https://www.sworldjournal.com/index.php/swj/article/view/swj25-00-034
DOI: 10.30888/2663-5712.2024-25-00-034

УДК 004.056.5

TECHNICAL STACK FOR OPEN SOURCE INTELLIGENCE
ТЕХНІЧНИЙ СТЕК РОЗВІДКИ З ВІДКРИТИХ ДЖЕРЕЛ

Korobeinikova T.I. / Коробейнікова Т.І.
c.t.s., as.prof. / к.т.н., доц.
ORCID: 0000-0003-2487-8742
Symak I.A. / Симак І.А.
студент / student
Lviv Polytechnic National University, S. Bandera St. 12, Lviv, 79013
Національний університет «Львівська політехніка», Львів, Бандери, 12, 79013

Анотація. *Розвідка відкритих джерел (OSINT) є важливою концепцією, методологією та технологією, що дозволяє збирати інформацію з відкритих джерел. У статті розглядається зв'язок між OSINT та іншими типами розвідки, зокрема HUMINT, яка використовує етичні методи збору інформації. З 2014 року Україна також намагається інтегрувати OSINT у військову сферу, проте її застосування в державному управлінні ще перебуває на стадії наукових розробок, що підкреслює актуальність дослідження цієї теми. Основна частина статті присвячена технічному стеку OSINT, який включає різноманітні інструменти та методи для збору та аналізу інформації. Розглядаються різні фреймворки, такі як OSINT Framework і MetaOSINT, які допомагають організувати та стандартизувати процес OSINT-розслідувань, полегшуючи роботу аналітиків. Описуються також інші інструменти, такі як Telegram-боти та техніка Dorks, які є ефективними для збору первинних даних. Наведено приклади корисних ресурсів, зокрема онлайн-спільнота HackYourMom та український OSINT-практик Molfar, які пропонують цінні колекції інструментів та ресурсів для дослідників і аналітиків. Стаття акцентує увагу на важливості вибору правильних методів та засобів для успішного OSINT-розслідування, підкреслюючи роль творчості та уяви аналітика у цьому процесі.*

Ключові слова: *розвідка відкритих джерел (OSINT), HUMINT, технічний стек OSINT, інструменти OSINT, фреймворк OSINT, MetaOSINT, Telegram-боти, техніка Dorks, національна безпека, аналіз інформації.*

Вступ.

Розвідка відкритих джерел (Open source intelligence, OSINT) – це концепція, методологія і технологія збору без інформації, яка доступна з відкритих джерел [1].

Окрім OSINT, існує ще один важливий напрямок розвідки – HUMINT ("human intelligence", розвідка по людях), що використовує етичні методи збору інформації, не завдаючи шкоди людям [2].

У сучасному світі HUMINT та OSINT тісно пов'язані і використовують багато спільних технологічних інструментів [3-5]. За оцінками експертів, розвідслужби США отримують від 35% до 95% розвідданих саме з відкритих джерел [6].

В провідних країнах світу OSINT визнаний як ключовий елемент для захисту національних інтересів та основа роботи силових відомств. В США та країнах НАТО існують цілі мережі центрів, що збирають, обробляють та аналізують інформацію з відкритих джерел. В Україні з 2014 року робляться спроби використовувати OSINT у військовій сфері. Проте, застосування цього інструменту в державному управлінні все ще перебуває на стадії наукових розробок. Це робить тему OSINT актуальною для досліджень.

Технічний стек розвідки з відкритих джерел.

Технічний стек розвідки з відкритих джерел містить інструменти та методи для збору та аналізу інформації. Компоненти стека можуть варіюватися в залежності від конкретних завдань.

Методи та засоби OSINT.

Важливо розуміти, що не існує єдиного універсального методу або засобу OSINT. Кожне розслідування залежить від уяви та творчості аналітика а також способу подання результатів. Вибір методу та засобу залежить від конкретної задачі, яку потрібно вирішити (табл. 1 і 2) [7].

