КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (34), 2026
ISSN 2663 – 4023
DOI 10.28925/2663-4023.2026.34.1392
УДК 004.056.53

Лозова Ірина Леонідівна
кандидат технічних наук
доцент кафедри управління кібербезпекою та захистом інформації
Державний університет інформаційно-комунікаційних технологій, Київ, Україна
ORCID: 0000-0002-7224-4763
illozovaya@gmail.com

Різак Михайло Васильович
доктор юридичних наук, старший дослідник
професор кафедри технічних систем кіберзахисту
Державний університет інформаційно-комунікаційних технологій, Київ, Україна
ORCID: 0009-0003-9844-3271
advokat.rizak@gmail.com

Лепеха Олег Миколайович,
кандидат юридичних наук
докторант
Державний університет інформаційно-комунікаційних технологій, Київ, Україна
ORCID: 0000-0003-1308-3469
olm3000@gmail.com

МЕТОДОЛОГІЧНИЙ ПІДХІД ДО ВИБОРУ OSINT-ІНСТРУМЕНТІВ ДЛЯ ВИРІШЕННЯ ЗАВДАНЬ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Анотація. У статті запропоновано методологічний підхід до вибору інструментів розвідки на основі відкритих джерел інформації (Open Source Intelligence, OSINT) для вирішення завдань інформаційної безпеки. Актуальність дослідження зумовлена значною кількістю сучасних OSINT-інструментів, їх функціональною спеціалізацією, відмінностями в рівні автоматизації, доступності, точності, можливостях інтеграції та характері інформаційних джерел. Це ускладнює обґрунтований вибір засобу для конкретного завдання та підвищує залежність результату від досвіду аналітика. На основі аналізу сучасних підходів до застосування OSINT систематизовано основні категорії інструментів, зокрема засоби оцінювання зовнішньої поверхні атаки, моніторингу витоків інформації, аналізу доменної та мережевої інфраструктури, SOCMINT, GEOINT, аналізу метаданих, візуалізації та кореляції даних. Запропоновано формалізувати процес вибору як багатокритеріальну процедуру, що складається з первинної фільтрації інструментів за відповідністю завданню інформаційної безпеки та подальшого ранжування за інтегральним показником. Для оцінювання запропоновано використовувати критерії рівня автоматизації, наявності API, зручності використання, точності та надійності результатів, швидкості отримання інформації, доступності, можливості експорту даних та інтеграції з іншими системами. Для кожного критерію використовується п’ятирівнева шкала оцінювання, а підсумковий показник визначається методом зваженої суми з урахуванням індивідуальних пріоритетів користувача. На основі запропонованого підходу реалізовано прототип системи, що забезпечує введення завдання, налаштування ваг критеріїв, фільтрацію бази знань, розрахунок інтегральних оцінок і формування рейтингу рекомендованих OSINT-інструментів. Запропонований підхід може використовуватися як основа для подальшого розвитку систем автоматизованої підтримки OSINT-аналітики, зокрема шляхом інтеграції актуальних даних про інструменти, API зовнішніх сервісів та більш складних методів багатокритеріального оцінювання.

Ключові слова: OSINT; інформаційна безпека; кібербезпека; OSINT-інструменти; багатокритеріальне оцінювання; ранжування; кіберрозвідка.

© І.Л. Лозова, М.В. Різак, О.М. Лепеха, 2026

ВСТУП

Сучасне інформаційне середовище характеризується стрімким зростанням обсягів даних, доступних із відкритих джерел. Вебресурси, соціальні мережі, публічні бази даних, реєстри, архіви вебсторінок, мережеві сервіси та інші інформаційні ресурси формують значний масив відомостей, який може бути використаний для вирішення завдань інформаційної та кібербезпеки. Саме систематичне отримання, оброблення, перевірка та аналіз таких даних становить основу OSINT-підходу.

OSINT активно застосовується для моніторингу інформаційного простору, аналізу кіберзагроз, дослідження цифрової інфраструктури, виявлення витоків інформації, цифрових розслідувань, оцінювання зовнішньої поверхні атаки та формування кіберрозвідувальної інформації. Огляд сучасного стану OSINT у кібербезпеці показує розширення кількості доступних інструментів та методів, а також активне використання засобів штучного інтелекту для автоматизації збору й аналізу відкритих даних [1].

Одночасно збільшення кількості OSINT-засобів створює нову прикладну проблему – вибір інструмента, який найбільшою мірою відповідає конкретному завданню інформаційної безпеки. Інструменти відрізняються не лише джерелами інформації, а й функціональним призначенням, рівнем автоматизації, точністю, швидкістю, доступністю, умовами використання, можливістю інтеграції та формами представлення результатів. Дослідження сучасних OSINT-інструментів також демонструють відсутність універсального засобу, здатного забезпечити виконання всіх типів розвідувальних завдань, що обумовлює необхідність комбінованого використання різних рішень.

