом великої кількості інформації про людей, організації, події та комунікаційні процеси. У сфері інформаційної безпеки вони використовуються для збору даних про цифрову присутність, оцінки ризиків соціальної інженерії, моніторингу інформаційних кампаній та виявлення бот-мереж [5, 8].

Відкриті профілі користувачів можуть містити інформацію про місце роботи, професійні навички, контакти, коло спілкування, фотографії, геолокаційні дані. У контексті кібербезпеки це може використовуватись як для підготовки фішингових атак, так і для проведення аудиту відкритих даних, що можуть бути використані зловмисниками [8].

Twitter/X є важливим джерелом для моніторингу актуальних інформаційних подій, пошуку публічних заяв, аналізу хештегів та тенденцій. Facebook використовується для дослідження профілів, груп, сторінок організацій та спільнот. Telegram виступає платформою, яка містить значну кількість каналів і чатів, що можуть використовуватися для поширення витоків, дезінформації та координації підозрілих дій [8].

OSINT-інструменти для соціальних мереж є SOCMINT. Даний клас інструментів орієнтований на систематичний моніторинг, збір та верифікацію даних, що генеруються користувачами у соціальних мережах та месенджерах. Специфіка даного інструменту полягає у можливості деанонімізації суб’єктів та встановлення прихованих зв’язків через аналіз «цифрових слідів» у відкритому доступі [5].

Функціональна архітектура SOCMINT:

- Автоматизоване відстеження динаміки згадок, використання специфічних хештегів та аналіз тональності коментарів. Це дозволяє в режимі

реального часу ідентифікувати зародження інформаційних приводів або репутаційних загроз.

- Вивчення історії активності, хронології публікацій та метаданих контенту. Важливою функцією є крос-платформений пошук, що дозволяє об’єднати розрізнені акаунти в різних мережах (Twitter/X, Facebook, Telegram) в єдиний цифровий профіль об’єкта [5, 8].
- Використання алгоритмів машинного навчання для виявлення фейкових акаунтів. Інструменти аналізують швидкість публікацій, ідентичність контенту та нетипові графи зв’язків, що є критичним для протидії дезінформації та координованим атакам [8].
- Вилучення координат із публікацій та сторіз, що дозволяє верифікувати фізичне місцезнаходження об’єкта або підтвердити факт події у конкретній локації .

1.2.3 Веб-архіви та WHOIS

Веб-архіви дозволяють отримувати історичні версії веб-ресурсів та відновлювати інформацію, яка була видалена або змінена. *Wayback Machine* та *Archive.today* є найбільш відомими сервісами такого типу, що широко використовуються у цифрових розслідуваннях [5].

Застосування веб-архівів у інформаційній безпеці включає фіксацію доказів, аналіз змін контенту, дослідження історії домену та пошук ознак фішингових сторінок. Архівування може бути корисним при документуванні кіберінцидентів, оскільки забезпечує можливість підтвердити існування певної сторінки у конкретний момент часу [5].

Wayback Machine є незамінним ресурсом для збору та аналізу цифрових доказів та розслідувань, оскільки він зберігає понад 800 мільярдів веб-сторінок, що дозволяє відстежити історію цифрового об'єкта протягом десятиліть [7].

Функціональні можливості Wayback Machine:

- Сервіс дозволяє переглядати версії сайтів на певну дату в минулому. Це критично важливо для виявлення видаленої компрометуючої інформації, зміни риторики в публікаціях або видалення контактних даних зі сторінок

компаній, що намагаються приховати свою діяльність [7].

- Функціонал сервісу дозволяє порівнювати дві різні версії однієї сторінки. Система підсвічує додані фрагменти тексту синім кольором, а видалені - жовтим. Це дозволяє аналітику швидко ідентифікувати правки, внесені в офіційні документи, умови користування або біографічні дані на сайтах [7].
- Wayback Machine надає можливість візуалізувати архітектуру сайту за роками. Це допомагає досліднику зрозуміти, які розділи були активними в минулому (наприклад, старі форуми або закриті бази даних), що може дати підказки про структуру IT-інфраструктури об'єкта розвідки [7].

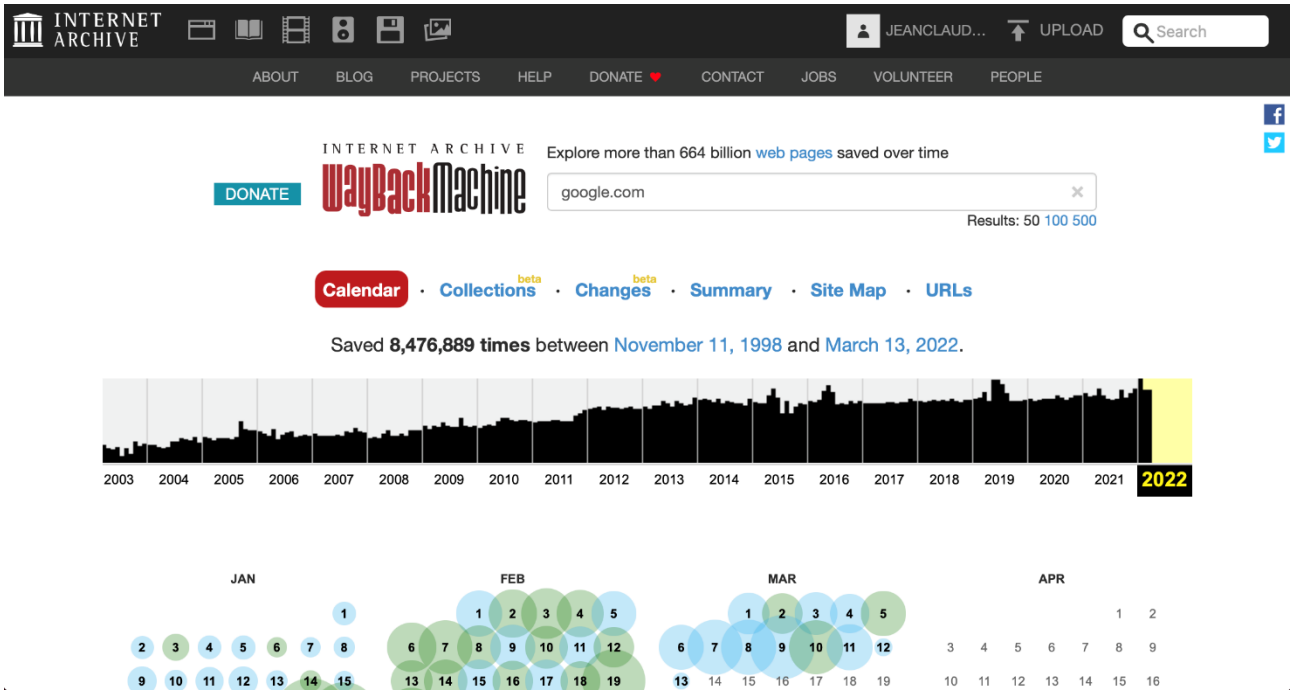


Рис. 1.2.2. Візуалізація інтенсивності архівації домену в Wayback Machine

У практиці OSINT-досліджень критичне значення мають інструменти створення статичних копій за запитом користувача. Провідним ресурсом у цій категорії є *Archive.today*. Даний сервіс спеціалізується на створенні моментальних «знімків» (snapshots) конкретних вебсторінок, забезпечуючи високу швидкість обробки даних та стійкість до обмежень доступу [12].

Аналіз функціональних можливостей:

- Сервіс орієнтований на створення статичних копій сторінок за

безпосереднім запитом користувача, що дозволяє миттєво фіксувати стан ресурсу в конкретний момент розслідування [12].

- На відміну від Wayback Machine, що фокусується на автоматичному та багатократному збереженні історії всього сайту, Archive.today концентрується на фіксації однієї, найбільш актуальної для дослідника версії сторінки [12].
- Платформа відома своєю здатністю архівувати контент навіть у випадках, коли доступ до сторінок заблоковано для інших пошукових та архівних ботів через налаштування сервера або географічні обмеження [12].

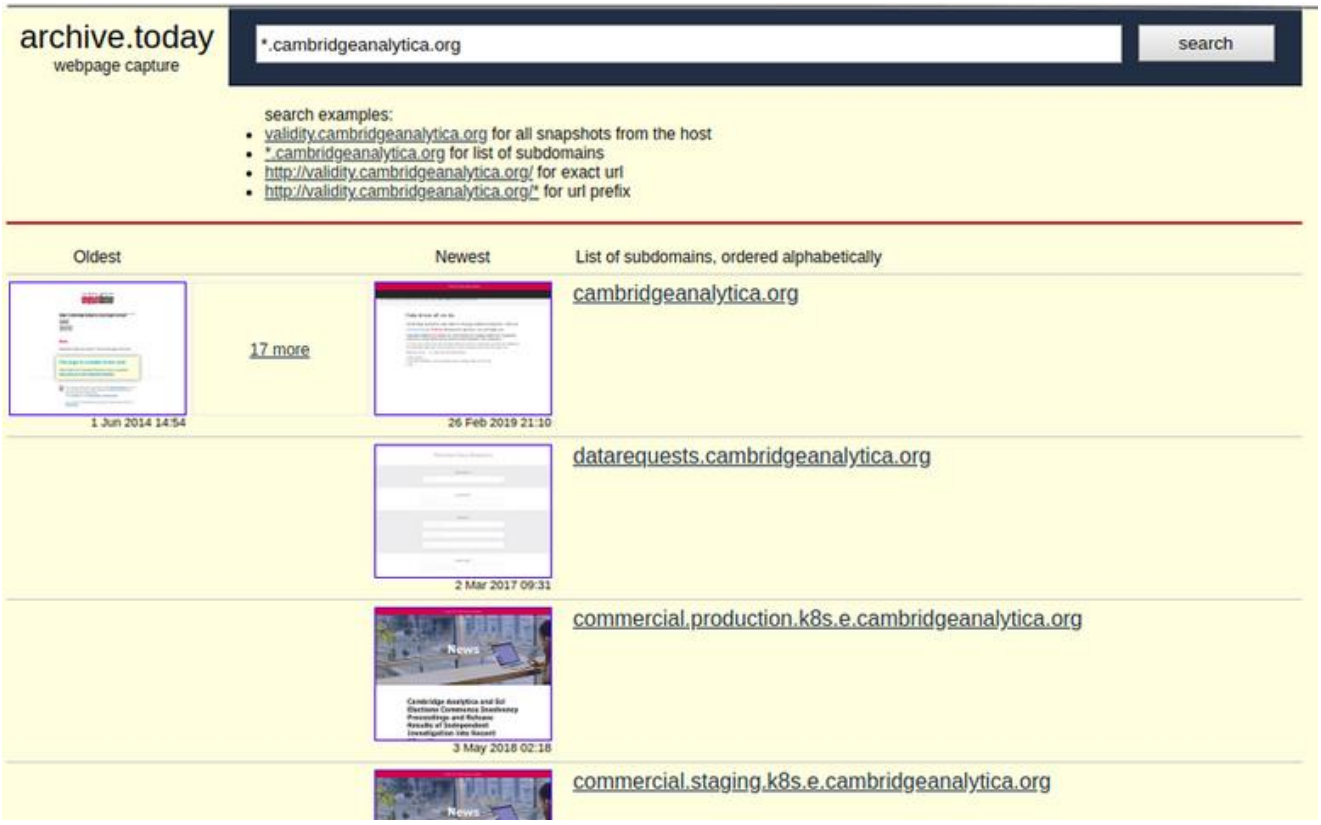


Рис. 1.2.3. Приклад запиту Archive.today

WHOIS-інструменти застосовуються для отримання інформації про домени: дата реєстрації, реєстратор, статус, іноді контактні дані або технічні параметри. Така інформація використовується для оцінки надійності доменів, виявлення підозрілих ресурсів та встановлення зв’язків між доменами [5, 7].

У практиці інформаційної безпеки WHOIS є важливим елементом аналізу фішингових атак, зареєстровані недавно або використовують однакових

реєстраторів [7].

Функціональні можливості цієї групи включають: ретроспективний аналіз сайтів, документування доказів, перевірку доменної інформації, встановлення часу створення домену та аналіз технічних параметрів доменної інфраструктури [7].

Таблиця 1.2.4.

Порівняння архітектурних підходів Wayback Machine та Archive.today

Параметр порівняння	**Wayback Machine**	**Archive.today**
Метод збору даних	Переважно автоматична індексація	За ініціативою користувача
Кількість версій	Численні варіанти на різні дати (Timeline)	Фокус на одній конкретній версії
Мета використання	Ретроспективний аналіз історії сайту	Миттєва фіксація доказів та обхід блокувань
Обробка блокувань	Дотримується обмежень robots.txt	Може ігнорувати технічні заборони архівації

1.2.4 Інструменти аналізу метаданих

Метадані є додатковою інформацією, яка супроводжує цифрові файли та може містити критично важливі відомості про походження даних. До метаданих належать EXIF-дані фото, технічні параметри відео, інформація про авторство документів, дати створення і редагування, дані про програмне забезпечення та пристрої. [10]

Аналіз метаданих у OSINT застосовується для встановлення достовірності матеріалів та перевірки їх автентичності. Наприклад, EXIF-дані можуть містити географічні координати, модель камери, дату і час створення зображення. У розслідуваннях це може бути використано як доказова інформація. [10]

ExifTool є одним із найбільш відомих та функціонально потужних інструментів для роботи з метаданими цифрових файлів. Він підтримує аналіз великої кількості форматів і дозволяє зчитувати, змінювати або видаляти метадані, що робить його універсальним засобом у OSINT-розслідуваннях. Інструмент широко використовується фахівцями з кібербезпеки та цифрової

криміналістики для перевірки походження файлів і встановлення прихованої інформації, яка може бути доказовою [13].

Функціональні можливості ExifTool:

- ExifTool дозволяє отримати повний перелік метаданих зображення або документа, включно з GPS-координатами, датою створення, типом пристрою та технічними параметрами. Це дає змогу визначити контекст створення файлу та перевірити його автентичність [13].
- Інструмент здатен зчитувати географічні координати, якщо вони були записані камерою або смартфоном. Це дозволяє визначати місце створення зображення та зіставляти координати з картографічними сервісами у рамках GEOINT-аналізу [13].
- ExifTool може показувати різні часові мітки: дату створення фото, дату редагування, дату експорту, що є важливим для встановлення хронології подій у цифрових розслідуваннях. Виявлення невідповідностей між часовими мітками може бути ознакою втручання або маніпуляції з файлом [13].
- Метадані можуть містити модель камери або смартфона, а також програму, яка використовувалась для редагування зображення (наприклад Photoshop або інші редактори). Це допомагає визначити, чи файл був змінений після створення, а також може вказувати на спосіб його отримання [13].

