

**Муравська Ю. Є.**  
*к.е.н., доцент, завідувач кафедри безпеки  
та правоохоронної діяльності,  
Західноукраїнський національний університет*

## **OSINT-ТЕХНОЛОГІЇ В СИСТЕМІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ**

Сучасні безпекові виклики, що постали перед Україною в умовах збройної агресії російської федерації, гібридних загроз, інформаційно-психологічних операцій та кібернетичного протиборства, зумовили необхідність суттєвого оновлення та переосмислення підходів до збору, аналізу й використання інформації у цілях національної безпеки. Однією з ключових тенденцій останнього десятиліття стало стрімке зростання значення OSINT-розвідки на основі відкритих джерел. Доступність цифрових технологій, масовість використання соціальних мереж, розвиток супутникової зйомки, відкритих реєстрів та інструментів аналітики зробили OSINT незамінним інструментом як для державних органів сектору безпеки й оборони, так і для правоохоронних структур, аналітичних центрів, журналістів-розслідувачів. У цьому контексті дослідження OSINT-технологій у системі національної безпеки України набуває не лише наукової, але й практичної актуальності.

Для України важливість OSINT підсилюється тим, що саме відкриті джерела часто дозволяють отримати оперативну, релевантну та незалежну інформацію про дії противника, порушення міжнародного права, військову активність, переміщення техніки, кіберзагрози та інформаційні операції. Це робить OSINT одним із ключових інструментів, які забезпечують ситуаційну обізнаність, стратегічне планування, інформаційну протидію та документування злочинів проти України. Актуальність дослідження розвідки з відкритих джерел пояснюється необхідністю проведення комплексного аналізу ролі та можливостей OSINT у сучасній системі національної безпеки України з акцентом на спеціалізованих технологічних інструментах, особливостях їх застосування та перспектив інтеграції у діяльність правоохоронних органів у сфері безпеки та оборони, а також на практичних механізмах використання відкритих джерел для протидії інформаційним, кібернетичним і військовим загрозам. Додаткову цінність становить узагальнення сучасного міжнародного досвіду у сфері OSINT та окреслення рекомендацій щодо його імплементації в український контекст з урахуванням специфіки умов війни.

Проблематика відкритих джерел інформації та їх використання у сфері національної безпеки представлена у працях українських та зарубіжних дослідників. Серед українських авторів слід виділити роботи Б. Віннічука, В. Стрелкова [4], С. Бочарова, В. Тищука, О. Біляя [1], які аналізували особливості OSINT-розвідки в забезпеченні національної безпеки. Питанням забезпечення національної безпеки України, інформаційній безпеці та протидії промислового шпигунству присвячені попередні праці авторки [2; 3; 7; 9]. Дослідження М. Тома, О. Василюва [5] присвячені використанню аналітики даних і цифрових інструментів для фіксації воєнних злочинів в Україні. У міжнародній науковій думці важливими є напрацювання А. Марлеку [8], Т. Коллеу [6], які систематизують методологію OSINT, окреслюють модель

«цифрової розвідки» та підходи НАТО, ЄС і США до роботи з відкритою інформацією.

Попри значний обсяг наукового доробку, комплексне дослідження OSINT-технологій саме у контексті національної безпеки України в умовах сучасної війни висвітлене недостатньо. Це обумовлює потребу у подальшому системному науковому аналізі даного питання.

Якщо звернутися до положень стандартів НАТО, можна чітко прослідкувати акцент на необхідності дотримуватися відповідного алгоритму, так званого розвідувального циклу, в процесі здійснення пошуково-розвідувальної роботи, а саме [6]:

1) постановка завдання – визначення чітких завдань, що лежать в основі OSINT-дослідження. Для прикладу, це може бути дослідження фізичної або юридичної особи на основі її зав'язків, оточення, контактів тощо);

2) збір інформації, що включає в себе методологію збору даних на основі переліку ключових запитів, здійснення процесу глобального пошуку інформації, та, в результаті, цілеспрямованого відбору інформації, що відповідає критеріям запити;

3) технічна обробка інформації – оцінка відповідності всієї зібраної інформації поставленій мені здійснення розвідки з подальшим її сортуванням відповідно до встановлених критеріїв (наприклад, час, місце, об'єкт, суб'єкт тощо);

4) обробка даних – зіставлення отриманої інформації з іншими результатами OSINT-даних, що може підтвердити чи спростувати висунуті гіпотези;

5) передача даних замовнику – включає формування заключного звіту OSINT-розвідки (переважно такий документ містить відповідні застереження щодо заборони його поширення та передачі третім особам).