Слід зазначити, що проблема вибору OSINT-засобів є предметом дослідження в сучасній науковій літературі. Зокрема, в [2] запропоновано категоризацію пошукових OSINT-інструментів за типом програмної реалізації та здійснено їх оцінювання з урахуванням функціональності, ефективності й обмежень. Інші дослідники здійснювали класифікацію OSINT-інструментів за інформаційними доменами та співвідносили їх із етапами Cyber Kill Chain [3]. Окремий напрям досліджень становить інтеграція різних OSINT-засобів для отримання та збагачення інформації про інформаційні системи [4].

Отже, науковий інтерес становить не лише класифікація наявних OSINT-інструментів, а й формалізація процесу їх вибору відповідно до конкретного завдання інформаційної безпеки.

Метою статті є розроблення методологічного підходу до вибору OSINT-інструментів на основі формалізованої системи критеріїв, первинного відбору та багатокритеріального ранжування.

OSINT є міждисциплінарним напрямом, що охоплює технології пошуку, збору, оброблення, аналізу, кореляції та верифікації інформації з відкритих джерел. У сфері кібербезпеки OSINT застосовується як для реактивних, так і для проактивних завдань.

У роботі [1] систематизовано сучасний стан OSINT у кібербезпеці та розглянуто його використання для аналізу соціальних мереж, цифрової криміналістики, кіберзлочинності та інших напрямів. Автори також акцентують увагу на перспективності застосування машинного та глибокого навчання для оброблення великих масивів відкритих даних.

В роботі [2] OSINT розглядається насамперед з позиції інструментів пошуку. Автор виділяє три основні категорії програмних засобів: інструменти, інтегровані з операційною системою або браузером; автономні програмні засоби; репозиторії посилань на спеціалізовані інструменти. Для засобів кожної категорії здійснено критичне оцінювання функціональності, ефективності та обмежень.

В [3] запропоновано класифікувати OSINT-інструменти за інформаційними доменами, з яких здійснюється отримання даних, та співвіднести їх використання з Cyber Kill Chain. Такий підхід демонструє доцільність розгляду OSINT-засобів не ізольовано, а в контексті конкретних завдань кібербезпеки.

В [4] досліджено можливість інтеграції різних OSINT-інструментів для збору інформації про IT-інфраструктуру організацій. Запропонований підхід передбачає послідовне збагачення інформації результатами роботи різних засобів, що дозволяє отримувати більш повну картину досліджуваного об’єкта.

Важливим є також напрям автоматизованого формування кіберрозвідувальної інформації. В [5] запропоновано платформу AECCP, яка використовує OSINT для збагачення інформації про кіберзагрози, її класифікації та кореляції. Результати дослідження демонструють потенціал автоматизації операцій із відкритими даними в процесах Threat Intelligence.

Окрему увагу сучасні дослідження приділяють використанню штучного інтелекту в OSINT. В [6] здійснено систематичний огляд 163 досліджень, присвячених поєднанню AI та OSINT, і показано, що автоматизація може зменшувати навантаження на аналітиків під час роботи з великими обсягами інформації.

Найближчим до проблематики вибору є дослідження [7], де автори здійснили порівняльний аналіз понад 150 OSINT-інструментів, сервісів та баз даних і показали суттєву різноманітність їх

функціональності, ліцензійних моделей та доступності. Одним із ключових висновків є відсутність універсального рішення, здатного задовольнити всі інформаційні потреби.

Питання застосування та систематизації OSINT-інструментів активно розробляється й у вітчизняній науковій літературі. Так, у роботі [8] досліджено наявні засоби та підходи до проведення OSINT-діяльності в контексті інформаційної безпеки особи та держави, що підкреслює безпекову значущість цього напряму для національного контексту. Узагальнені відомості про категорії та практичне застосування OSINT-інструментів систематизовано в навчальних виданнях [9; 10], положення яких використано при формуванні переліку функціональних категорій інструментів у цьому дослідженні. Окремої уваги заслуговує зростання ролі OSINT в умовах збройного конфлікту: у роботі [11] проаналізовано застосування методів OSINT у кібербезпеці під час воєнних дій, що додатково підтверджує актуальність оперативного й обґрунтованого вибору інструментів. Практичні аспекти застосування OSINT для цифрових розслідувань кіберінцидентів розглянуто в [12]. Водночас дослідження [13] звертає увагу на подвійну природу OSINT-технологій, які можуть використовуватися не лише для захисту, а й як інструмент деанонімізації особи, що актуалізує питання етичного та зваженого застосування таких засобів. Попередні результати щодо побудови системи підтримки вибору OSINT-інструментів було представлено на науково-практичній конференції [14]; цю статтю присвячено подальшому розвитку та формалізації запропонованого підходу.