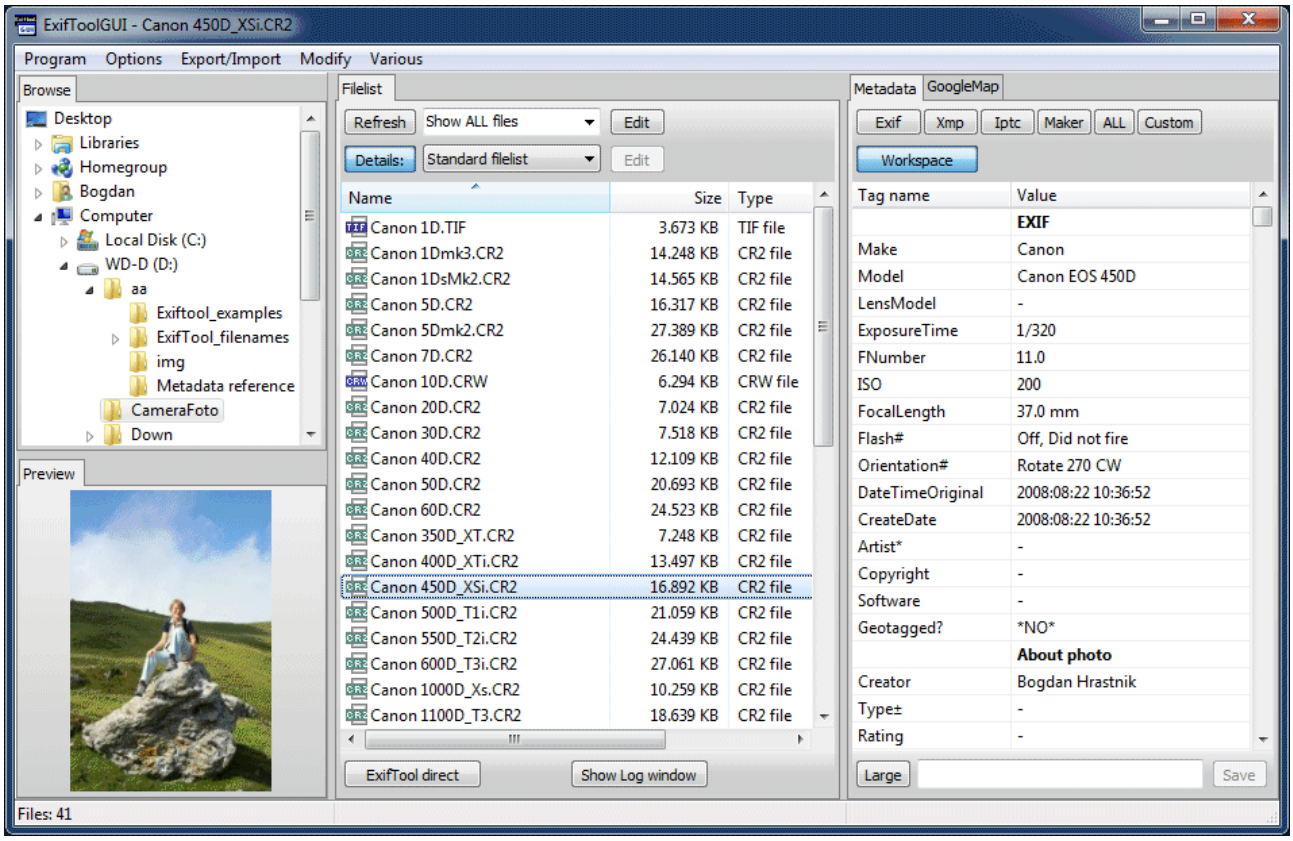


Рис. 1.2.4. Принцип роботи ExifTool by Phil Harvey

FotoForensics є спеціалізованим веб-сервісом, який використовується для аналізу цифрових зображень з метою виявлення ознак редагування або підробки. Його популярність у OSINT та цифрових розслідуваннях пояснюється тим, що він дозволяє швидко перевіряти підозрілі фотографії та виявляти області, які могли бути змінені у графічному редакторі. Це є важливим у випадках поширення фейкових фото або маніпуляційного контенту [27].

Функціональні можливості FotoForensics:

- Основною функцією FotoForensics є ELA-аналіз, який дозволяє виявляти різницю у рівнях стиснення окремих частин зображення. Якщо зображення редагувалося (наприклад, вставлявся інший об’єкт), відредаговані ділянки можуть мати інший рівень компресії та виділятися на ELA-карті. Це дає можливість визначати потенційні області підробки [27].
- Сервіс дозволяє оцінювати загальну структуру файлу та шукати аномальні ділянки, які можуть вказувати на накладання фрагментів, ретуш або зміну окремих об’єктів. Такий аналіз особливо важливий для перевірки фото, що

використовується у фейкових новинах або інформаційних операціях.

- Сервіс дозволяє аналізувати шум, структуру пікселів і градієнти, що може допомогти виявити замасковані зміни. Наприклад, при зміні тексту на зображенні або при вставці об’єктів часто з’являються нехарактерні артефакти.
- FotoForensics може виявляти ознаки обробки, що характерні для Photoshop та інших редакторів, якщо зображення зберігалося із відповідними параметрами. Це дозволяє зробити припущення щодо того, чи є фото оригінальним [7].

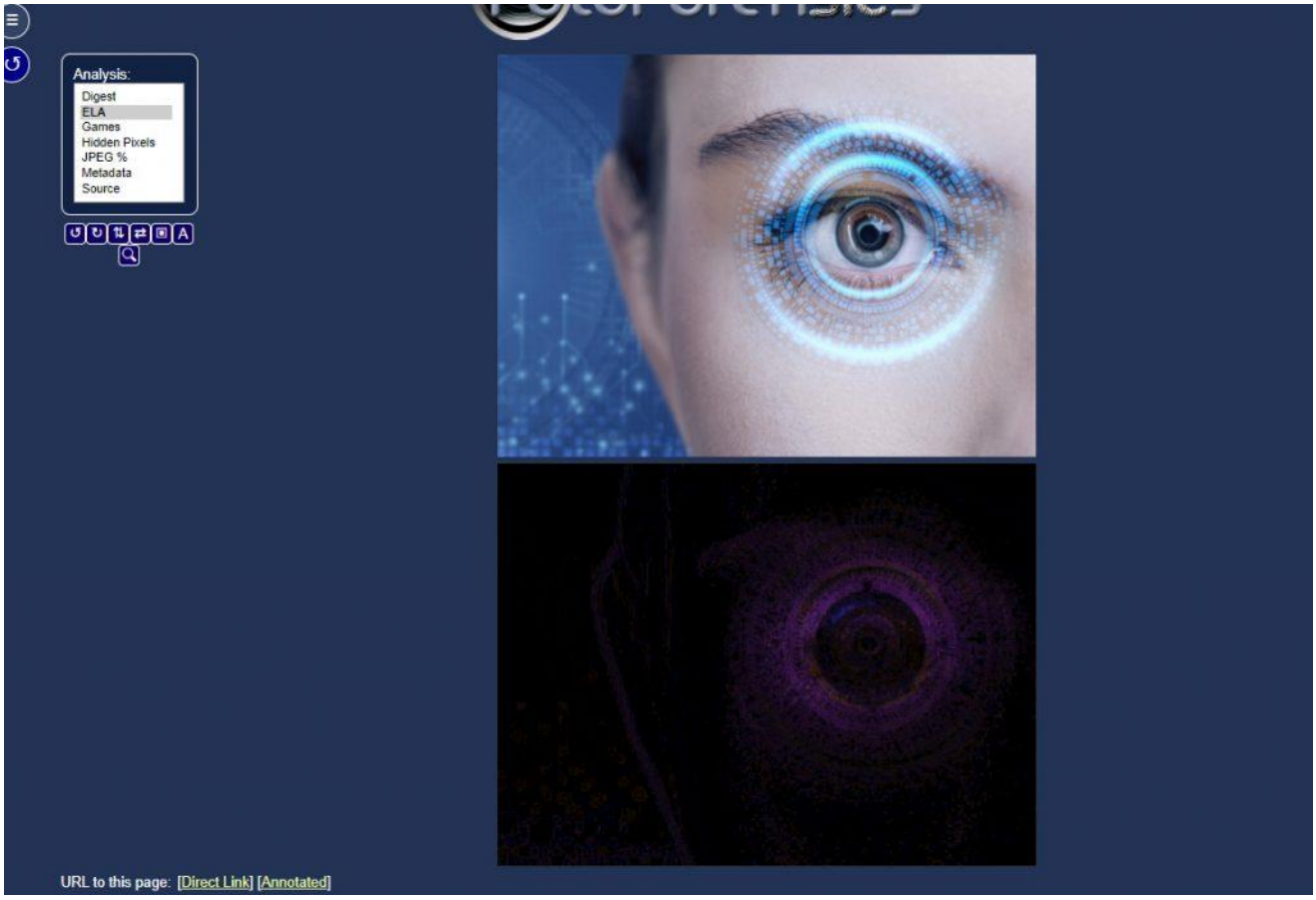


Рис. 1.2.5. Приклад, як виглядає змінене фото, за допомогою інструменту FotoForensics

1.2.5 Інструменти візуалізації та кореляції даних

Значна кількість даних, отриманих у процесі OSINT, потребує структуризації та аналізу зв’язків. Для цього використовуються інструменти кореляції та візуалізації, які дозволяють представити інформацію у вигляді

графів, схем, мережевих моделей або аналітичних діаграм. [5]

Графовий підхід є особливо ефективним для аналізу зв'язків між доменами, IP-адресами, акаунтами, організаціями та подіями. Maltego є прикладом інструмента, який дозволяє будувати мережі взаємозв'язків і застосовується для аналізу кіберзагроз та соціальних структур. [5, 8]

Програмне забезпечення *Maltego* є одним із найбільш затребуваних інструментів у сфері кіберрозвідки, оскільки воно дозволяє автоматизувати процес збору даних та візуалізувати складні інформаційні структури [5]. Основне призначення платформи полягає у пошуку та аналізі інформації у профілях соціальних мереж, ідентифікації за адресами електронної пошти, номерами телефонів та іншими ідентифікаторами [5].

Методологія роботи та базові компоненти:

Maltego здійснює пошук у відкритих джерелах, інтегрує отримані дані у єдині схеми та вибудовує логічні взаємозв'язки між ними. Для реалізації цього процесу в архітектурі системи використовуються три фундаментальні елементи:

- *Entities* - візуальне представлення одиниць інформації (наприклад, конкретна особа, доменне ім'я або IP-адреса).
- *Transforms* - спеціалізовані скрипти, що виконують пошук інформації в реальному часі та перетворюють один об'єкт на інший.
- *Links* - лінії, що демонструють логічну залежність та взаємодію між об'єктами на графіку.

Однією з ключових функцій програми є агрегація даних через Maltego Transform Hub - централізований вузол, що надає доступ до численних зовнішніх джерел та баз даних.

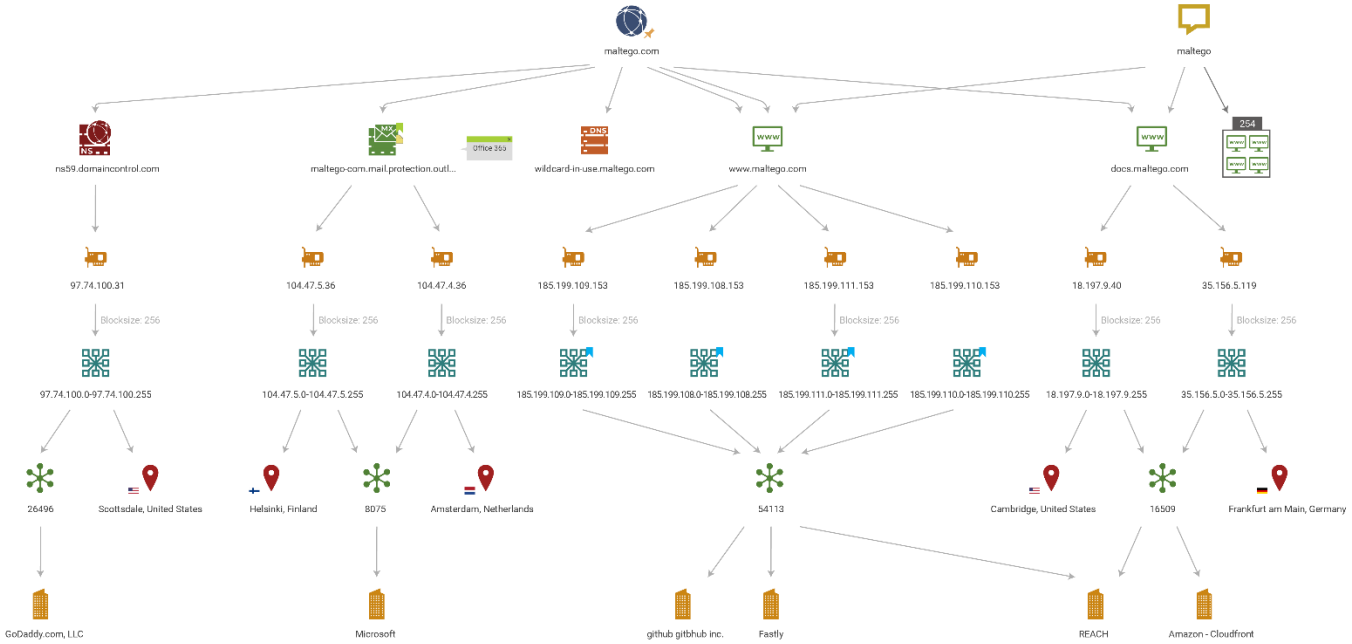


Рис. 1.2.6. Результат пошуку за запитом «домен maltego.com» в ПЗ Maltego

1.3 Проблематика вибору OSINT-інструментів і необхідність автоматизованої підтримки прийняття рішень

Вибір конкретного OSINT-інструмента для вирішення практичних завдань залишається складною проблемою, оскільки ринок OSINT-рішень характеризується великою кількістю сервісів, платформ і фреймворків, які відрізняються функціональністю, методами збору даних, точністю результатів та рівнем автоматизації [14].

Проблема вибору OSINT-інструментів також пов’язана з тим, що ефективність OSINT залежить не лише від інструмента, але й від методики його застосування, типу задачі, якості джерел та компетенцій аналітика. Тому організації часто стикаються з труднощами визначення найбільш доцільного інструмента для конкретної задачі, що зумовлює потребу у створенні СППР, які можуть автоматизувати вибір [5].

1.3.1 Надмірна кількість OSINT-інструментів та відсутність універсального рішення

Однією з основних проблем є те, що сучасний OSINT-сегмент включає сотні різних інструментів, сервісів та програмних платформ. Вони можуть бути

вузькоспеціалізованими (наприклад, для аналізу доменів або метаданих файлів) або комплексними (фреймворки для збору й кореляції даних). Через це вибір інструмента потребує попереднього аналізу можливостей кожного засобу та визначення, чи відповідає він конкретним завданням інформаційної безпеки [5].

У більшості випадків організація потребує не одного інструмента, а комплексу рішень, які доповнюють одне одного. Наприклад, для розслідування кіберінциденту можуть одночасно використовуватися пошукові системи, інструменти аналізу доменів, засоби перевірки витоків, сервіси аналізу соціальних мереж та інструменти візуалізації зв’язків. Такий підхід підвищує ефективність аналізу, але ускладнює вибір оптимальної конфігурації інструментів [14].

Важливим фактором є також постійні зміни у функціоналі OSINT-сервісів. Деякі платформи змінюють правила доступу до API, вводять платні обмеження або блокують автоматизований збір даних. У результаті навіть раніше ефективний інструмент може втратити актуальність або перестати бути доступним для організації [14].

Таким чином, проблема полягає у відсутності універсального OSINT-рішення, яке б забезпечувало повний цикл роботи з відкритими даними. Це створює необхідність розробки підходів до системного вибору інструментів [5].