Таблиця 1 – Методи OSINT

Пошук за ключовими словами	Пошук за зображенням	Форензичний аналіз цифрових слідів	Пошук інформації в Dark Web
Аналіз контенту	Мережевий аналіз	Геопросторовий аналіз	Веб-скрапінг
Перевірка достовірності	Перевірка фактів	Підтвердження з інших джерел	Моніторинг
Пошук людей	Аналіз мови та тексту	Моніторинг веб-камер і дронів	Візуалізація даних

Авторська розробка

Таблиця 2 – Засоби OSINT

Пошукові системи: Google, Bing, DuckDuckGo;	Соц.мережі: Facebook, Twitter, LinkedIn, Telegram, Instagram;	Інструменти для пошуку зображень: TinEye, Google Images, Yandex Images;	Новинні портали: BBC, CNN, Reuters; Виявлення фейків: Fake News Watch, Bellingcat
Урядові веб-сайти: Державні портали, веб-сайти міністерств;	Наукові репозиторії: PubMed, arXiv, Google Scholar;	Бази даних: LexisNexis, Factiva, World Bank Open Data;	Інструменти для веб-скрапінгу: Scrapy, BeautifulSoup, Selenium;
Інструменти для аналізу даних: Excel, Python, Maltego;	Інструменти для візуалізації даних: Tableau, Power BI, Google Charts;	Інструменти для мережевого аналізу: Gephi, NodeXL;	Інструменти для геопросторового аналізу: QGIS, ArcGIS;
Форуми та веб-сайти: Reddit, Quora;	Інструменти для пошуку в темному веб: TOR, I2P;	Інструменти для аналізу зображень: EXIFTool, FotoForensics;	Інструменти для перевірки фактів: FactCheck.org, PolitiFact;

Авторська розробка

OSINT інструменти для збору та аналізу інформації.

Фреймворки OSINT – це програмні комплекси, які допомагають збирати, аналізувати та візуалізувати інформацію з відкритих джерел. Вони пропонують широкий спектр інструментів та функцій, які полегшують процес OSINT-розслідувань і роблять OSINT-розвідку більш організованою, стандартизованою та ефективною, дозволяючи розвідникам зосередитися на найважливіших аспектах дослідження.

OSINT Framework. Серед найвідоміших фреймворків є OSINT Framework [8] (рис. 1). Цей веб-сайт слугує порталом до безлічі джерел інформації, охоплюючи практично всі аспекти OSINT-розвідки. Для кращого орієнтування та зручного пошуку всі дані на OSINT Framework чітко структуровані за категоріями.

Кожна категорія містить ретельно підібрані посилання на інструменти, ресурси та сервіси, які допоможуть отримати необхідну інформацію з відповідних джерел.