Аналіз наведених досліджень дозволяє визначити наукову проблему: наявні роботи значною мірою зосереджені на класифікації, порівнянні або практичному застосуванні OSINT-інструментів, тоді як задача формалізованого вибору конкретного інструмента відповідно до характеристик завдання та індивідуальних пріоритетів користувача потребує подальшого розвитку. Саме цю проблему покладено в основу запропонованого методологічного підходу.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Проведений аналіз дозволив виділити основні напрями, в яких OSINT може використовуватися для забезпечення інформаційної безпеки.

Першим напрямом є моніторинг витоків інформації. Відкриті джерела можуть містити відомості про скомпрометовані облікові записи, документи, технічну інформацію та інші дані, які були оприлюднені внаслідок витоку. Для таких завдань використовуються спеціалізовані сервіси перевірки компрометації та пошуку витоків.

Другий напрям – виявлення фішингових та шкідливих ресурсів. OSINT дозволяє досліджувати доменні імена, IP-адреси, DNS-записи, сертифікати та інші характеристики зовнішньої інфраструктури. Такий аналіз може бути використаний для виявлення доменів, що імітують легітимні ресурси.

Третій напрям – оцінювання зовнішньої поверхні атаки (Attack Surface). У цьому випадку завданням є визначення доступних з Інтернету цифрових активів організації: доменів, піддоменів, IP-адрес, мережевих сервісів та інших компонентів інфраструктури.

Четвертий напрям – SOCMINT, тобто аналіз відкритої інформації соціальних мереж і месенджерів. Він може застосовуватися для дослідження цифрової присутності об’єктів, виявлення зв’язків між акаунтами, моніторингу інформаційних кампаній та аналізу публічної активності.

П’ятий напрям – GEOINT та геопросторовий аналіз, що передбачає використання картографічних і супутникових даних для встановлення або перевірки просторового контексту подій.

Шостий напрям – аналіз метаданих та мультимедійного контенту. Інформація про час створення файлу, пристрій, координати та інші параметри може використовуватися для перевірки походження цифрових матеріалів.

Сьомий напрям – візуалізація та кореляція інформації. Для цього використовуються засоби побудови графів і встановлення взаємозв’язків між доменами, IP-адресами, акаунтами, організаціями та іншими об’єктами.

Отже, OSINT-інструменти характеризуються вираженою функціональною спеціалізацією. Це підтверджує необхідність їх вибору не за принципом «найкращий інструмент загалом», а відповідно до конкретного завдання, вимог до результату та умов застосування.

Запропонований підхід розглядає вибір OSINT-інструмента як послідовність чотирьох основних етапів:

1) визначення завдання інформаційної безпеки;
2) первинна фільтрація інструментів за функціональною відповідністю;
3) багатокритеріальне оцінювання відібраних інструментів;
4) формування рейтингу та рекомендацій.

Такий підхід дає змогу поєднати переваги класифікації OSINT-засобів із формалізованим механізмом прийняття рішення.

Нехай:

- $Z = \{z_1, z_2, ...z_m\}$ – множина можливих завдань інформаційної безпеки;
- $T = \{t_1, t_2, ...t_k\}$ – множина доступних OSINT-інструментів;
- $t \in T$ – окремий OSINT-інструмент;
- $z \in Z$ – завдання інформаційної безпеки;
- $C = \{c_1, c_2, ...c_n\}$ – множина критеріїв оцінювання;
- w_i – ваговий коефіцієнт відповідного критерію;
- $s_i(t)$ – оцінка інструмента t за i-м критерієм.

Для забезпечення коректного використання вагових коефіцієнтів їх сума повинна задовольняти умову:

$$\sum_{i=1}^{n} w_i = 1, w_i \geq 0.$$

На першому етапі формується множина інструментів, функціональні можливості яких відповідають заданому завданню інформаційної безпеки:

$$T_z = \{t \in T \mid z \in Tasks(t)\},$$

де $Tasks(t)$ — множина завдань, які підтримує інструмент t.

Таким чином, до етапу багатокритеріального оцінювання допускаються лише ті OSINT-засоби, функціональні можливості яких відповідають визначеному завданню. Саме така логіка первинної фільтрації реалізується у прототипі запропонованої системи.

Для багатокритеріального оцінювання запропоновано використовувати вісім критеріїв:

Таблиця 1

Перелік критеріїв оцінювання OSINT-засобів та їх характеристика

Позначення	Критерій	Характеристика
c_1	автоматизація	здатність автоматично виконувати операції збору та аналізу
c_2	API	можливість програмної інтеграції
c_3	зручність	простота використання та доступність документації
c_4	точність	достовірність та надійність отриманих результатів
c_5	швидкість	час отримання результату
c_6	доступність	вартість та обмеження доступу
c_7	експорт	можливість збереження та подальшого використання результатів
c_8	інтеграція	сумісність з іншими системами та платформами

Визначений перелік критеріїв сформовано з урахуванням технічних та організаційних аспектів використання OSINT-засобів. Зазначені характеристики розглядаються як основа для формалізованого порівняння та персоналізації процесу вибору інструмента.