1.3.2 Проблеми достовірності, повноти та актуальності OSINT-даних

Іншою важливою проблемою є те, що відкриті джерела не гарантують достовірності інформації. OSINT-дані можуть бути неповними, застарілими або навмисно викривленими, що особливо характерно для соціальних мереж та інформаційних ресурсів, де поширюється дезінформація. Це створює ризик отримання хибних аналітичних висновків та неправильних управлінських рішень [14].

Також проблемою є відсутність структурованості даних. Інформація з відкритих джерел часто подається у неструктурованому вигляді: текстові повідомлення, коментарі, зображення, відео або фрагменти вебсторінок. У результаті аналітик змушений витрачати значний час на попередню обробку

даних, що знижує оперативність реагування на загрози [14].

Особливу складність створює верифікація інформації. Наприклад, під час аналізу інформаційних операцій необхідно визначити першоджерело повідомлення, оцінити наявність бот-активності, встановити зв’язки між акаунтами та перевірити достовірність мультимедійного контенту. Такі завдання потребують використання різних інструментів та методів, що ускладнює вибір оптимального рішення [15].

Таким чином, проблема якості даних в OSINT є однією з ключових причин, чому потрібна автоматизована підтримка прийняття рішень, яка враховує критерії достовірності та надійності джерел [14].

1.3.3 Обмеження ручного аналізу та складність обробки великих обсягів даних

У процесі OSINT-аналітики часто виникає необхідність роботи з великими масивами даних, що можуть включати тисячі вебсторінок, публікацій у соціальних мережах, доменних записів, IP-адрес та витоків даних. Ручна обробка такої інформації є надзвичайно ресурсоємною та практично неефективною, оскільки потребує значних затрат часу та людських ресурсів [5].

Ручний підхід також підвищує ймовірність помилок. Аналітик може пропустити важливі ознаки загрози, неправильно інтерпретувати дані або не врахувати взаємозв’язки між об’єктами. Це особливо критично в умовах швидкого розвитку кібератак, коли час реагування є визначальним фактором ефективності захисту [14].

Окремою проблемою є складність кореляції даних. Наприклад, у випадку аналізу фішинг атаки необхідно одночасно перевірити домен, IP-адресу, SSL-сертифікат, пов’язані ресурси, згадки у відкритих джерелах, а також можливі зв’язки із відомими злочинними групами. Виконання таких завдань вручну ускладнює оперативне прийняття рішень [15].

У результаті виникає потреба у застосуванні автоматизованих засобів збору та обробки даних, а також у впровадженні систем підтримки прийняття рішень, які можуть зменшити навантаження на аналітика та підвищити

ефективність аналізу [15].

1.3.4 Необхідність формалізації критеріїв вибору та роль систем підтримки прийняття рішень

Вибір OSINT-інструмента має здійснюватися не інтуїтивно, а на основі формалізованих критеріїв, які дозволяють оцінити ефективність та придатність засобу для конкретної задачі. Основними критеріями можуть бути: тип джерел, які підтримує інструмент; рівень автоматизації; можливість інтеграції з іншими системами; точність результатів; зручність використання; ресурсоємність; можливість масштабування [5].

У практиці інформаційної безпеки важливим є врахування організаційних факторів. Наприклад, великі компанії з SOC-підрозділами можуть впроваджувати комплексні платформи OSINT-аналітики, тоді як малі організації частіше використовують окремі сервіси або безкоштовні інструменти. Відсутність єдиного підходу до оцінювання ускладнює вибір і часто призводить до неефективного використання ресурсів [14].

Автоматизована підтримка прийняття рішень у цьому контексті розглядається як перспективний напрям, що дозволяє систематизувати критерії вибору та зменшити суб’єктивність. СППР може враховувати характеристики задачі, доступні ресурси організації та вимоги до результатів, після чого пропонувати оптимальний набір інструментів [15].

Таким чином, необхідність формалізації критеріїв вибору та впровадження автоматизованих систем підтримки рішень є логічним етапом розвитку OSINT-підходів у кібербезпеці [15].

1.3.5 Порівняльний аналіз існуючих підходів до вибору OSINT-інструментів

Для обґрунтування необхідності автоматизованої підтримки прийняття рішень доцільно виконати порівняльний аналіз підходів, які застосовуються при виборі OSINT-інструментів. У реальних умовах організації можуть застосовувати різні моделі вибору: ручний експертний підхід, частково автоматизований підхід із використанням шаблонів, або комплексні системи, що

інтегруються з кіберрозвідкою та Threat Intelligence.

З метою порівняння підходів було сформовано систему критеріїв оцінювання, що відображає ключові вимоги до вибору OSINT-інструментів. Критерії оцінювалися за рівнем прояву: низький / середній / високий, що дозволяє підвищити зрозумілість та уникнути цифрових шкал, які можуть бути менш наочними.

Таблиця 1.3.1

Критерії оцінювання підходів до вибору OSINT-інструментів

Критерій	**Позначення**	**Опис**
Рівень автоматизації вибору	AB	Наскільки процес вибору може бути виконаний автоматично
Масштабованість	M	Здатність підходу працювати з великою кількістю інструментів та джерел
Об’єктивність результатів	OP	Зменшення суб’єктивності експертного впливу
Гнучкість до різних задач	ГЗ	Можливість адаптації під різні сценарії кібербезпеки
Ресурсні витрати	РВ	Обсяг часу, персоналу та технічних ресурсів для реалізації
Придатність до SOC/CSIRT	SC	Чи можна застосовувати підхід у структурі SOC/CSIRT
Інтеграція з Threat Intelligence	TI	Чи підтримує підхід кореляцію з TI-даними

Таблиця 1.3.2

Порівняння підходів до вибору OSINT-інструментів

Підхід	**AB**	**M**	**OP**	**ГЗ**	**РВ**	**SC**	**TI**
Ручний експертний вибір	низький	низька	низька	середня	високі	середня	низька
Вибір за шаблонами (чек-листи, матриці)	середній	середня	середня	середня	середні	середня	середня
Напівавтоматизований вибір (скрипти, фільтри, API)	середній	висока	середня	висока	середні	висока	середня
Автоматизована СППР	високий	висока	висока	висока	середні	висока	висока

Таблиця 1.3.3

Порівняльний аналіз проблем вибору OSINT-інструментів на практиці

Проблема	**Наслідок для кібербезпеки**	**Потреба в автоматизації**
Велика кількість інструментів	складність вибору, втрати часу	висока
Нестабільність доступу до джерел (API, політики платформ)	зниження ефективності моніторингу	висока
Неоднорідність форматів даних	потреба ручної обробки	висока
Складність кореляції даних	пропуск важливих зв’язків	висока
Суб’єктивність оцінювання	помилки у виборі інструментів	середня
Дефіцит кваліфікованих фахівців	неможливість ефективного використання OSINT	висока

Таблиця 1.3.4

Порівняння категорій OSINT-інструментів за критичними характеристиками

Категорія OSINT-інструментів	**Переваги**	**Недоліки**	**Основні задачі**
Пошукові системи та спеціалізовані пошуки	швидкість, доступність	поверхневий аналіз, багато шуму	пошук згадок, файлів, витоків
SOCMINT (соцмережі/месенджери)	актуальність інформації	багато фейків, складність перевірки	дезінформація, профілі, зв’язки
Веб-архіви та WHOIS	історичний аналіз	неповнота архівації	фіксація доказів, доменний аналіз
Метадані та медіааналіз	доказовість	метадані можуть бути стерті	цифрова криміналістика
Візуалізація та кореляція	наочність, зв’язки	потребує навичок	threat intelligence, розслідування

Проведений порівняльний аналіз показує, що вибір OSINT-інструментів є складним процесом, оскільки залежить від багатьох факторів: типу задачі, джерел інформації, рівня автоматизації та вимог до точності результатів. Через це універсального рішення не існує, а ефективність залежить від правильного поєднання інструментів та методів роботи з даними.

Ручний вибір інструментів, який часто застосовується на практиці, є найбільш доступним, однак він має суттєві недоліки. Основною проблемою є залежність від досвіду аналітика та високі витрати часу. Крім того, у таких умовах зростає ризик помилок, пропуску важливих джерел або використання неактуальних інструментів.

Більш структуровані підходи, наприклад використання чек-листів або матриць критеріїв, дозволяють частково впорядкувати процес вибору, однак вони не завжди враховують швидку зміну цифрового середовища. OSINT-інструменти можуть втрачати актуальність через блокування платформ, зміну API або появу нових обмежень доступу. У результаті такі методи потребують постійного оновлення.

Найбільш ефективним підходом за результатами аналізу є автоматизована підтримка прийняття рішень, оскільки вона дозволяє зменшити суб’єктивність, підвищити швидкість вибору інструментів та враховувати декілька критеріїв одночасно. Це особливо важливо у випадках, коли OSINT використовується для реагування на інциденти або моніторингу загроз у режимі реального часу.

Таким чином, результати порівняння підтверджують, що впровадження автоматизованої системи підтримки вибору OSINT-інструментів є доцільним, оскільки вона забезпечує більш обґрунтований вибір інструментів, підвищує ефективність аналізу та дозволяє організації швидше адаптуватися до сучасних кіберзагроз.

Висновки до розділу 1

У першому розділі кваліфікаційної роботи було проведено аналіз можливостей застосування OSINT-інструментів у сфері інформаційної безпеки

та визначено їх роль у сучасних процесах виявлення й протидії загрозам. Розглянуто, що OSINT є ефективним інструментарієм для отримання актуальної інформації з відкритих джерел, який може використовуватися як у державному секторі, так і в корпоративному середовищі для підвищення рівня кіберзахисту.

Було визначено основні напрями застосування OSINT у забезпеченні інформаційної безпеки. Зокрема, встановлено, що OSINT може бути використаний для моніторингу витоків інформації, протидії соціальній інженерії та фішингу, виявлення шкідливих ресурсів, кіберрозвідки щодо атакуючих груп, оцінки Attack Surface організацій, протидії дезінформаційним кампаніям та підтримки цифрових розслідувань. Доведено, що ефективність OSINT визначається не лише доступом до даних, а й правильністю методики збору, аналізу та верифікації інформації.

Також було виконано класифікацію OSINT-інструментів та проведено аналіз їх функціональних можливостей. Було визначено основні категорії інструментів, серед яких пошукові системи, сервіси аналізу мережевої інфраструктури, інструменти SOCMINT, веб-архіви, WHOIS-засоби, інструменти аналізу метаданих та засоби візуалізації й кореляції даних. Показано, що кожна категорія має власну спеціалізацію, переваги та обмеження, тому у практичній діяльності зазвичай застосовується комбінований підхід, що дозволяє підвищити точність та повноту результатів аналізу.

У висновку було проаналізовано основні проблеми вибору OSINT-інструментів та обґрунтовано необхідність автоматизованої підтримки прийняття рішень. Встановлено, що ключовими труднощами є велика кількість інструментів, нестабільність доступу до джерел, складність перевірки достовірності даних, відсутність універсального рішення та залежність результатів від досвіду аналітика. Проведений порівняльний аналіз показав, що найбільш перспективним підходом є впровадження автоматизованих систем підтримки вибору OSINT-інструментів, які дозволяють зменшити суб’єктивність, підвищити оперативність обробки інформації та покращити ефективність використання ресурсів.

Отже, результати першого розділу підтверджують актуальність теми дослідження та формують теоретичну основу для подальшої розробки системи підтримки вибору OSINT-інструментів для вирішення завдань інформаційної безпеки. Отримані висновки будуть використані в наступних розділах роботи для визначення вимог до системи, побудови її структури та розробки механізму автоматизованого прийняття рішень.

РОЗДІЛ 2 РОЗРОБКА СИСТЕМИ ПІДТРИМКИ ВИБОРУ OSINT-ІНСТРУМЕНТІВ

У другому розділі здійснюється розробка системи підтримки вибору OSINT-інструментів для задач інформаційної безпеки. Визначаються основні вимоги до системи, критерії оцінювання інструментів та принципи формування бази знань.

Особлива увага приділяється побудові системі прийняття рішень, яка дозволяє здійснювати автоматизований вибір найбільш релевантних OSINT-інструментів залежно від поставленої задачі та заданих параметрів оцінювання.

2.1 Формування вимог до системи підтримки вибору OSINT-інструментів

Ефективне використання OSINT у сфері інформаційної безпеки потребує не лише наявності окремих інструментів збору та аналізу відкритих даних, а й системного підходу до їх вибору. Як показано у попередньому розділі, ринок OSINT-рішень характеризується значною кількістю сервісів, що мають різні функціональні можливості, обмеження доступу, різну точність результатів і рівень автоматизації. Через це процес вибору інструментів часто стає суб’єктивним і залежить від досвіду аналітика.

Для зменшення впливу людського фактору та підвищення ефективності роботи аналітика доцільним є створення СППР, яка забезпечуватиме автоматизований вибір OSINT-інструментів залежно від завдання інформаційної безпеки. Формування вимог до такої системи є ключовим етапом проєктування, оскільки саме вимоги визначають функціональність, структуру, модулі та майбутню реалізацію системи.

2.1.1 Призначення та мета системи підтримки вибору OSINT-інструментів

Основною метою розроблюваної СППР є автоматизована підтримка вибору найбільш доцільних OSINT-інструментів для виконання конкретних

завдань інформаційної безпеки. Система повинна допомагати аналітику формувати перелік рекомендованих інструментів, враховуючи їх функціональні характеристики та задані критерії оцінювання.

Система має забезпечувати підтримку основних напрямів використання OSINT, які були розглянуті у розділі 1, зокрема:

- моніторинг витоків інформації;
- аналіз фішингових ресурсів;
- оцінку Attack Surface організації;
- SOCMINT;
- GEOINT-аналіз;
- аналіз метаданих і мультимедійних файлів;
- підтримку threat intelligence та цифрових розслідувань.

Таким чином, СППР повинна виступати як інструмент оптимізації процесу вибору OSINT-рішень та зменшення витрат часу на підбір відповідного інструментарію

2.1.2 Вхідні дані та критерії оцінювання інструментів (розширено)

Функціонування системи підтримки вибору OSINT-інструментів ґрунтується на використанні структурованих вхідних даних, які задаються користувачем перед запуском алгоритму оцінювання. На відміну від ручного вибору інструментів, де рішення залежить від суб’єктивного досвіду аналітика, СППР формує рекомендації на основі формалізованих критеріїв і вагових коефіцієнтів, що дозволяє підвищити об’єктивність результатів.

Важливим елементом є *вагові коефіцієнти критеріїв*, які визначають важливість кожного критерію для користувача.

Наприклад, у ситуації реагування на інцидент важливими можуть бути швидкість та автоматизація. Натомість у випадку академічного розслідування або журналістського OSINT аналізу більшу роль можуть відігравати точність і можливість експорту даних.

Таблиця 2.1.1

Шкала оцінювання критеріїв

Оцінка	**Пояснення оцінки**
1	дуже низький рівень / практично відсутня характеристика
2	низький рівень
3	середній рівень
4	високий рівень
5	дуже високий рівень / максимально виражена характеристика

Для ранжування OSINT-інструментів необхідно визначити єдиний числовий показник, який буде відображати відповідність інструмента вимогам користувача. Таким показником є інтегральна оцінка Score.

Модель розрахунку Score базується на методі зваженої суми. Для кожного інструмента беруться оцінки критеріїв (1–5) та множаться на вагові коефіцієнти. Після цього всі отримані значення підсумовуються.

Формально Score можна представити таким чином:

$$Score = \sum_{i=1}^{n} (C_i \cdot W_i)$$

де:

- C_i– оцінка інструмента за критерієм i,
- W_i– ваговий коефіцієнт критерію i,
- n– кількість критеріїв.