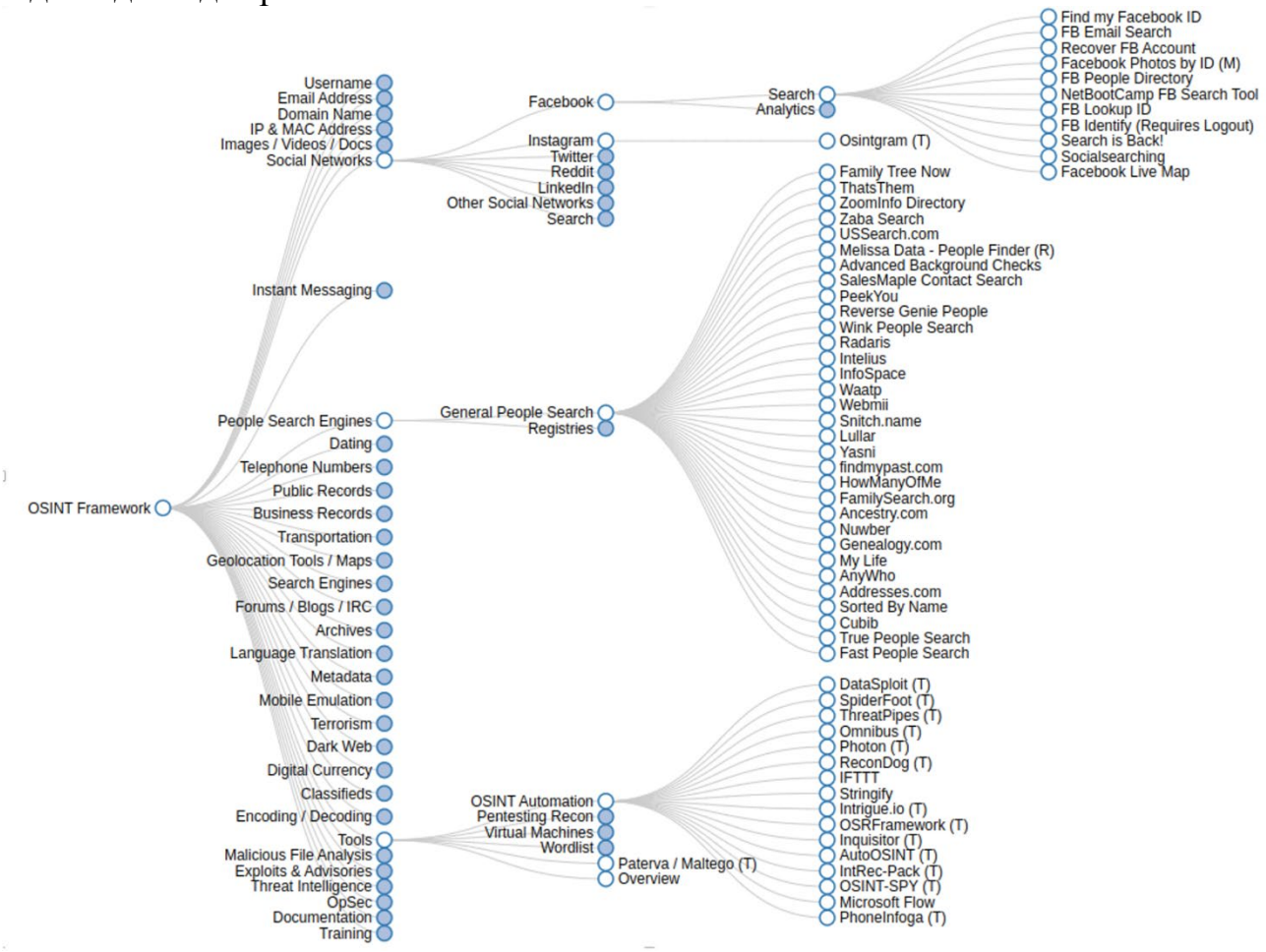

Рисунок 1 – Інтерфейс та інструменти OSINT Framework

Джерело [8]

OSINT Framework пропонує широкий спектр категорій з інструментами та джерелами інформації (табл. 3).

MetaOSINT. MetaOSINT (табл. 4) – це безкоштовний онлайн-каталог, який агрегує та систематизує "найкращі" інструменти та ресурси для OSINT розвідки з відкритих джерел. Він створений для того, щоб дослідники, аналітики та ентузіасти OSINT могли швидко знаходити потрібні їм інструменти та

економити час на пошуку [9]. У 2018 році, проводячи цифрові розслідування на колишній посаді, автор почав створювати закладки для списків інструментів і ресурсів, корисних для OSINT. Колекція зростала, і після структурування була опублікована у вигляді веб-додатку MetaOSINT у 2021 році [10].