Застосування вагових коефіцієнтів є принциповим, оскільки значущість окремих критеріїв залежить від характеру конкретного завдання інформаційної безпеки. Наприклад, під час оперативного аналізу інциденту більшу вагу можуть мати критерії швидкості та автоматизації, тоді як для цифрового розслідування пріоритетними можуть бути точність, можливість експорту та зручність подальшого аналізу результатів.

Для уніфікації оцінювання використовується п’ятирівнева шкала:

Таблиця 2

Шкала оцінювання

Оцінка	Рівень характеристики
1	дуже низький
2	низький
3	середній
4	високий
5	дуже високий

Отже, $s_i(t) \in \{1,2,3,4,5\}$.

Така шкала дає змогу представити якісні характеристики OSINT-інструментів у числовій формі та використати їх для подальшого багатокритеріального оцінювання.

Для формування рейтингу OSINT-інструментів застосовується метод зваженої суми. Інтегральний показник придатності інструмента визначається як:

$$Score(t) = \sum_{i=1}^{n} w_i s_i(t),$$

де: $s_i(t)$ – оцінка інструмента t за i-м критерієм, w_i – ваговий коефіцієнт i-го критерію, n – загальна кількість критеріїв.

За умови $\sum_{i=1}^{n} w_i = 1$ та $s_i(t) \in [1,5]$, інтегральний показник також належить інтервалу $1 \le Score(t) \le 5$.

Чим більше значення $Score(t)$, тим вищою є інтегральна оцінка придатності OSINT-інструмента для заданого завдання. Для формування рейтингу відібраних інструментів використовується впорядкування множини T_z за спаданням значення інтегрального показника:

$$Score(t_{(1)}) \ge Score(t_{(2)}) \ge ... \ge Score(t_{(r)}),$$

де $t_{(j)}$ — j-й інструмент у сформованому рейтингу, а $r = |T_z|$ — кількість інструментів, що пройшли первинну фільтрацію.

Перевагою запропонованого підходу є можливість адаптувати рейтинг до конкретного сценарію застосування. Зміна вагових коефіцієнтів не потребує зміни характеристик інструментів у базі знань, а впливає лише на значення їх інтегральної оцінки та, відповідно, на порядок ранжування. Таким чином, один і той самий набір OSINT-інструментів може отримувати різні рейтинги для різних завдань інформаційної безпеки. Такий підхід відповідає принципу контекстної придатності OSINT-засобів: інструмент не є універсально оптимальним, а його доцільність визначається відповідністю функціональних можливостей вимогам конкретного завдання.

Функціонування запропонованого підходу передбачає наявність структурованої бази знань. Вона є інформаційною основою процедури вибору та повинна забезпечувати однорідне представлення характеристик різних інструментів. Для кожного інструмента доцільно зберігати:

- назву;
- функціональну категорію;
- опис призначення;
- перелік підтримуваних завдань;
- оцінки за визначеними критеріями (автоматизація, наявність API, точність, швидкість тощо).

Функціонально до бази знань було включено інструменти таких категорій:

- оцінювання Attack Surface;
- аналіз загроз;
- моніторинг витоків;
- автоматизація OSINT;
- візуалізація та кореляція;
- аналіз доменів і DNS;
- аналіз метаданих та медіа;
- SOCMINT;

– GEOINT.

Серед прикладів розглянутих інструментів – Shodan, Censys, BuiltWith, VirusTotal, Have I Been Pwned, IntelX, SpiderFoot, Recon-ng, Maltego, WHOIS Lookup, SecurityTrails, ExifTool, FotoForensics, Google Maps, Google Earth та Sentinel Hub.

Важливою характеристикою бази знань OSINT-інструментів є її масштабованість та здатність до актуалізації. Динамічний розвиток OSINT-середовища супроводжується появою нових сервісів і змінюванням функціональних можливостей наявних засобів, їх API, моделей тарифікації та політик доступу. За таких умов статичне представлення характеристик інструментів поступово втрачає актуальність, що може негативно впливати на достовірність результатів їх порівняння та вибору. Тому функціонування бази знань доцільно реалізовувати з урахуванням механізмів регулярного оновлення та актуалізації інформації про OSINT-інструменти.

Для практичної перевірки запропонованого методологічного підходу реалізовано прототип системи підтримки прийняття рішень у формі вебзастосунку, що забезпечує послідовне виконання процедур введення параметрів завдання, вибору та фільтрації OSINT-інструментів, їх багатокритеріального оцінювання, ранжування та формування рекомендацій. Функціональну структуру прототипу сформовано з таких основних компонентів:

1) модуль введення параметрів;
2) база знань OSINT-інструментів;
3) модуль функціональної фільтрації;
4) модуль багатокритеріального оцінювання;
5) модуль ранжування;
6) модуль формування рекомендацій.