Таким чином, чим більші оцінки інструмента та чим більші ваги критеріїв, тим вищим буде результат.

Також, для коректної роботи СППР необхідно сформувати критерії, які описують функціональні характеристики інструментів. У даній роботі пропонується застосовувати набір критеріїв, що охоплює технічні та організаційні аспекти використання OSINT-засобів.

1) Рівень автоматизації

Критерій відображає, наскільки інструмент здатний виконувати операції збору та аналізу даних автоматично. Це є важливим фактором у SOC/CSIRT

середовищі, де аналітик працює з великою кількістю інцидентів.

Високий рівень автоматизації дозволяє:

- зменшити навантаження на аналітика;
- прискорити розслідування;
- обробляти великі масиви даних.

Низька автоматизація означає, що більшість дій виконується вручну

2) Наявність API

API є важливим елементом для інтеграції OSINT-інструмента з іншими системами, наприклад:

- SOC-платформами;
- SIEM;
- Threat Intelligence платформами;
- скриптами автоматичного збору.

Якщо інструмент має API, він може використовуватися не лише вручну, а й як частина автоматизованого ланцюга обробки даних.

3) Зручність використання

Даний критерій описує, наскільки легко аналітику працювати з інструментом.

На оцінку зручності впливають:

- інтерфейс (GUI або CLI);
- наявність документації;
- доступність навчальних матеріалів;
- простота виконання типових задач.

Наприклад, веб-сервіси зазвичай мають високий рівень зручності, тоді як CLI-інструменти потребують технічної підготовки.

4) Точність та надійність результатів

Цей критерій є одним з ключових, оскільки OSINT-аналітика потребує максимальної достовірності.

Точність залежить від:

- якості джерел даних;

- частоти оновлення баз;
- рівня фільтрації помилкових результатів;
- наявності механізмів верифікації.

У сфері кібербезпеки помилкові результати можуть призвести до хибних управлінських рішень.

5) Швидкість отримання результатів

Критерій відображає, як швидко інструмент надає інформацію після запуску запиту.

Швидкість є критичною в умовах:

- реагування на фішинг;
- блокування шкідливих доменів;
- моніторингу витоків;
- оперативного аналізу інцидентів.

6) Доступність / вартість

Багато OSINT-сервісів мають обмеження безкоштовних функцій. У корпоративному середовищі це може бути важливим фактором вибору.

Критерій враховує:

- наявність free-версії;
- доступність без реєстрації;
- ціну підписки;
- обмеження по кількості запитів.

7) Можливість експорту даних

У професійному OSINT-аналізі важливо не лише знайти інформацію, а й зафіксувати її для подальшого використання у звітах, доказовій базі або презентаціях.

Експорт може включати:

- JSON, CSV, PDF-звіти;
- графові структури;
- API-вивантаження.

8) Інтеграція з іншими системами

Критерій описує здатність інструмента працювати у зв’язці з іншими продуктами або платформами.

Це може включати:

- сумісність із SIEM;
- інтеграцію з Threat Intelligence;
- можливість використання в SOC-процесах;
- підтримку зовнішніх модулів.

2.1.3 Функціональні вимоги до системи

Функціональні вимоги визначають перелік задач, які повинна виконувати система підтримки вибору OSINT-інструментів, а також описують логіку її роботи та очікувані результати. Оскільки OSINT-аналіз передбачає використання різних категорій інструментів залежно від мети дослідження, СППР повинна забезпечувати можливість гнучкого вибору та обґрунтованого ранжування інструментів на основі формалізованих критеріїв.

Запропонована система повинна реалізовувати повний цикл підтримки прийняття рішення: від введення початкових параметрів користувачем до отримання впорядкованого списку рекомендованих OSINT-інструментів. Схема функціональних вимог зображена на Рис. 2.1.1

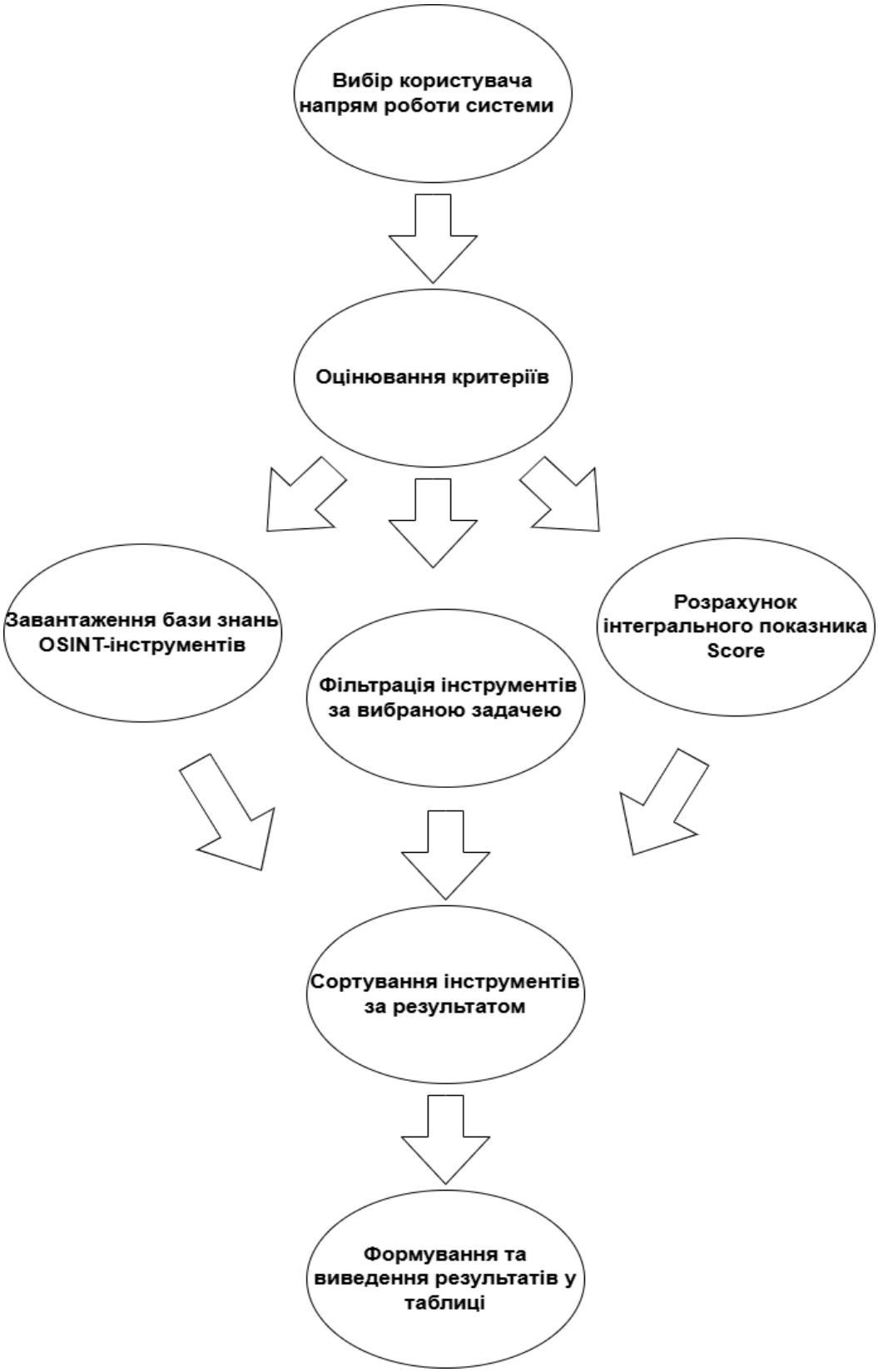


Рис.2.1.1. Схема функціональних вимог

2.1.4 Вимоги до структури бази знань OSINT-інструментів

Ключовим елементом системи підтримки вибору OSINT-інструментів є база знань, оскільки саме вона забезпечує інформаційне наповнення системи та

є основою для формування рекомендацій. Від правильності структурування бази знань залежить точність оцінювання інструментів, можливість їх порівняння, а також коректність роботи алгоритму підтримки прийняття рішень.

У межах даної роботи база знань розглядається як сукупність впорядкованих даних про OSINT-інструменти, які можуть бути використані для вирішення завдань інформаційної безпеки. Вона повинна містити не лише загальний опис інструментів, але й формалізовані характеристики, які дозволяють оцінювати їх ефективність за визначеними критеріями.

База знань повинна включати основні інформаційні параметри, необхідні для коректного функціонування системи, зокрема:

- назву OSINT-інструмента;
- категорію інструмента;
- короткий опис функціонального призначення;
- перелік задач інформаційної безпеки, які підтримує інструмент;
- оцінки за визначеними критеріями (автоматизація, наявність API, точність, швидкість тощо).

Перш за все, база знань повинна містити базову ідентифікаційну інформацію про кожен інструмент. До неї належать назва та категорія. Назва дозволяє однозначно визначити інструмент у системі, а категорія дає можливість класифікувати інструменти за напрямами застосування. Наприклад, інструменти можуть належати до категорій «Моніторинг витоків» або «Аналіз загроз». Такий підхід спрощує роботу користувача, оскільки дозволяє швидко зорієнтуватися у сфері призначення інструмента.

Обов’язковим елементом є короткий опис інструмента. Він необхідний для пояснення його функціонального призначення, основних можливостей та практичного застосування. Опис повинен бути стислим, але інформативним, щоб користувач міг зрозуміти, чому система рекомендує саме цей інструмент і які результати можна очікувати від його використання.

Особливу роль відіграє перелік завдань інформаційної безпеки, які підтримує інструмент. Цей параметр визначає сферу застосування інструмента

та дозволяє системі виконувати первинну фільтрацію. Наприклад, якщо користувач обирає завдання «моніторинг витоків», система повинна враховувати лише ті інструменти, які здатні працювати з витоками даних. Таким чином, завдання виступають як основний механізм логічного зв’язку між потребою користувача та рекомендованими інструментами.

Наступним важливим компонентом бази знань є система оцінювання інструментів за критеріями. Для кожного OSINT-засобу необхідно зберігати значення оцінок за критеріями, які використовуються у процесі формування рейтингу. Ці оцінки мають бути представлені у вигляді числових значень, що дозволяє здійснювати математичні обчислення інтегрального показника ефективності. Наявність стандартизованої шкали (наприклад 1–5) забезпечує можливість порівняння інструментів між собою та побудови ранжованого списку рекомендацій.

Також потрібно, щоб база знань була структурована за єдиним шаблоном. Якщо інформація про різні інструменти подається у різних форматах або з пропущеними параметрами, це призведе до зниження точності рекомендацій. Тому необхідно забезпечити однаковий набір полів для кожного інструмента.

Окрім цього, база знань повинна бути масштабованою. Оскільки у сфері OSINT постійно з’являються нові інструменти, а існуючі можуть змінювати свої можливості або політику доступу, база повинна підтримувати можливість регулярного оновлення. Це означає, що вона має бути зручною для доповнення новими записами та редагування вже наявних.

Таким чином, база знань OSINT-інструментів повинна бути структурованою, повною та придатною для подальшої формалізованої обробки. Її правильне формування забезпечує ефективну роботу системи підтримки прийняття рішень і підвищує точність рекомендацій при виборі інструментів для виконання завдань інформаційної безпеки.

2.2 Побудова системи прийняття рішень щодо вибору OSINT-інструментів залежно від завдань інформаційної безпеки

Система підтримки прийняття рішень у виборі OSINT-інструментів створюється з метою забезпечення обґрунтованого, повторюваного та формалізованого механізму підбору засобів розвідки залежно від конкретних задач інформаційної безпеки. Вона поєднує в собі логічну фільтрацію, багатокритеріальне оцінювання та класифікацію інструментів із подальшим ранжуванням у вигляді рейтингу рекомендацій.

Система ґрунтується на базі знань OSINT-інструментів (структурованій таблиці зі значеннями показників), логіці відбору інструментів за підтримуваними задачами, та механізмі розрахунку узагальненої оцінки (інтегрального показника), що дозволяє створювати релевантні рекомендації для користувача.

Завдання системи полягають у наступному:

1. Встановити відповідність між поставленою користувачем задачею безпеки і можливостями OSINT-інструментів.

2. Забезпечити адаптацію під різні пріоритети та вимоги користувача через вагові коефіцієнти критеріїв.

3. Створити рейтинг інструментів за інтегральною оцінкою, що відображає їхню придатність і ефективність для конкретної задачі.

2.2.1 Формалізація логіки системи вибору

Після вибору користувачем завдання інформаційної безпеки система відбирає з бази знань лише ті інструменти, які підтримують обрану задачу. Це відбувається на основі сукупності задач, зазначених у описі кожного інструмента.

Логічний механізм системи можна описати умовою:

- Нехай Z - множина можливих задач інформаційної безпеки (наприклад, оцінка Attack Surface, моніторинг витоків, SOCMINT тощо).
- Для кожного інструмента t у базі знань визначений список задач, які він підтримує.

- Обраний користувачем елемент $z \in Z$ фільтрує інструменти: система розглядає лише ті t, для яких $z \in tasks(t)$.

Цей механізм забезпечує базову відсіювання несумісних з поточною задачею засобів і створює первинний набір кандидатовий інструментів для подальшого оцінювання.

2.2.2 Категоризація OSINT-інструментів у системі

Для того, щоб система була зрозумілою та структурованою, інструменти OSINT класифікуються за функціональними групами. Така категоризація дозволяє не лише правильно відбирати інструменти за підтримкою задач, а й представляти їх у звіті у вигляді змістовних груп, що відповідають практичним напрямам роботи аналітика.

Нижче наведено детальні таблиці 2.2.1-2.2.9 категорій інструментів з описом:

Таблиця 2.2.1

Інструменти для оцінки Attack Surface

Інструмент	**Короткий опис**
Shodan	Пошукова система для пристроїв та сервісів, підключених до Інтернету. Дозволяє знаходити сервери, відкриті порти, IoT-пристрої та іншу інфраструктуру, що відповідає за зовнішні атаки [16].
Censys	Платформа для аналізу великої кількості відкритих сервісів та пристроїв у глобальній мережі; дозволяє оцінювати стан TLS/HTTPS, відкриті порти та інші зовнішні ознаки експозиції [17].
BuiltWith	Сервіс для визначення технологій, що використовуються на сайті, що важливо для оцінки тієї частини Attack Surface, яка пов’язана зі стеком технологій веб-ресурсу [18].

Таблиця 2.2.2

Інструменти для аналізу загроз

Інструмент	**Короткий опис**
VirusTotal	Онлайн-сервіс, що аналізує URL, файли, IP та домени за допомогою численних антивірусних движків і баз даних загроз; дозволяє отримувати репутаційні дані та індикатори загроз [19].

Таблиця 2.2.3

Моніторинг витоків і компрометацій

Інструмент	**Короткий опис**
Have I Been Pwned	Сервіс-трекер, що показує, чи були електронні адреси, домени або облікові записи включені у відомі витоки даних; дозволяє оцінити ризик компрометації облікових записів [20].
IntelX (Intelligence X)	Пошуковий сервіс для даних витоків, включно з публікаціями в даркнеті, документами й наборами даних; використовується для виявлення компрометованої інформації [21].