Таблиця 3 – OSINT Framework

Пошукові системи	Соціальні мережі	Блоги та форуми	Телефонні номери
Медіаплатформи	Інструменти аналізу	IP-адреси	Географічні ресурси
Хеш-значення	Аналіз зображень	Аналізу тексту	…

Авторська розробка

Таблиця 4 – OSINT Основні функції MetaOSINT

300 інструментів OSINT-розвідки	Зручна категоризація	Детальні описи інструментів
Пошук за ключовими словами	Система рейтингів	Постійне оновлення

Авторська розробка

HackYourMom – це онлайн-спільнота, академія та кібер-армія, яка фокусується на кібербезпеці та OSINT. Вони пропонують різні ресурси для OSINT-дослідників, включаючи колекції ресурсів, які містять посилання на корисні веб-сайти, інструменти та бази даних [11]. Важливо зазначити, що HackYourMom – це спільнота, яка орієнтована на фахівців з кібербезпеки та OSINT-дослідників. Їхні ресурси можуть бути складними для початківців, але вони можуть бути дуже корисними для досвідчених користувачів. Окрім колекцій ресурсів, HackYourMom також пропонує: статті та блоги про різні теми, пов'язані з кібербезпекою та OSINT; форуми, де користувачі можуть спілкуватися один з одним та ділитися своїми знаннями; навчальні курси з кібербезпеки та OSINT.

Molfar – це український OSINT-практик, який щедро ділиться своїми знаннями та досвідом через блог, YouTube-канал та Telegram-канал. Він також пропонує платні OSINT-консультації та навчання. Серед ресурсів Molfar можна виділити кілька цінних колекцій [12]:

- OSINT-інструменти: пошукові системи, соціальні мережі, геолокаційні інструменти, аналітичні інструменти тощо;
- Реєстри юридичних осіб: бази даних, державні та приватні реєстри юридичних осіб в різних країнах світу;
- OSINT розслідування: описи реальних OSINT-розслідувань, які були проведені Molfar та іншими OSINT-практиками.

Важливо зазначити, що колекції ресурсів Molfar постійно оновлюються та доповнюються новими інструментами, ресурсами та інформацією. Це робить їх цінним джерелом OSINT.

Dorks – найефективніша техніка отримання первинних даних на початку OSINT розслідування. Dorks, також відомі як Hacking Operators, – це спеціальні пошукові запити, які дозволяють знаходити конкретну інформацію в пошукових системах. Вони використовуються OSINT-практиками для збору первинних даних на початковому етапі розслідування. Dorks дають можливість виявляти веб-сайти, файли, каталоги, зображення, документи та інші дані, які можуть бути релевантними для розслідування.

Соціальні мережі стали невід'ємною частиною життя багатьох людей і крім розважальної функції є цінним джерелом інформації про людей, включаючи їхні особисті дані, уподобання, політичні погляди тощо.

Telegram боти є одним з інструментів, які використовуються для для пошуку інформації про особу. Ці програмні інструменти, які автоматизують процес збору даних з відкритих джерел та можуть допомогти дослідникам знайти потрібну інформацію з меншою затратою ресурсів та часу. Зазвичай бот поєднує в собі декілька десятків інструментів та повертає опрацьовану інформацію із кожного з них.

Висновки. У роботі запропоновано технічний стек розвідки з відкритих джерел, що надає важливий огляд концепції та практичного застосування розвідки відкритих джерел у сучасному світі. Зокрема в роботі, підкреслено важливість співіснування OSINT і HUMINT, демонструючи, що обидва напрямки розвідки взаємопов'язані і використовують спільні технологічні засоби. Висвітлюється ключова роль OSINT у захисті національних інтересів та державної безпеки, особливо в контексті розвинених країн, де існують спеціалізовані центри збору та аналізу інформації з відкритих джерел. Оглядаються основні компоненти технічного стеку розвідки з відкритих джерел, що включають методи та інструменти для збору та аналізу інформації. Представлені різні фреймворки та інструменти, такі як OSINT Framework і MetaOSINT, які сприяють ефективному збору, аналізу та візуалізації інформації. В статті наведено приклади корисних ресурсів, таких як онлайн-спільнота HackYourMom та український OSINT-практик Molfar, які надають цінні інструменти та ресурси для дослідників і аналітиків. В цілому, стаття підкреслює важливість розвідки відкритих джерел у сучасному світі, як ключового елементу для забезпечення національної безпеки та ефективного аналізу інформації.