Процес роботи системи починається з вибору користувачем завдання інформаційної безпеки. Після цього визначаються ваги критеріїв. Система звертається до бази знань і відбирає інструменти, які підтримують заданий тип завдання. Для відібраних засобів розраховується інтегральний показник, після чого формується впорядкований список рекомендацій.

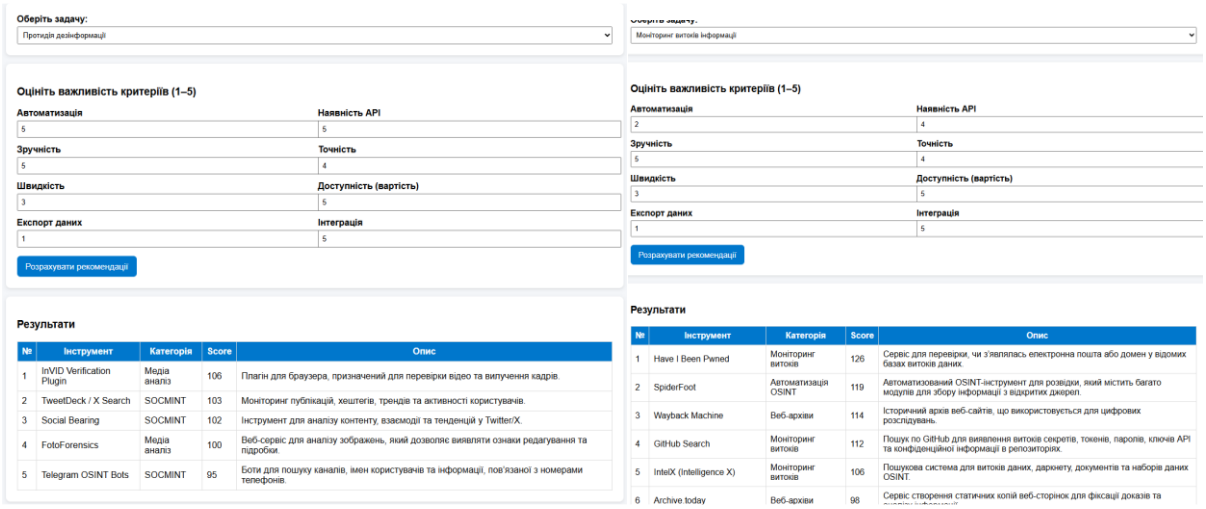
Запропонована архітектура відповідає принципу модульності, оскільки база знань, алгоритм оцінювання та користувацький інтерфейс функціонують як окремі компоненти. Це спрощує подальше розширення системи.

Для перевірки запропонованого методологічного підходу проведено функціональне тестування реалізованого прототипу системи підтримки прийняття рішень на типових завданнях інформаційної безпеки. Метою тестування було перевірити коректність виконання основних етапів запропонованої процедури вибору OSINT-інструментів та оцінити здатність системи адаптувати сформований рейтинг до зміни контексту завдання і пріоритетів користувача.

Перший сценарій передбачав вирішення завдання протидії дезінформації. Користувач визначав відповідний тип завдання та задавав вагові коефіцієнти критеріїв оцінювання, після чого система здійснювала фільтрацію доступних OSINT-інструментів, розраховувала їх інтегральні показники та формувала впорядкований рейтинг.

Другий сценарій стосувався моніторингу витоків даних. Після зміни типу завдання та параметрів оцінювання система виконувала повторний розрахунок інтегральних показників і формувала новий рейтинг. Отримані результати продемонстрували, що порядок ранжування залежить не лише від складу доступних OSINT-інструментів, а й від специфіки поставленого завдання та встановлених користувачем пріоритетів критеріїв.

Третій сценарій передбачав виконання завдання SOCMINT, у межах якого перевірялася коректність первинної фільтрації інструментів за функціональною відповідністю роботі з інформацією із соціальних мереж та подальшого ранжування відібраних засобів відповідно до визначених критеріїв.



а) протидія дезінформації б) моніторинг витоків даних

в) SOCMINT

Рис. 1. Результати функціонального тестування прототипу на трьох сценаріях вибору OSINT-інструментів

За результатами функціонального тестування підтверджено коректність реалізації основних операцій системи: оброблення параметрів, введених користувачем; фільтрації OSINT-інструментів відповідно до обраного завдання; розрахунку інтегрального показника; сортування інструментів за його значенням; формування та відображення рейтингу рекомендованих засобів.