Таблиця 2.2.4

Автоматизація OSINT

Інструмент	**Короткий опис**
SpiderFoot	Автоматизований інструмент OSINT для збору та кореляції даних з понад 200 джерел щодо IP-адрес, доменів, email та інших атрибутів; має веб-інтерфейс та підтримує інтеграцію з багатьма платформами OSINT [22].
Recon-ng	Модульний фреймворк OSINT для автоматичного збору даних через API та модулі (командний рядок); використовується для розвідки доменів, піддоменів, контактів [23].

Таблиця 2.2.5

Візуалізація та кореляція зв’язків

Інструмент	**Короткий опис**
Maltego	Платформа для візуального аналізу і побудови графів зв’язків між різними об’єктами на основі OSINT-даних; дозволяє автоматизувати об’єднання даних з різних джерел в єдині графічні моделі [24].

Таблиця 2.2.6

Інструменти для аналізу доменів та DNS

Інструмент	**Короткий опис**
WHOIS Lookup	Інструмент для отримання реєстраційної інформації про домен: дату реєстрації, сервери DNS тощо; використовується для перевірки походження доменів [25].
SecurityTrails	Сервіс для історичного аналізу DNS, піддоменів та інших записів домену, що застосовується для оцінки змін у інфраструктурі [26].

Таблиця 2.2.7

Інструменти аналізу метаданих та медіа

Інструмент	**Короткий опис**
ExifTool	Потужний інструмент для перегляду та аналізу метаданих фото, відео та документів (EXIF, GPS-координати, часові відмітки тощо); застосовується для перевірки автентичності та походження медіафайлів [13].
FotoForensics	Онлайн-сервіс для аналізу зображень та виявлення ознак редагування / маніпуляцій у фото (наприклад, через ELA-аналіз) [27].

Таблиця 2.2.8

Інструменти SOCMINT (соціальна розвідка)

Інструмент	**Короткий опис**
Google Dorks	Метод використання розширених пошукових операторів Google для знаходження прихованих даних, файлів, сторінок та директорій, які можуть містити чутливу інформацію [28].
Telegram OSINT Bots	Спеціальні боти для Telegram, що дозволяють шукати канали, користувачів та пов’язану публічну інформацію [29].
TweetDeck / X Search	Інструмент для моніторингу публікацій, хештегів, активності користувачів у Twitter відповідно до заданих параметрів [30].

Таблиця 2.2.9

GEOINT та місцеположення

Інструмент	**Короткий опис**
Google Maps	Карти та супутникові знімки для перевірки географічного контексту об’єктів, аналіз маршруту та оцінки локації [31].
Google Earth	Інструмент для перегляду історичних супутникових знімків, аналізу територій та геопросторової інформації [31].
Sentinel Hub	Платформа для аналізу супутникових даних із відкритих місій Sentinel; корисна для геопросторового аналізу в інцидентних розслідуваннях [32].

2.3 Проєктування архітектури системи підтримки вибору OSINT-інструментів

Після запуску системи підтримки вибору OSINT-інструментів користувач отримує доступ до головної сторінки з інтерфейсом для введення початкових

параметрів. На цьому етапі користувач обирає тип завдання інформаційної безпеки, яке необхідно вирішити. Таким чином система визначає напрям аналізу та формує основу для подальшого відбору інструментів.

Наступним кроком користувач задає важливість критеріїв оцінювання, встановлюючи вагові коефіцієнти для характеристик інструментів. Введені значення використовуються системою як основа для формування персоналізованої системи оцінювання.

Після введення вхідних даних система звертається до бази знань OSINT-інструментів, у якій кожен інструмент описаний за категорією, переліком задач застосування та оцінками за критеріями. На основі обраного завдання здійснюється фільтрація інструментів: у подальших розрахунках беруть участь лише ті засоби, які підтримують вибрану користувачем задачу.

Далі система виконує обчислення інтегрального показника ефективності (Score) для кожного інструмента. Розрахунок здійснюється шляхом множення значень критеріїв на відповідні вагові коефіцієнти та подальшого підсумовування отриманих результатів.

Після завершення обчислень система формує рейтинг інструментів, сортує їх за спаданням показника Score та виводить результат у вигляді списку рекомендацій. Покрокова робота системи зазначена на Рис. 2.3.1.

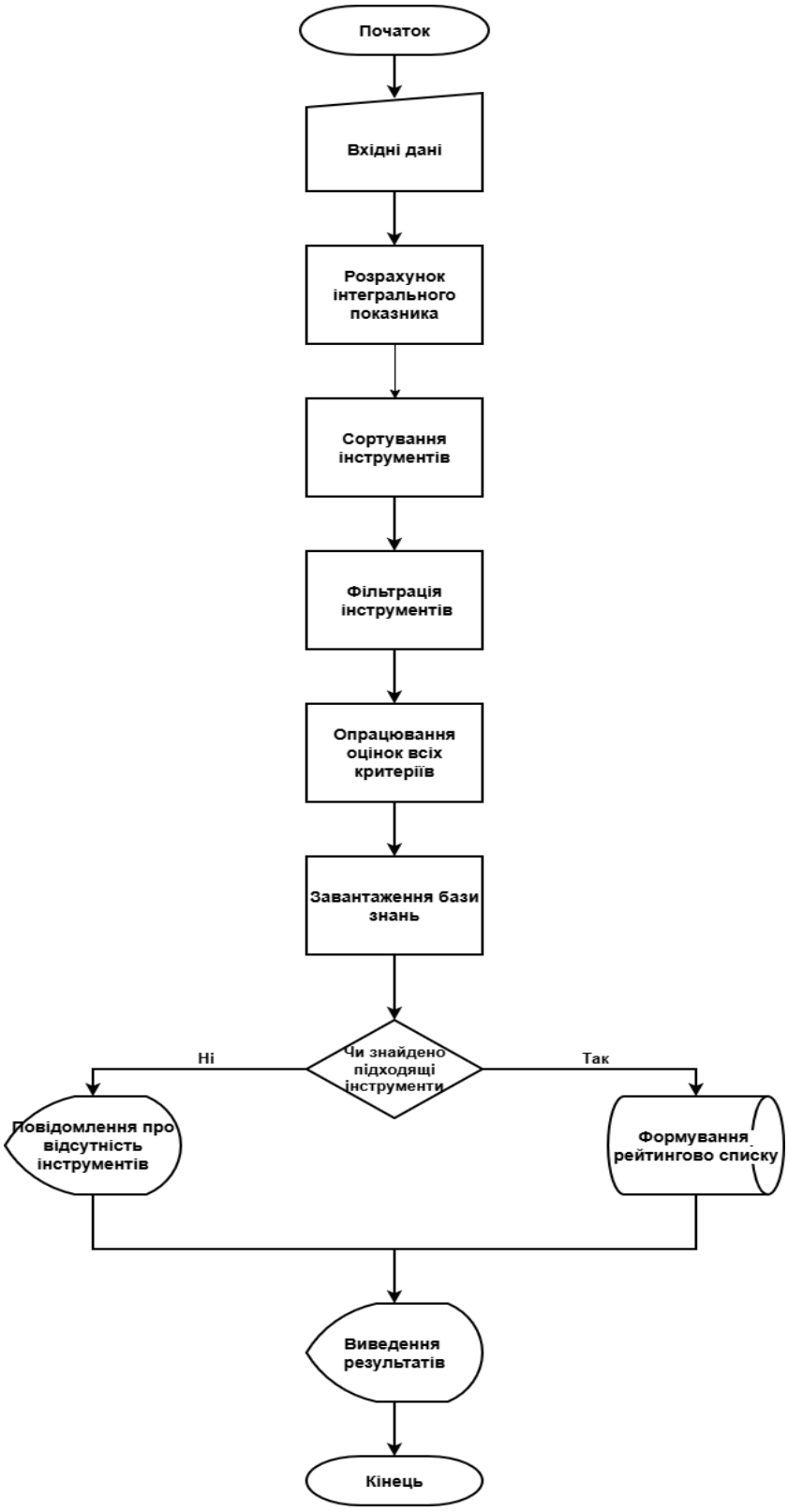


Рис. 2.3.1. Блок-схема роботи системи

Висновки до розділу 2

У другому розділі було розглянуто процес розробки системи підтримки вибору OSINT-інструментів та визначено основні підходи до її побудови.

Проведене дослідження дозволило встановити, що вибір OSINT-засобів у сфері інформаційної безпеки є складною задачею, оскільки сучасний ринок характеризується великою кількістю інструментів, які відрізняються функціональними можливостями, умовами доступу, рівнем автоматизації та ефективністю використання.

У межах виконання завдань розділу було сформовано вимоги до системи підтримки вибору OSINT-інструментів. Визначено, що система повинна забезпечувати можливість введення параметрів користувачем, підтримувати формалізовані критерії оцінювання та формувати результати у вигляді рейтингового списку рекомендованих інструментів. Також обґрунтовано необхідність застосування системи критеріїв, що дозволяє виконувати об’єктивне порівняння інструментів та зменшувати вплив суб’єктивних факторів при прийнятті рішення.

У процесі дослідження було визначено основні критерії оцінювання OSINT-інструментів, які є найбільш значущими для практичного застосування в інформаційній безпеці. До них належать рівень автоматизації, наявність API, зручність використання, точність та надійність результатів, швидкість роботи, доступність або вартість, можливість експорту даних та інтеграція з іншими системами. Запропоновано використовувати шкалу оцінювання для подальшого розрахунку узагальненого показника ефективності, що дозволяє виконувати ранжування інструментів за заданими умовами.

Окрему увагу приділено формуванню вимог до структури бази знань OSINT-інструментів. Встановлено, що база знань повинна містити назву інструмента, його категорію, опис призначення, перелік підтримуваних завдань та оцінки за критеріями. Такий підхід забезпечує можливість оновлення системи та розширення її функціональності без необхідності суттєвих змін у логіці роботи.

На основі визначених вимог було розроблено систему прийняття рішень, яка забезпечує послідовний процес вибору інструментів: від введення користувачем задачі та критеріїв до фільтрації інструментів за відповідністю,

оцінювання та формування рейтингу. Така система дозволяє підвищити ефективність процесу вибору та скоротити час, необхідний для аналізу великої кількості доступних OSINT-засобів.

У результаті виконання розділу було спроєктовано загальну архітектуру системи підтримки вибору OSINT-інструментів. Запропонована архітектура включає основні модулі введення даних, обробки бази знань, оцінювання інструментів та формування рекомендацій. Встановлено, що така структура є логічною та придатною для подальшої практичної реалізації у вигляді веб-застосунку.

РОЗДІЛ 3 РЕАЛІЗАЦІЯ СИСТЕМИ ПІДТРИМКИ ВИБОРУ OSINT-ІНСТРУМЕНТІВ

У третьому розділі розглядається практична реалізація системи підтримки вибору OSINT-інструментів. Описуються використані програмні засоби та технології розробки, структура бази знань і механізм оцінювання інструментів.

Також проводиться тестування створеної системи на практичних кейсах інформаційної безпеки та аналіз отриманих результатів роботи веб-додатка.

3.1 Використані програмні засоби та технології для реалізації системи підтримки вибору OSINT-інструментів

У межах даної кваліфікаційної роботи було реалізовано веб-орієнтовану систему підтримки вибору OSINT-інструментів, яка дозволяє користувачу підібрати найбільш доцільні засоби залежно від завдання інформаційної безпеки та заданих критеріїв оцінювання. Для створення програмного продукту було обрано набір сучасних технологій, які забезпечують зручність розробки, простоту використання та можливість подальшого розширення системи.

Основною мовою програмування для створення системи підтримки вибору OSINT-інструментів було обрано *Python*. Дана мова програмування є однією з найпоширеніших у сфері веб-розробки, аналізу даних, автоматизації процесів та кібербезпеки. Python характеризується зрозумілим синтаксисом, високою читабельністю коду та великою кількістю готових бібліотек, що значно спрощує процес створення програмних систем. Завдяки підтримці різних моделей програмування Python дозволяє реалізовувати як прості програмні модулі, так і повноцінні інформаційні системи. Використання даної мови у межах роботи дозволило швидко реалізувати систему підтримки та забезпечити обробку даних користувача [33].

Однією з причин вибору Python є його широке застосування у сфері інформаційної безпеки та OSINT-досліджень. Значна кількість сучасних інструментів для автоматизації збору інформації, аналізу даних та побудови

систем підтримки прийняття рішень реалізовані саме з використанням Python. Це робить мову доцільною для створення систем, орієнтованих на аналіз та оцінювання OSINT-інструментів.

Для реалізації програмного модуля веб-додатку використано фреймворк *Flask*. Даний фреймворк забезпечує створення веб-застосунків із мінімальною кількістю службового коду та дозволяє реалізовувати необхідну функціональність поступово, залежно від потреб проєкту. Flask використовується для організації взаємодії між користувацьким інтерфейсом та програмною логікою системи. У межах реалізованої системи фреймворк забезпечує прийом HTTP-запитів від користувача, обробку введених параметрів, виконання розрахунку інтегрального показника та передачу результатів на веб-сторінку [34].

Система реалізує основну логіку підтримки прийняття рішень. Після отримання параметрів від користувача система виконує аналіз бази знань OSINT-інструментів, здійснює фільтрацію інструментів відповідно до обраної задачі інформаційної безпеки та проводить розрахунок рейтингу для кожного інструмента. Після завершення обчислень результати передаються користувачу у вигляді впорядкованого списку рекомендацій.

Для створення користувацького інтерфейсу було використано *HTML*, *CSS* та *JavaScript*.

HTML застосовується для формування структури веб-сторінки та створення елементів взаємодії з користувачем. За допомогою HTML реалізовано форму вибору задач інформаційної безпеки, блок налаштування критеріїв оцінювання та область відображення результатів [35].

CSS використовується для оформлення зовнішнього вигляду системи. За допомогою таблиць стилів реалізовано кольорове оформлення елементів інтерфейсу, форматування таблиць результатів, розташування блоків та адаптацію інтерфейсу для зручного сприйняття інформації користувачем. Використання CSS дозволило зробити інтерфейс більш структурованим та зрозумілим [35].

JavaScript застосовується для забезпечення інтерактивності веб-додатку. З його допомогою реалізовано обробку подій, зчитування введених параметрів, відправлення запитів до програмного модуля системи та автоматичне оновлення результатів без перезавантаження сторінки. Це дозволило забезпечити більш швидку та зручну взаємодію користувача із системою [35].

Для передачі даних між користувацьким інтерфейсом та програмним модулем системи використовується технологія *AJAX* та формат *JSON*. AJAX дозволяє виконувати обмін даними у фоновому режимі без повного оновлення веб-сторінки, що позитивно впливає на швидкодію системи та зручність роботи користувача. Формат JSON використовується як універсальний спосіб представлення структурованих даних. Його використання є доцільним через простоту структури, компактність та підтримку як у Python, так і у JavaScript [36].

База знань системи реалізована у вигляді окремого *JSON-файлу tools.json*. У даному файлі зберігається інформація про OSINT-інструменти, включаючи назву, категорію, короткий опис, перелік підтримуваних задач та оцінки за критеріями. Такий спосіб організації даних дозволяє забезпечити гнучкість системи та спрощує процес її оновлення. У разі необхідності користувач або адміністратор системи може додати новий інструмент або змінити існуючі характеристики без зміни програмного коду.

Розробка програмного модуля виконувалася у середовищі *Visual Studio Code*. Дане середовище розробки забезпечує підтримку роботи з Python та веб-технологіями, має інтегрований термінал, засоби підсвічування синтаксису та інструменти для налагодження програмного коду. Використання Visual Studio Code дозволило ефективно організувати структуру проєкту, здійснювати тестування роботи веб-додатку та контролювати процес реалізації системи [37].