Таким чином, вивчення OSINT-технологій у системі національної безпеки України є важливим напрямом сучасних наукових досліджень, що відповідає актуальним потребам держави в умовах воєнної та гібридної агресії. Збір та синтез відкритих даних є вагомим складовою протидії сучасним викликам і загрозам національній безпеці України, що особливо актуально в сучасних умовах воєнного стану, і саме завдяки інструментам OSINT-розвідки представники правоохоронних органів виявляють місцезнаходження військових формувань і техніки країни-агресора, ідентифікують особисті дані воєнних злочинців, а також збирають необхідну доказову базу, проводять психологічно-інформаційний вплив на ворога, розкривають колаборантів, відкривають напрямки ворожої пропаганди тощо.

#### **ЛІТЕРАТУРА:**

1. Бочаров С., Тищук В., Біляй О. Застосування OSINT в оперативно-слідчій діяльності: можливості та обмеження. // Суспільні та правничі студії. 2025.

URL: <https://sts.nangu.edu.ua/article/download/336692/325308> (дата звернення: 10.04.2026 р.)

2. Вівчар О. І., Муравська Ю. Є., Гевко В. Л. Практичні контексти національної безпеки на умовах партнерства: позитивні екстерналії та ефективність забезпечення. Вісник Хмельницького національного університету.

Серія: економічні науки. – 2022. №1 С. 7-11. ISSN 2307-5740

URL:<http://journals.khnu.km.ua/vestnik/?p=11668>

а. З. Волощук В., Заєць К., Муравська Ю. Національна безпека як інструмент збереження Української державності. Актуальні проблеми правознавства. 2024. Випуск. 2. С. 111-118.

4. Віннічук Б. В., Стрелков В. В. Роль OSINT-розвідки в забезпеченні національної безпеки. // Міжнародна та національна безпека: теоретичні і прикладні аспекти : матеріали VIII Міжнар. наук.-практ. конф., 15 берез. 2024 р. Дніпро : ДДУВС, 2024. Ч. 2. С. 335–336. URL: <https://er.dduvs.edu.ua/handle/123456789/14208> (дата звернення: 10.04.2026 р.)

5. Тома М. Г., Василюва О. В. Інструменти OSINT: фіксація воєнних злочинів в Україні. // Актуальні проблеми права та безпеки. 2025. № 1. URL: <https://app-journal.in.ua/wp-content/uploads/2025/04/136.pdf> (дата звернення: 10.04.2026 р.)

6. Colley T. The War on Open-Source Intelligence. // International Journal of Intelligence and CounterIntelligence. 2025. URL: <https://www.tandfonline.com/doi/full/10.1080/0163660X.2025.2554477> (дата звернення: 10.04.2026 р.)

7. K. Zaiets, Yu. Muravska, T. Slipchenko, V. Kaniuka, I. Melnyk. The etymology of the concept “military conflict” as a determinant of political orientation. Law, Policy and Security. Vol. 2. 2024. P.39-51. URL: <https://lpas.com.ua/journals/vol-2-no-2-2024> (дата звернення: 10.04.2026 р.)

8. Marleku A. Public intelligence as a strategic tool: The role of real-time public intelligence in modern conflicts. Security and Defence Quarterly. 2025. URL: <https://securityanddefence.pl/pdf-205566-127235?filename=Public+intelligence+as+a.pdf> (дата звернення: 10.04.2026 р.)

9. Yuzvyk I., Farion-Melnyk A., Lutsiv R., Muravska Y., Moskaliuk N., Kolesnikov A. The implementation of artificial intelligence in criminal law practice: challenges and prospects for development. The 13th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS). The crossing point of Intelligent Data Acquisition & Advanced Computing Systems and East & West Scientists 4-6 September 2025. Gliwice, Poland Vol. 1. P. 630-635.