Таким чином, проведене тестування підтвердило функціональну працездатність прототипу та продемонструвало можливість практичного використання запропонованого підходу для формалізації процесу вибору OSINT-інструментів. Зокрема, встановлено, що зміна контексту завдання та вагових коефіцієнтів призводить до відповідної зміни результатів ранжування, що забезпечує персоналізацію рекомендацій.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

У дослідженні запропоновано методологічний підхід до формалізації процесу вибору OSINT-інструментів для виконання завдань інформаційної безпеки. Запропонований підхід поєднує первинну фільтрацію засобів за функціональною відповідністю визначеному завданню з подальшим багатокритеріальним оцінюванням та ранжуванням. Для оцінювання сформовано систему з восьми критеріїв: рівень автоматизації, наявність API, зручність використання, точність, швидкість, доступність, можливість експорту та інтеграція. Для їх урахування використано п’ятирівневу шкалу та метод зваженої суми, що забезпечує адаптацію результатів вибору до специфіки завдання та пріоритетів користувача.

На основі запропонованого підходу реалізовано прототип системи підтримки прийняття рішень у формі вебзастосунку. Система забезпечує введення параметрів завдання, роботу зі структурованою базою знань OSINT-інструментів, функціональну фільтрацію, розрахунок інтегральних показників, формування рейтингу та рекомендацій. Функціональне тестування на сценаріях протидії дезінформації, моніторингу витоків інформації та SOCMINT підтвердило коректність реалізації зазначених процедур та продемонструвало залежність результатів ранжування від контексту завдання і встановлених ваг критеріїв.

Практичне значення отриманих результатів полягає у можливості використання запропонованого підходу як засобу підтримки діяльності аналітика інформаційної безпеки під час вибору OSINT-інструментарію. На відміну від ручного або частково автоматизованого вибору, запропонована система формалізує процедуру прийняття рішення та забезпечує її адаптацію до конкретного сценарію застосування. Водночас система не призначена для повної заміни експерта: якість відкритих даних може залежати від їх повноти, актуальності та достовірності, тому остаточна оцінка доцільності використання конкретного інструмента має здійснюватися фахівцем.

Основними обмеженнями проведеного дослідження є використання обмеженої бази інструментів та характеристик, що потребують регулярного актуалізування, а також відсутність масштабного статистичного порівняння сформованих рекомендацій із незалежними експертними рішеннями на репрезентативній множині завдань. Тому результати експерименту підтверджують функціональну працездатність та контекстну адаптивність запропонованого механізму, однак не дають підстав робити висновок про його універсальну перевагу над експертним вибором.

Перспективи подальших досліджень пов’язані з автоматизованим оновленням бази знань на основі API та відкритих каталогів, інтеграцією системи з платформами Threat Intelligence, застосуванням методів нечіткого та інших багатокритеріальних підходів, а також використанням машинного навчання для адаптивного визначення ваг критеріїв і формування рекомендацій. Окремим напрямом є проведення масштабного експериментального дослідження із залученням реальних сценаріїв інформаційної безпеки та порівняння результатів роботи системи з рішеннями експертів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Yadav, A., Kumar, A., & Singh, V. (2023). Open-source intelligence: A comprehensive review of the current state, applications and future perspectives in cyber security. Artificial Intelligence Review, 56, 12407–12438. https://doi.org/10.1007/s10462-023-10454-y
2. Mider, D. (2024). Open source intelligence on the internet – categorisation and evaluation of search tools. Internal Security Review, (31), 383–412. https://doi.org/10.4467/20801335PBW.24.030.20807
3. Yamin, M. M., Ullah, M., Ullah, H., Katt, B., Hijji, M., & Muhammad, K. (2022). Mapping tools for open source intelligence with cyber kill chain for adversarial aware security. Mathematics, 10(12), Article 2054. https://doi.org/10.3390/math10122054
4. Stodelov, D., & Miloslavskaya, N. (2022). Open source INTelligence tools. Procedia Computer Science, 213, 83–88. https://doi.org/10.1016/j.procs.2022.11.041
5. Martins, C., & Medeiros, I. (2022). Generating quality threat intelligence leveraging OSINT and a cyber threat unified taxonomy. ACM Transactions on Privacy and Security, 25(3), Article 19, 1–39. https://doi.org/10.1145/3530977
6. Browne, T. O., Abedin, M., & Chowdhury, M. J. M. (2024). A systematic review on research utilising artificial intelligence for open source intelligence (OSINT) applications. International Journal of Information Security, 23, 2911–2938. https://doi.org/10.1007/s10207-024-00868-2
7. Lazarov, W., Moravec, V., Loutocký, P., Vostoupal, J., & Martinásek, Z. (2026). Comparative analysis of OSINT tools, techniques, and legal aspects. Computers & Security, 168, Article 104938. https://doi.org/10.1016/j.cose.2026.104938
8. Івкова, В. С., & Опірський, І. Р. (2025). Дослідження існуючих засобів та підходів до проведення OSINT в контексті інформаційної безпеки особи та держави. Cybersecurity: Education, Science, Technique, 3(27), 165–179. https://doi.org/10.28925/2663-4023.2025.27.749
9. Користін, О., Демедюк, С., Ісмайлов, К., Ланде, Д., та ін. (2025). OSINT Open Source Intelligence. Інструменти та методи: навчальний посібник. 7БЦ. https://doi.org/10.32782/osint-instruments-2025
10. Ланде, Д. В. (2024). OSINT у кібербезпеці: навчальний посібник. ТОВ «Інжиніринг».
11. Мірошніченко, І. О., & Ланде, Д. В. (2024). Роль методів OSINT в кібербезпеці та їх застосування під час воєнних конфліктів. У Теоретичні і прикладні проблеми фізики, математики та