У процесі розробки було створено окремі програмні модулі для програмної логіки, користувацького інтерфейсу та зберігання бази знань. Такий підхід дозволив забезпечити модульність системи та спростити подальше вдосконалення функціоналу веб-додатку.

3.2 Побудова бази знань OSINT-інструментів і реалізація системи оцінювання критеріїв

У процесі реалізації системи підтримки вибору OSINT-інструментів одним із основних етапів стало формування бази знань, яка використовується для зберігання інформації про інструменти відкритої розвідки та подальшого формування рекомендацій користувачу. База знань є основою функціонування всієї системи, оскільки саме вона містить структуровані дані про характеристики інструментів та їх відповідність задачам інформаційної безпеки.

Для реалізації бази знань було сформовано окремий файл, у якому зберігається перелік OSINT-інструментів та їх параметри. Кожен інструмент описується набором полів: назвою, категорією, коротким описом, переліком підтримуваних задач та оцінками за критеріями. Такий підхід дозволяє систематизувати інформацію та забезпечити можливість автоматизованого аналізу.

На рисунку 3.2.1 наведено структуру бази знань OSINT-інструментів у середовищі розробки.

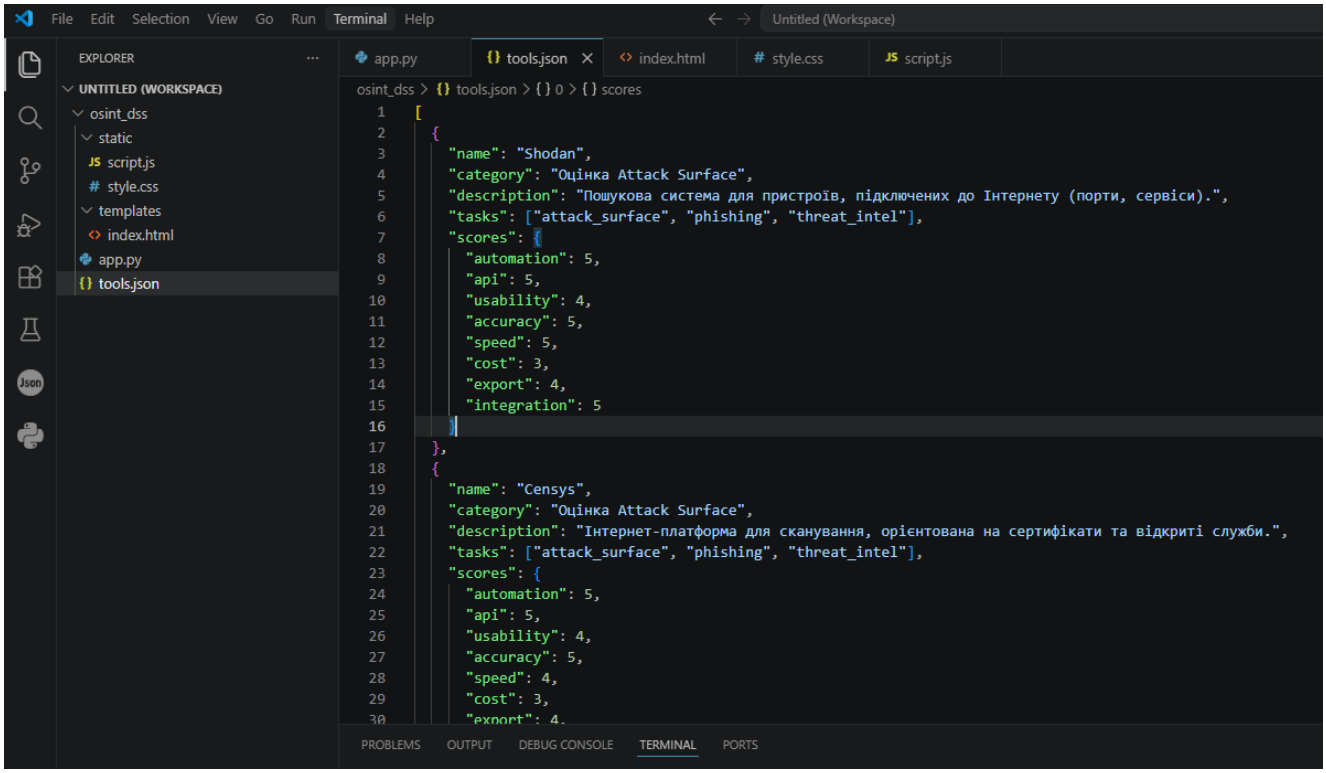


Рис. 3.2.1. Структура бази знань OSINT-інструментів

Під час формування бази знань до системи були включені інструменти різних категорій: аналіз Attack Surface, моніторинг витоків даних, GEOINT, SOCMINT, аналіз метаданих, автоматизація OSINT та веб-архіви. Це дозволило охопити основні напрями використання OSINT у сфері інформаційної безпеки. Для кожного інструмента було визначено перелік задач, які він підтримує.

У системі також реалізовано механізм оцінювання інструментів за набором критеріїв. Для цього кожному критерію присвоюється оцінка за шкалою від 1 до 5, де більше значення відповідає кращому рівню реалізації певної характеристики. Основні критерії для оцінювання описувалися в попередньому розділі.

Оцінки критеріїв використовуються для подальшого розрахунку інтегрального показника ефективності інструмента. Завдяки цьому система може автоматично формувати рейтинг інструментів відповідно до потреб користувача.

На рисунку 3.2.2 наведено приклад структури оцінювання інструмента за критеріями.

Рис. 3.2.2. Приклад оцінювання OSINT-інструмента за критеріями

Після формування бази знань було реалізовано механізм обробки даних, який дозволяє системі здійснювати фільтрацію інструментів за задачами інформаційної безпеки та виконувати розрахунок інтегрального показника.

Система аналізує введені користувачем вагові коефіцієнти критеріїв і на їх основі формує підсумковий рейтинг інструментів.

Обчислення Score виконується шляхом множення оцінки кожного критерію на його ваговий коефіцієнт та подальшого підсумовування отриманих значень. Такий підхід забезпечує гнучкість системи та дозволяє адаптувати результати до різних сценаріїв використання.

На рисунку 3.2.3 наведено фрагмент програмного модуля, який реалізує механізм розрахунку інтегральної оцінки інструментів.

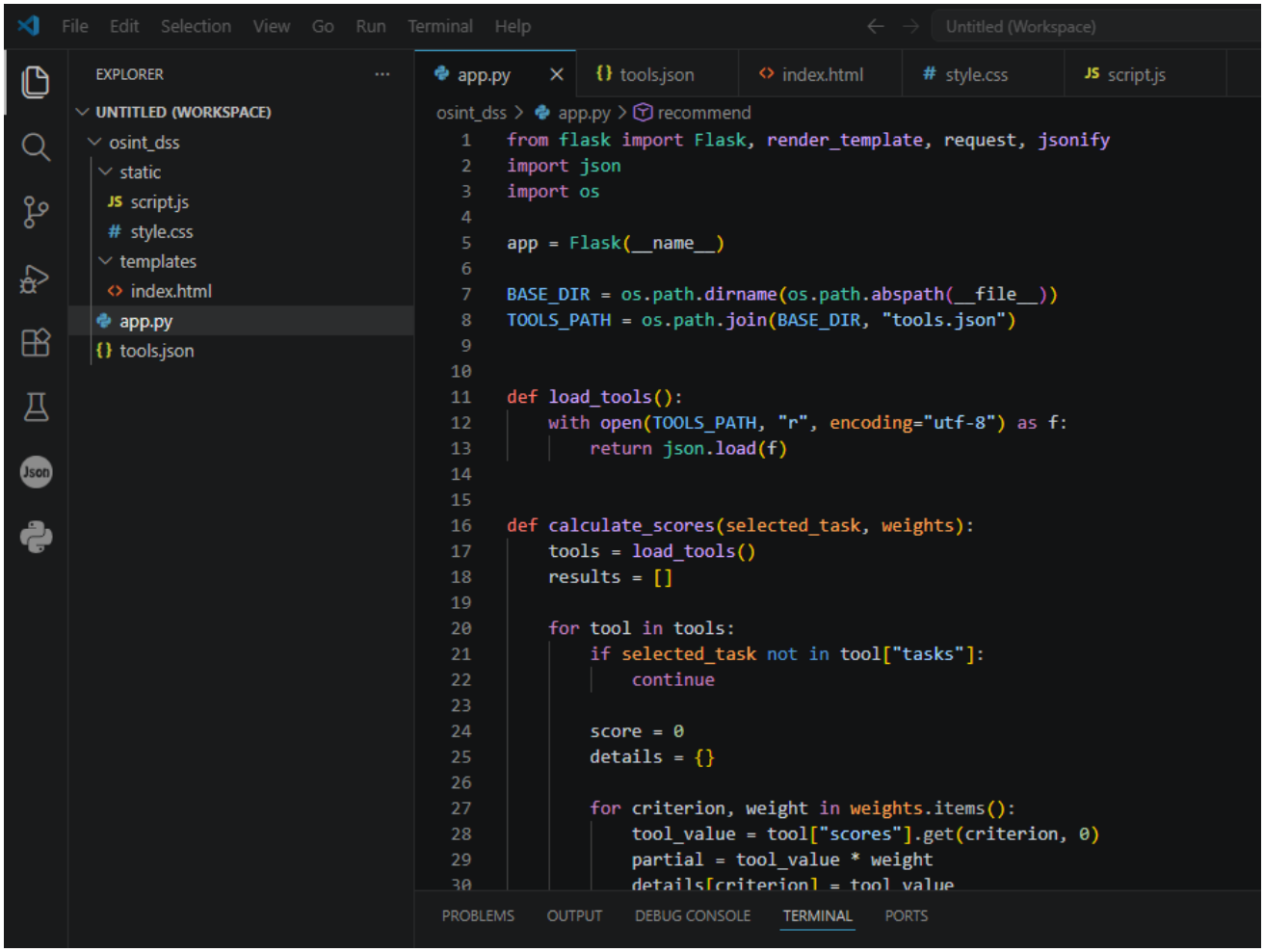


Рис. 3.2.3. Реалізація функції розрахунку інтегрального показника Score

Таким чином, реалізована база знань та система оцінювання критеріїв забезпечують автоматизований механізм підтримки прийняття рішень щодо вибору OSINT-інструментів. Структурований підхід до зберігання даних і

використання системи критеріїв дозволяють легко розширювати систему новими інструментами та адаптувати її до потреб фахівців з інформаційної безпеки.

3.3 Тестування системи на практичних кейсах інформаційної безпеки

Після завершення розробки системи було проведено тестування її роботи на практичних прикладах із сфери інформаційної безпеки. Основною метою тестування стала перевірка правильності роботи системи, коректності розрахунку оцінки Score та зручності використання інтерфейсу.

На рисунку 3.3.1 наведено головне вікно системи з формою введення параметрів.

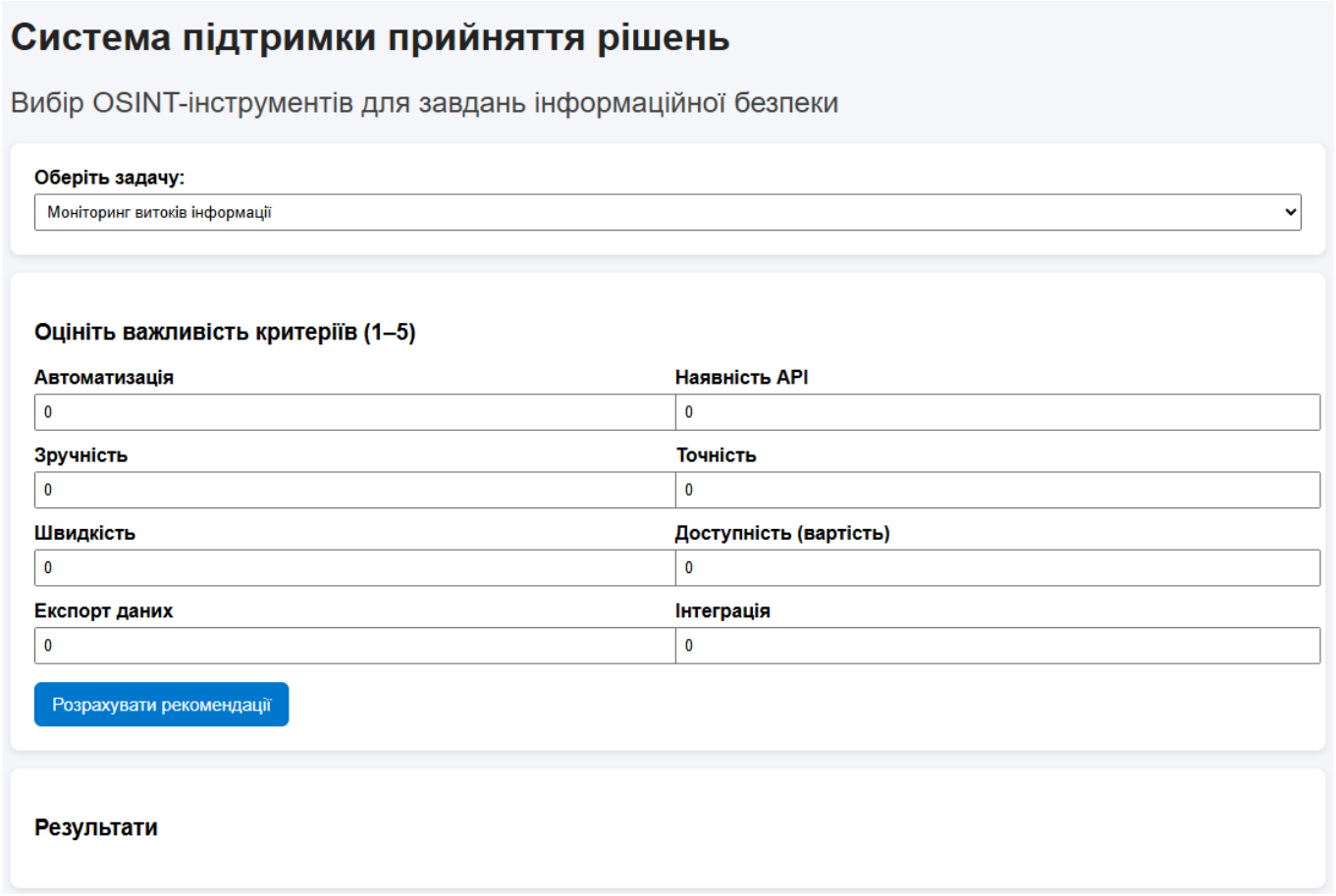
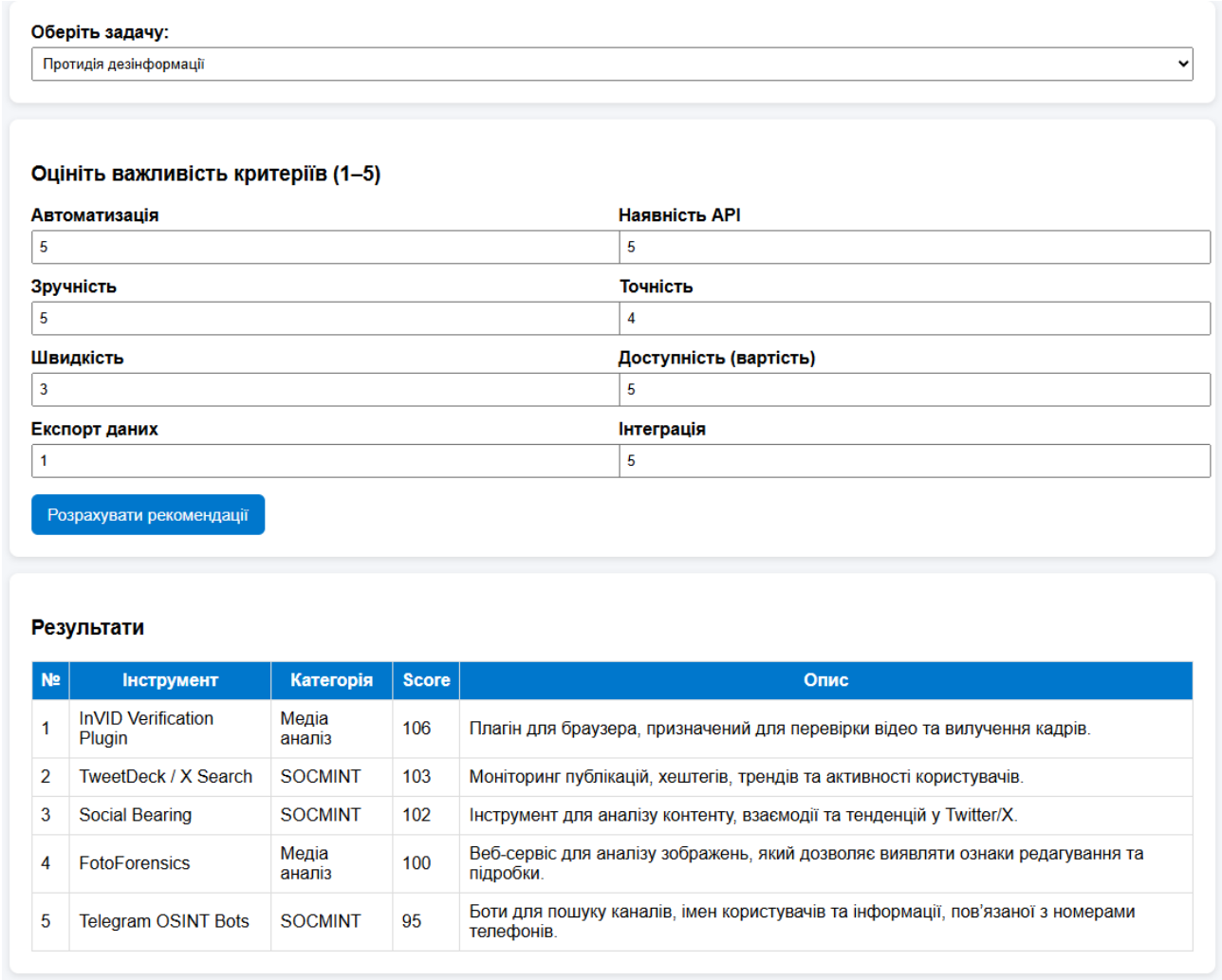