Література:

1. Ржевська Н.Ф. Розвідка відкритих джерел (OPEN SOURCE INTELLIGENCE) Ржевська Н. Ф., Кожушко О. О. Розвідка відкритих джерел. URL: http://ena.lp.edu.ua/bitstream/ntb/19232/1/53 – Rzhevska-257-261.pdf.

2. Минько О. В. Використання технологій OSINT для отримання розвідувальної інформації / О. В. Минько, О. Ю. Іохов, В. Т. Оленченко, К. В. Власов // Системи управління, навігації та зв'язку. – 2016. – Вип. 4. – С. 81-84. – Режим доступу: http://nbuv.gov.ua/UJRN/suntz_2016_4_22.

3. Нсер, А. М., Міночкін, Д. А. (2022). Розвідка на основі відкритих джерел. Збірник матеріалів міжн. НТК «Перспективи телекомунікацій», 224–226. http://conferenc.its.kpi.ua/proc/article/view/256894.

4. Heather J. Williams, Ilana Blum. Defining Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise https://www.rand.org/pubs/research_reports/RR1964.html

5. National defense authorization act for fiscal year 2006. URL: http://www.dod.gov/dodgc/olc/docs/PL109-163.pdf

6. Open source intelligence (Headquarters, Department of the Army) URL: https://fas.org/irp/doddir/army/fmi2- 22-9.pdf

7. Яровой, Т. С. (2019). OSINT, як перспективний інструмент контролю за лобістською діяльністю в контексті державної безпеки. Експерт: парадигми юридичних наук і державного управління, (4(6), 201-208. https://doi.org/10.32689/2617-9660-2019-4(6)-201-208

8. OSINT Framework [Електронний ресурс] – Режим доступу до ресурсу: https://osintframework.com/.

9. Metaosint [Електронний ресурс] – Режим доступу до ресурсу: https://metaosint.github.io/.

10. 2023 OSINT Landscape Trends: A Data-Driven Analysis [Електронний ресурс] – Режим доступу до ресурсу: https://metaosint.github.io/2023-osint-trends-analysis.html.

11. Засоби розслідування та колекції ресурсів OSINT (Частина 2) [Електронний ресурс] – Режим доступу до ресурсу: https://hackyourmom.com/kibervijna/zasoby-rozsliduvannya-ta-kolekcziyi-resursiv-osint-chatsyna-2/.

12. Molfar – OSINT [Електронний ресурс] – Режим доступу до ресурсу: https://molfar.com.

Abstract. *Open Source Intelligence (OSINT) is an important concept, methodology, and technology that enables the collection of information from open sources. The article examines the relationship between OSINT and other types of intelligence, specifically HUMINT, which uses ethical methods of information gathering. Since 2014, Ukraine has also been attempting to integrate OSINT into the military sphere, but its application in government administration is still at the stage of scientific development, highlighting the relevance of researching this topic. The main part of the article is dedicated to the OSINT technological stack, which includes various tools and methods for collecting and analyzing information. Different frameworks, such as OSINT Framework and MetaOSINT, are discussed, which help organize and standardize the OSINT investigation process, making analysts' work easier. Other tools, such as Telegram bots and Dorks techniques, which are effective for collecting primary data, are also described. Examples of useful resources are provided, including the online community HackYourMom and the Ukrainian OSINT practitioner Molfar, which offer valuable collections of tools and resources for researchers and analysts. The article emphasizes the importance of choosing the right methods and tools for successful OSINT investigations, highlighting the role of creativity and imagination of the analyst in this process.*

Keywords: *Open Source Intelligence (OSINT), HUMINT, OSINT technological stack, OSINT tools, OSINT framework, MetaOSINT, Telegram bots, Dorks technique, national security, information analysis.*

Науковий керівник: к.т.н., доц. Коробейнікова Т.І.

Стаття надіслана: 19.05.2024 р.