інформатики: матеріали XXII Всеукраїнської науково-практичної конференції студентів, аспірантів та молодих вчених (с. 282–284). КПІ ім. Ігоря Сікорського. https://ela.kpi.ua/handle/123456789/69980

12. Полотай, О., & Балацька, В. (2026). Використання OSINT у цифрових розслідуваннях кіберінцидентів. У Modern scientific inventions: Current problems, theories and challenges: матеріали XIV Міжнар. наук.-практ. конф. (с. 184–187). https://sci.ldubgd.edu.ua/jspui/handle/123456789/17638
13. Главацька, А., Ангельська, О., & Опірський, І. (2024). Дослідження технології використання OSINT як нової загрози з деанонімізації особи в інтернет-просторі. Cybersecurity: Education, Science, Technique, 1(25), 19–50. https://doi.org/10.28925/2663-4023.2024.25.1950
14. Лозова, І. Л., & Клопова, А. А. (2026). Система підтримки вибору OSINT-інструментів для вирішення завдань інформаційної безпеки. У Стратегії кіберстійкості: управління ризиками та безперервність бізнесу: матеріали Всеукр. наук.-практ. конф. (с. 100–103).

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (34), 2026
ISSN 2663 – 4023

Iryna Lozova
Candidate of Technical Sciences
Associate Professor, Department of Cybersecurity and Information Protection Management
State University of Information and Communication Technologies, Kyiv, Ukraine
ORCID: 0000-0002-7224-4763
illozovaya@gmail.com

Mykhailo Rizak
Doctor of Sciences in Law, Senior Researcher
Professor, Department of Technical Cybersecurity Systems
State University of Information and Communication Technologies, Kyiv, Ukraine
ORCID: 0009-0003-9844-3271
advokat.rizak@gmail.com

Oleh Lepekha
Candidate of Sciences in Law
Doctoral Student
State University of Information and Communication Technologies, Kyiv, Ukraine
ORCID: 0000-0003-1308-3469
olm3000@gmail.com

A METHODOLOGICAL APPROACH TO THE SELECTION OF OSINT TOOLS FOR INFORMATION SECURITY TASKS

Abstract. This paper proposes a methodological approach to selecting Open Source Intelligence (OSINT) tools for addressing information security tasks. The relevance of the study is determined by the large number of modern OSINT tools, their functional specialization, differences in the level of automation, availability, accuracy, integration capabilities, and the nature of the information sources they utilize. These factors complicate the informed selection of an appropriate tool for a specific task and increase the dependence of the results on the analyst's experience. Based on an analysis of contemporary approaches to OSINT application, the main categories of tools are systematized, including tools for external attack surface assessment, information leak monitoring, domain and network infrastructure analysis, SOCMINT, GEOINT, metadata analysis, data visualization, and data correlation. The selection process is proposed to be formalized as a multi-criteria procedure consisting of the initial filtering of tools according to their relevance to a specific information security task, followed by their ranking based on an integral score. The proposed evaluation criteria include the level of automation, API availability, ease of use, accuracy and reliability of results, information retrieval speed, accessibility, data export capabilities, and integration with other systems. Each criterion is evaluated using a five-level scale, while the overall score is calculated using the weighted sum method, taking into account the individual priorities of the user. Based on the proposed approach, a prototype system was developed to support the input of a task, configuration of criterion weights, filtering of the knowledge base, calculation of integral scores, and generation of a ranking of recommended OSINT tools. The proposed approach can serve as a basis for further development of automated OSINT analytics support systems, particularly through the integration of up-to-date tool data, external service APIs, and more advanced multi-criteria evaluation methods.

Keywords: OSINT; information security; cybersecurity; OSINT tools; multi-criteria evaluation; ranking; cyber intelligence.