Рис. 3.3.1. Головне вікно системи

До прикладу, можна обрати вибір інструментів для протидії дезінформації. Встановлюємо бажані значення критеріїв автоматизації та точності результатів.

У результаті система сформувала рейтинг інструментів.



№	Інструмент	Категорія	Score	Опис
1	InVID Verification Plugin	Медіа аналіз	106	Плагін для браузера, призначений для перевірки відео та вилучення кадрів.
2	TweetDeck / X Search	SOCMINT	103	Моніторинг публікацій, хештегів, трендів та активності користувачів.
3	Social Bearing	SOCMINT	102	Інструмент для аналізу контенту, взаємодії та тенденцій у Twitter/X.
4	FotoForensics	Медіа аналіз	100	Веб-сервіс для аналізу зображень, який дозволяє виявляти ознаки редагування та підробки.
5	Telegram OSINT Bots	SOCMINT	95	Боти для пошуку каналів, імен користувачів та інформації, пов'язаної з номерами телефонів.

Рис. 3.3.2. Результати вибору інструментів для протидії дезінформації

Також було протестовано роботу системи для задач моніторингу витоків даних. Після зміни параметрів система автоматично оновила рейтинг та запропонувала інші інструменти, які краще відповідають поставленій задачі.

Моніторинг витоків інформації

Оцініть важливість критеріїв (1–5)

Автоматизація	**Наявність API**
2	4
Зручність	**Точність**
5	4
Швидкість	**Доступність (вартість)**
3	5
Експорт даних	**Інтеграція**
1	5

Розрахувати рекомендації

Результати

№	Інструмент	Категорія	Score	Опис
1	Have I Been Pwned	Моніторинг витоків	126	Сервіс для перевірки, чи з'являлась електронна пошта або домен у відомих базах витоків даних.
2	SpiderFoot	Автоматизація OSINT	119	Автоматизований OSINT-інструмент для розвідки, який містить багато модулів для збору інформації з відкритих джерел.
3	Wayback Machine	Веб-архіви	114	Історичний архів веб-сайтів, що використовується для цифрових розслідувань.
4	GitHub Search	Моніторинг витоків	112	Пошук по GitHub для виявлення витоків секретів, токенів, паролів, ключів API та конфіденційної інформації в репозиторіях.
5	IntelX (Intelligence X)	Моніторинг витоків	106	Пошукова система для витоків даних, даркнету, документів та наборів даних OSINT.
6	Archive.today	Веб-архіви	98	Сервіс створення статичних копій веб-сторінок для фіксації доказів та

Рис 3.3.3. Результати вибору інструментів для моніторингу витоків даних

Додатково було перевірено роботу системи для задач SOCMINT та аналізу соціальних мереж. Система коректно виконувала фільтрацію інструментів та формувала рейтинг відповідно до введених користувачем критеріїв.

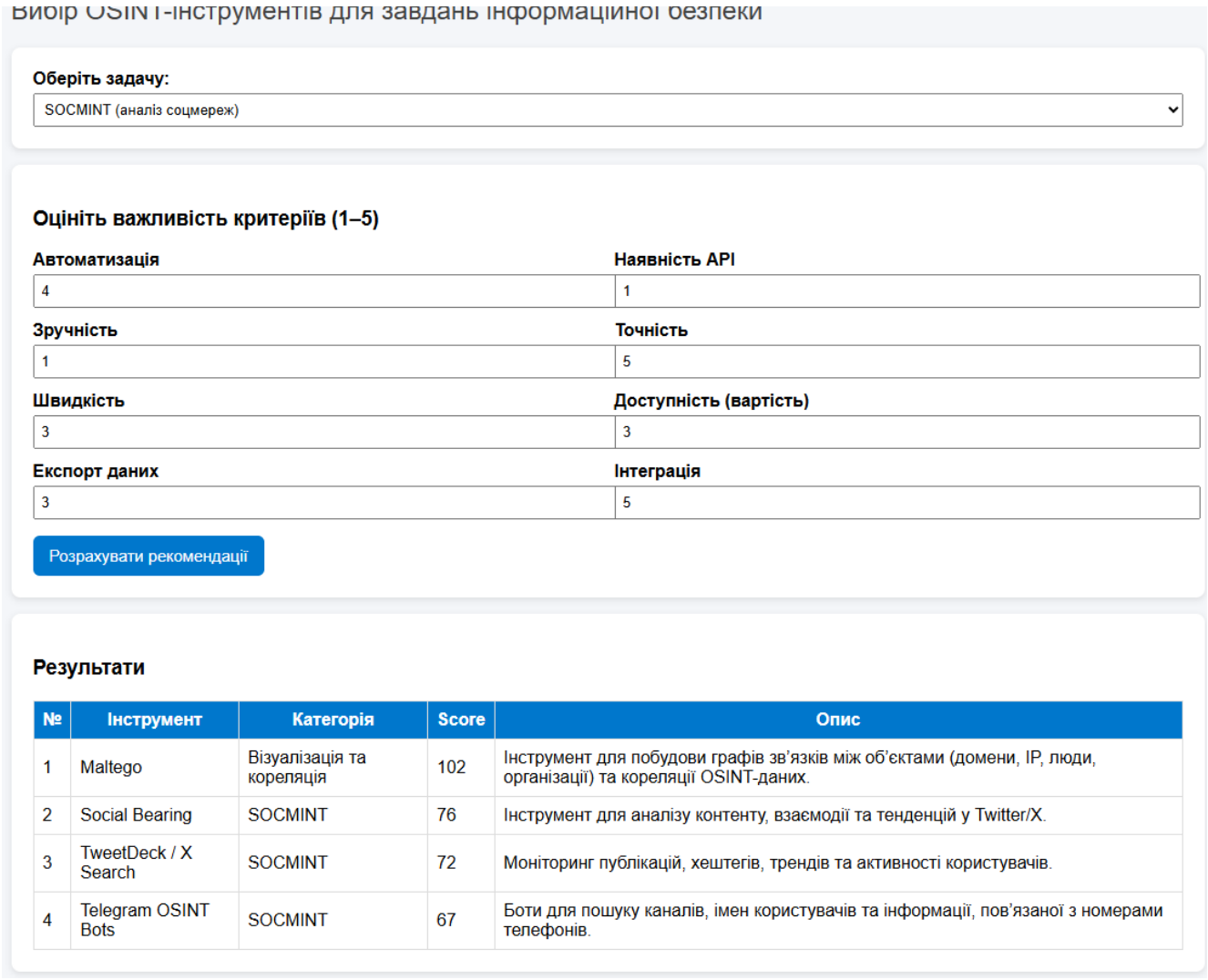


Рис. 3.3.4. Результати роботи системи для задач SOCMINT

У результаті тестування було встановлено, що система правильно виконує:

- обробку введених користувачем параметрів;
- фільтрацію інструментів за задачами;
- розрахунок показника Score;
- сортування та відображення результатів.

Отримані результати підтвердили працездатність реалізованої системи та можливість її використання для підтримки вибору OSINT-інструментів у сфері інформаційної безпеки.

Висновки до розділу 3

У третьому розділі було реалізовано систему підтримки вибору OSINT-інструментів для задач інформаційної безпеки. У процесі роботи було визначено та використано необхідні програмні засоби і технології для створення веб-додатка, зокрема мову програмування Python, фреймворк Flask, а також HTML, CSS і JavaScript для реалізації користувацького інтерфейсу.

У ході розробки було сформовано базу знань OSINT-інструментів, яка містить структуровану інформацію про інструменти, їх категорії, опис, підтримувані задачі та оцінки за визначеними критеріями. Це дозволило реалізувати механізм автоматизованого аналізу та порівняння інструментів залежно від потреб користувача.

Також у межах розділу було реалізовано систему оцінювання, що базується на використанні вагових коефіцієнтів критеріїв та розрахунку інтегрального показника Score. Реалізований механізм забезпечує формування рейтингу інструментів відповідно до обраної задачі інформаційної безпеки та заданих параметрів оцінювання.

Під час тестування системи на практичних кейсах було перевірено коректність роботи функціональних модулів, правильність фільтрації інструментів та формування результатів. Отримані результати підтвердили працездатність системи та можливість її використання для підтримки прийняття рішень під час вибору OSINT-інструментів.

Таким чином, у результаті виконання третього розділу було створено працездатний прототип системи підтримки вибору OSINT-інструментів, який може бути використаний як основа для подальшого розвитку та вдосконалення у сфері інформаційної безпеки.

ВИСНОВКИ

У результаті виконання кваліфікаційної роботи було досліджено особливості використання OSINT-інструментів у сфері інформаційної безпеки та проаналізовано сучасні підходи до автоматизації процесу їх вибору. Встановлено, що сьогодні існує велика кількість OSINT-засобів, які відрізняються функціональними можливостями, спеціалізацією, рівнем автоматизації та ефективністю застосування. Це ускладнює процес вибору оптимального інструмента для конкретної задачі інформаційної безпеки та створює потребу у використанні систем підтримки прийняття рішень.

У ході роботи було проаналізовано основні категорії OSINT-інструментів, які застосовуються для аналізу Attack Surface, моніторингу витоків даних, SOCMINT, GEOINT, аналізу метаданих, перевірки дезінформації та дослідження доменної інфраструктури. Досліджено функціональні можливості таких інструментів, як Shodan, Censys, VirusTotal, Wayback Machine, Archive.today, ExifTool та інших. Визначено їх переваги, особливості використання та значення для проведення OSINT-досліджень у сфері кібербезпеки.

У межах роботи було обґрунтовано необхідність створення системи підтримки вибору OSINT-інструментів, яка дозволяє автоматизувати процес аналізу та ранжування засобів залежно від поставленої задачі. Визначено основні вимоги до системи, критерії оцінювання інструментів та структуру бази знань, необхідної для реалізації механізму підтримки прийняття рішень.

У процесі дослідження було побудовано систему прийняття рішень щодо вибору OSINT-інструментів. Встановлено, що використання вагових коефіцієнтів критеріїв дозволяє адаптувати результати роботи системи до потреб користувача та специфіки задачі інформаційної безпеки. Розроблена система забезпечує фільтрацію інструментів за напрямами використання, аналіз критеріїв оцінювання та формування рейтингу найбільш релевантних засобів.

Також у роботі було спроєктовано архітектуру системи підтримки вибору OSINT-інструментів. Визначено основні функціональні модулі системи,

принцип їх взаємодії та логіку обробки даних. Встановлено, що модульний підхід до побудови системи забезпечує можливість подальшого розширення функціоналу та оновлення бази знань без суттєвих змін структури системи.

У практичній частині роботи було реалізовано веб-додаток системи підтримки вибору OSINT-інструментів із використанням мови програмування Python та фреймворку Flask. Розроблено механізм збереження бази знань, реалізовано систему оцінювання інструментів та алгоритм розрахунку інтегрального показника Score. Система дозволяє користувачу обирати задачу інформаційної безпеки, задавати вагу критеріїв оцінювання та отримувати список рекомендованих OSINT-інструментів, відсортованих за рейтингом.

У ході тестування системи було перевірено коректність роботи функціональних модулів, правильність розрахунку оцінок та логіку формування рекомендацій. Встановлено, що система коректно виконує фільтрацію інструментів, аналізує критерії оцінювання та формує результати відповідно до введених параметрів. Отримані результати підтвердили працездатність створеної системи та можливість її практичного використання у сфері інформаційної безпеки.

Практичне значення отриманих результатів полягає у можливості використання розробленої системи як допоміжного інструмента для фахівців з кібербезпеки, аналітиків OSINT, SOC-аналітиків та студентів спеціальності «Кібербезпека». Розроблена система може бути основою для подальшого вдосконалення, зокрема шляхом інтеграції API реальних сервісів, розширення бази знань, реалізації автоматичного оновлення даних та впровадження більш складних систем оцінювання і машинного навчання.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Мірошніченко І. О., Ланде Д. В. РОЛЬ МЕТОДІВ OSINT В КІБЕРБЕЗПЕЦІ ТА ЇХ ЗАСТОСУВАННЯ ПІД ЧАС ВОЄННИХ КОНФЛІКТІВ. Київ, 2024. С. 282-284. URL: https://ela.kpi.ua/server/api/core/bitstreams/a04460d3-93d9-48b7-ba83-f5bace2083ec/content

2. Ivkova V., Opirskyy I. OSINT TECHNOLOGIES AS A THREAT TO STATE CYBERSECURITY. *Cybersecurity: Education, Science, Technique*. 2025. Т. 3, № 27. С. 165–179. DOI: https://doi.org/10.28925/2663-4023.2025.27.749

3. Д.В. Ланде. OSINT у кібербезпеці : навч. пос. / Ланде Д.В. – Київ: ТОВ «Інжиніринг», 2024. С. 522. ISBN 978- 966-2344-97-4

4. Думчиков М.О. Відкрита розвідка (OSINT) у протидії інформаційним війнам: аналітичні інструменти та правові межі. Електронне наукове видання «Аналітично-порівняльне правознавство». 2025. Т. 2, № 6. С. 273–277. DOI: https://doi.org/10.24144/2788-6018.2025.06.2.43

5. Користін О., Демедюк С., Ісмайлов К., Ланде Д. та ін., за заг. ред. Користіна О.Є., Демедюка С.В.. OSINT Open Source Intelligence. Інструменти та методи: навчальний посібник – Київ: 7БЦ, 2025. С. 460. DOI: 10.32782/osint-instruments-2025 URL: https://aord.com.ua/cms/uploads/OSINT_Open_Source_Intelligence_Instrumenti_ta_metodi_31913d17f8.pdf

6. Полотай О., Балацька В. Використання OSINT у цифрових розслідуваннях кіберінцидентів. Львівський державний університет безпеки життєдіяльності. С. 184-187.

URL:https://sci.ldubgd.edu.ua/jspui/bitstream/123456789/17638/1/Polotai_Balatska.pdf

7. Івкова В. С., Опірський І. Р. Дослідження існуючих засобів та підходів до проведення OSINT в контексті інформаційної безпеки особи та держави. *Cybersecurity: Education, Science, Technique*. 2025. Т. 3, № 27. С. 165–179. DOI: https://doi.org/10.28925/2663-4023.2025.27.749

URL:https://science.lpnu.ua/uk/csn/vsi-vypusky/vypusk-7-nomer-1-2025/doslidzhennya-isnuyuchyh-zasobiv-ta-pidhodiv-do-provedennya

8. Легальне шпигунство: 3 кейси, коли OSINT корисний у роботі. Laba.ua [Електронний ресурс]. URL: https://laba.ua/blog/4345-lehalne-shpyhunstvo-3-keysy-koly-osint-korysnyy-v-roboti

9. Топ 10 OSINT-інструментів для розвідки з відкритим вихідним кодом. Softlist [Електронний ресурс]. URL: https://softlist.com.ua/ua/news/top-10-luchshykh-ynstrumentov-osint-dlia-razvedki-s-otkrytym-ishodnym-kodom

10. Могилевич Д., Могилевич В., Кононова І. АНАЛІЗ OSINT ІНСТРУМЕНТІВ ДЛЯ ДОСЛІДЖЕННЯ СОЦІАЛЬНИХ МЕРЕЖ. Herald of Khmelnytskyi National University. Technical sciences. 2025. Т. 359, № 6.1. С. 235–242. DOI: https://doi.org/10.31891/2307-5732-2025-359-33

URL:https://heraldts.khmnu.edu.ua/index.php/heraldts/article/download/2290/2209/7702

11. Поради з використання сервісу Wayback Machine від Internet Archive у вашому наступному розслідуванні. Global Investigative Journalism Network. 2021 [Електронний ресурс]. URL:https://gijn.org/ua/resurs-ua/poradi-z-vikoristanna-servisu-wayback-machine-vid-internet-archive-u-vasomu-nastupnomu-rozsliduvanni/

12. Веб-архів: як подивитися, як виглядав сайт раніше. Advermedia Blog. 2023 [Електронний ресурс]. URL:https://advermedia.ua/blog/web-archive-yak-podivitisya-yak-viglyadav-sajt-ranishe/

13. ExifTool – Metadata Analyzer [Електронний ресурс]. URL: https://exiftool.org

14. Главацька, А., Ангельська , О., Опірський, І. ДОСЛІДЖЕННЯ ТЕХНОЛОГІЇ ВИКОРИСТАННЯ OSINT ЯК НОВОЇ ЗАГРОЗИ З ДЕАНОНІМІЗАЦІЇ ОСОБИ В ІНТЕРНЕТ ПРОСТОРІ. *Cybersecurity: Education, Science, Technique*. 2024. Т. 1, № 25. С. 19–50. DOI: https://doi.org/10.28925/2663-4023.2024.25.1950

URL:https://csecurity.kubg.edu.ua/index.php/journal/article/view/647

15. Зоренко Д.С., Лех Р.В., Кулик Д. О., Червяков О. І. ВИКОРИСТАННЯ

ІНСТРУМЕНТІВ ТА МЕТОДІВ OSINT ДЛЯ ОТРИМАННЯ ПОШУКОВОЇ ІНФОРМАЦІЇ. Практичний порадник 4-те видання. ІПЮК для СБУ, 2023. 36 с. URL: https://dspace.nlu.edu.ua/server/api/core/bitstreams/d67bcc03-5055-42c6-8c94-44d6adcc2276/content

16. Shodan: Search Engine for Internet-Connected Devices. [Електронний ресурс]. URL: https://www.shodan.io/

17. Censys: Search Engine for Cyber Analysis and Attack Surface Management. [Електронний ресурс]. URL: https://censys.io/

18. BuiltWith: Technology Lookup and Web Infrastructure Analytics. [Електронний ресурс]. URL: https://builtwith.com/

19. VirusTotal: Intelligence Overview and Malware Dataset Analysis. [Електронний ресурс]. URL: https://www.virustotal.com/gui/intelligence-overview

20. Have I Been Pwned: OSINT Data Breach Analysis Tool. OSINT Newsletter. [Електронний ресурс]. URL: https://tools.osintnewsletter.com/osint-tools/have-i-been-pwned

21. IntelX: Intelligence X Search Engine and Data Archive. [Електронний ресурс]. URL: https://intelx.io/about

22. SpiderFoot: Automated OSINT Collection and Threat Intelligence Tool. [Електронний ресурс]. URL: https://spiderrfoot.com/

23. Beginners guide to Recon-ng. Hackercool Magazine. 2025. [Електронний ресурс]. URL: https://hackercoolmagazine.com/beginners-guide-to-recon-ng/?srsltid=AfmBOoqf0k3UTFKz_7bJKHP8GpW7Xm5j_TgyqzZmzunnpjS1YpV8rwy3

24. Maltego: The Future of OSINT and Data Link Analysis. Maltego Blog. [Електронний ресурс]. URL: https://www.maltego.com/blog/the-future-of-osint

25. WHOIS Lookup: Mastering WHOIS OSINT for Effective Domain and IP Investigations. WhoisFreaks Resource. [Електронний ресурс]. URL: https://whoisfreaks.com/resources/blog/mastering-whois-osint-for-effective-domain-and-ip-investigations

26. SecurityTrails: Top 5 Domain and IP Intelligence Tools in OSINT. Dev.to.

[Електронний ресурс]. URL: https://dev.to/stark_zhuang_df5076f35c68/top-5-domain-and-ip-intelligence-tools-in-osint-2a73

27. FotoForensics: Photo Forensic and IMINT Guide. *KR-Labs Research*. [Електронний ресурс]. URL:https://research.kr-labs.com.ua/photo-forensic-and-imint-guide/

28. Google Dorks на службі у OSINT. KR. 2023. Labs Research. [Електронний ресурс]. URL: https://research.kr-labs.com.ua/google-dorks-for-osint/

29. A selection of the best Telegram OSINT bots. 2023. HackYourMom. [Електронний ресурс]. URL: https://hackyourmom.com/en/servisy/dobirka-krashhyh-osint-botiv-telegram/

30. How to Use TweetDeck for Open Source Investigations. 2019. Global Investigative Journalism Network. [Електронний ресурс]. URL: https://gijn.org/stories/how-to-use-tweetdeck-for-open-source-investigations/

31. Exploring Google OSINT. 2024. [Електронний ресурс]. URL: Medium. https://osintteam.blog/exploring-google-osint-ebb7ddd0cb6b

32. Sentinel Hub: Satellite Imagery and Earth Observation Systems for OSINT. [Електронний ресурс]. URL: https://www.sentinel-hub.com/

33. Python. [Електронний ресурс]. URL: https://uk.wikipedia.org/wiki/Python

34. Flask. [Електронний ресурс]. URL: https://uk.wikipedia.org/wiki/Flask

35. Введення в HTML. Основи. HyperskillUA. [Електронний ресурс]. URL: https://w3schoolsua.github.io/hyperskillua/34/index.html#gsc.tab=0

36. JSON. [Електронний ресурс]. URL: https://uk.wikipedia.org/wiki/JSON

37. Visual Studio Code. [Електронний ресурс]. URL: https://uk.wikipedia.org/wiki/Visual_Studio_Code

38. Лозова І. Л., Клопова А. А. Система підтримки вибору OSINT-інструментів для вирішення завдань інформаційної безпеки. Стратегії кіберстійкості: управління ризиками та безперервність бізнесу: матеріали всеукр. наук.-практ. конф., м. Київ, 25 лютого 2026 р. С. 100-103.

Додаток А

ПРОГРАМНИЙ ЛІСТИНГ

app.py

```
from flask import Flask, render_template, request, jsonify
import json
import os
app = Flask(__name__)
BASE_DIR = os.path.dirname(os.path.abspath(__file__))
TOOLS_PATH = os.path.join(BASE_DIR, "tools.json")
def load_tools():
    with open(TOOLS_PATH, "r", encoding="utf-8") as f:
        return json.load(f)
def calculate_scores(selected_task, weights):
    tools = load_tools()
    results = []
    for tool in tools:
        if selected_task not in tool["tasks"]:
            continue
        score = 0
        details = {}
        for criterion, weight in weights.items():
            tool_value = tool["scores"].get(criterion, 0)
            partial = tool_value * weight
            details[criterion] = tool_value
            score += partial
        results.append({
            "name": tool["name"],
            "category": tool["category"],
            "description": tool["description"],
            "score": round(score, 2),
```

```
            "details": details
        })
    results.sort(key=lambda x: x["score"], reverse=True)
    return results
@app.route("/")
def index():
    return render_template("index.html")
@app.route("/recommend", methods=["POST"])
def recommend():
    data = request.json
    print("REQUEST DATA:", data)
    selected_task = data.get("task")
    weights = data.get("weights")
    results = calculate_scores(selected_task, weights)
    print("RESULTS COUNT:", len(results))
    return jsonify({
        "task": selected_task,
        "results": results[:10]
    })
if __name__ == "__main__":
    app.run(debug=True)
```

index.html

```
<!DOCTYPE html>
<html lang="uk">
<head>
    <meta charset="UTF-8">
    <title>СППР вибору OSINT-інструментів</title>
    <link rel="stylesheet" href="/static/style.css">
</head>
<body>
```

```
  <div class="container">
    <h1>Система підтримки прийняття рішень</h1>
    <h2>Вибір OSINT-інструментів для завдань інформаційної безпеки</h2>
    <div class="block">
      <label>Оберіть задачу:</label>
      <select id="task">
        <option value="leaks">Моніторинг витоків інформації</option>
        <option value="phishing">Виявлення фішингу та шкідливих
доменів</option>
        <option value="attack_surface">Оцінка Attack Surface </option>
        <option value="socmint">SOCMINT (аналіз соцмереж)</option>
        <option value="geoint">GEOINT (геопросторовий аналіз)</option>
        <option value="metadata">Аналіз метаданих / медіа</option>
        <option value="threat_intel">Threat Intelligence / кореляція</option>
        <option value="disinfo">Протидія дезінформації</option>
      </select>
    </div>
    <div class="block">
      <h3>Оцініть важливість критеріїв (1–5)</h3>
      <div class="grid">
        <div>
          <label>Автоматизація</label>
          <input type="number" id="automation" min="1" max="5" value="5">
        </div>
        <div>
          <label>Наявність API</label>
          <input type="number" id="api" min="1" max="5" value="4">
        </div>
        <div>
          <label>Зручність</label>
```

```
            <input type="number" id="usability" min="1" max="5" value="4">
        </div>
        <div>
            <label>Точність</label>
            <input type="number" id="accuracy" min="1" max="5" value="5">
        </div>
        <div>
            <label>Швидкість</label>
            <input type="number" id="speed" min="1" max="5" value="4">
        </div>
        <div>
            <label>Доступність (вартість)</label>
            <input type="number" id="cost" min="1" max="5" value="3">
        </div>
        <div>
            <label>Експорт даних</label>
            <input type="number" id="export" min="1" max="5" value="3">
        </div>
        <div>
            <label>Інтеграція</label>
            <input type="number" id="integration" min="1" max="5" value="4">
        </div>
    </div>
    <button onclick="getRecommendations()">Розрахувати
рекомендації</button>
</div>
<div class="block">
    <h3>Результати</h3>
    <div id="results"></div>
</div>
```

```
    </div>
    <script src="/static/script.js"></script>
</body>
</html>
```

style.css

```
body {
    font-family: Arial, sans-serif;
    background: #f4f6f9;
    margin: 0;
    padding: 0;
}
.container {
    width: 90%;
    max-width: 1100px;
    margin: auto;
    padding: 20px;
}
h1 {
    color: #222;
}
h2 {
    color: #444;
    font-weight: normal;
}
.block {
    background: white;
    padding: 20px;
    margin-top: 15px;
    border-radius: 8px;
    box-shadow: 0 2px 6px rgba(0,0,0,0.1);
```

```
}
.grid {
    display: grid;
    grid-template-columns: repeat(2, 1fr);
    gap: 12px;
    margin-top: 10px;
}
label {
    font-weight: bold;
}
input, select {
    width: 100%;
    padding: 6px;
    margin-top: 4px;
}
button {
    margin-top: 15px;
    padding: 10px 15px;
    border: none;
    background: #0077cc;
    color: white;
    cursor: pointer;
    border-radius: 6px;
    font-size: 15px;
}
button:hover {
    background: #005fa3;
}
table {
    width: 100%;
```

```
    border-collapse: collapse;
    margin-top: 15px;
}
table th, table td {
    border: 1px solid #ddd;
    padding: 8px;
}
table th {
    background: #0077cc;
    color: white;
}
```

script.js

```
async function getRecommendations() {
    const task = document.getElementById("task").value;
    const weights = {
        automation: parseInt(document.getElementById("automation").value),
        api: parseInt(document.getElementById("api").value),
        usability: parseInt(document.getElementById("usability").value),
        accuracy: parseInt(document.getElementById("accuracy").value),
        speed: parseInt(document.getElementById("speed").value),
        cost: parseInt(document.getElementById("cost").value),
        export: parseInt(document.getElementById("export").value),
        integration: parseInt(document.getElementById("integration").value)
    };
    const response = await fetch("/recommend", {
        method: "POST",
        headers: {"Content-Type": "application/json"},
        body: JSON.stringify({task: task, weights: weights})
    });
    const data = await response.json();
```

```
    if (data.error) {
        document.getElementById("results").innerHTML = "<p>Помилка: " +
data.error + "</p>";
        return;
    }
    let html =
"<table><tr><th>№</th><th>Інструмент</th><th>Категорія</th><th>Score</th><
th>Опис</th></tr>";
    data.results.forEach((tool, index) => {
        html += `<tr>
            <td>${index + 1}</td>
            <td>${tool.name}</td>
            <td>${tool.category}</td>
            <td>${tool.score}</td>
            <td>${tool.description}</td>
        </tr>`;
    });
    html += "</table>";
    document.getElementById("results").innerHTML = html;
}
```