REFERENCES

1. Yadav, A., Kumar, A., & Singh, V. (2023). Open-source intelligence: A comprehensive review of the current state, applications and future perspectives in cyber security. Artificial Intelligence Review, 56, 12407–12438. https://doi.org/10.1007/s10462-023-10454-y
2. Mider, D. (2024). Open source intelligence on the internet – categorisation and evaluation of search tools. Internal Security Review, (31), 383–412. https://doi.org/10.4467/20801335PBW.24.030.20807

3. Yamin, M. M., Ullah, M., Ullah, H., Katt, B., Hijji, M., & Muhammad, K. (2022). Mapping tools for open source intelligence with cyber kill chain for adversarial aware security. Mathematics, 10(12), Article 2054. https://doi.org/10.3390/math10122054
4. Stodelov, D., & Miloslavskaya, N. (2022). Open source INTelligence tools. Procedia Computer Science, 213, 83–88. https://doi.org/10.1016/j.procs.2022.11.041
5. Martins, C., & Medeiros, I. (2022). Generating quality threat intelligence leveraging OSINT and a cyber threat unified taxonomy. ACM Transactions on Privacy and Security, 25(3), Article 19, 1–39. https://doi.org/10.1145/3530977
6. Browne, T. O., Abedin, M., & Chowdhury, M. J. M. (2024). A systematic review on research utilising artificial intelligence for open source intelligence (OSINT) applications. International Journal of Information Security, 23, 2911–2938. https://doi.org/10.1007/s10207-024-00868-2
7. Lazarov, W., Moravec, V., Loutocký, P., Vostoupal, J., & Martinásek, Z. (2026). Comparative analysis of OSINT tools, techniques, and legal aspects. Computers & Security, 168, Article 104938. https://doi.org/10.1016/j.cose.2026.104938
8. Ivkova, V. S., & Opirskyi, I. R. (2025). Doslidzhennia isnuiuchykh zasobiv ta pidkhodiv do provedennia OSINT v konteksti informatsiinoi bezpeky osoby ta derzhavy [Study of existing tools and approaches to conducting OSINT in the context of information security of an individual and the state]. Cybersecurity: Education, Science, Technique, 3(27), 165–179. https://doi.org/10.28925/2663-4023.2025.27.749 [in Ukrainian].
9. Korystin, O., Demediuk, S., Ismailov, K., Lande, D., et al. (Eds.). (2025). OSINT Open Source Intelligence. Instrumenty ta metody [OSINT Open Source Intelligence. Tools and methods] [Study guide]. 7BTs. https://doi.org/10.32782/osint-instruments-2025 [in Ukrainian].
10. Lande, D. V. (2024). OSINT u kiberbezpetsi [OSINT in cybersecurity] [Study guide]. TOV Inzhynirynh. [in Ukrainian].
11. Miroshnichenko, I. O., & Lande, D. V. (2024). Rol metodiv OSINT v kiberbezpetsi ta yikh zastosuvannia pid chas voiennykh konfliktiv [The role of OSINT methods in cybersecurity and their application during military conflicts]. In Teoretychni i prykladni problemy fizyky, matematyky ta informatyky: Proceedings of the XXII All-Ukrainian Scientific and Practical Conference of Students, Postgraduates and Young Scientists (pp. 282–284). Igor Sikorsky Kyiv Polytechnic Institute. https://ela.kpi.ua/handle/123456789/69980 [in Ukrainian].
12. Polotai, O., & Balatska, V. (2026). Vykorystannia OSINT u tsyfrovykh rozsliduvanniakh kiberintsydentiv [Using OSINT in digital investigations of cyber incidents]. In Modern scientific inventions: current problems, theories and challenges: Proceedings of the XIV International Scientific and Practical Conference (pp. 184–187). https://sci.ldubgd.edu.ua/jspui/handle/123456789/17638 [in Ukrainian].
13. Hlavatska, A., Anhelska, O., & Opirskyi, I. (2024). Doslidzhennia tekhnolohii vykorystannia OSINT yak novoi zahrozy z deanonimizatsii osoby v internet-prostori [A study of OSINT technology as a new threat of personal deanonymization in the internet space]. Cybersecurity: Education, Science, Technique, 1(25), 19–50. https://doi.org/10.28925/2663-4023.2024.25.1950 [in Ukrainian].
14. Lozova, I. L., & Klopova, A. A. (2026). Systema pidtrymky vyboru OSINT-instrumentiv dlia vyrishennia zavdan informatsiinoi bezpeky [A decision support system for selecting OSINT tools to solve information security tasks]. In Stratehii kiberstiikosti: upravlinnia ryzykamy ta bezperervnist biznesu: Proceedings of the All-Ukrainian Scientific and Practical Conference (pp. 100–103). Kyiv. [in Ukrainian].

Отримано редакцією журналу / Received: 09.03.26
Прорецензовано / Revised: .25.03.26
Схвалено до друку / Accepted: 24.09.26

(cc) BY-NC-SA

This work is licensed under Creative Commons Attribution-noncommercial-sharealike 4.0 International License.