УДК 351.746:004.738.5

С. В. Бочаров, В. В. Тищук, С. В. Бєлай

ВИКОРИСТАННЯ OSINT В ОПЕРАТИВНО-РОЗШУКОВІЙ ДІЯЛЬНОСТІ: ІНСТРУМЕНТИ І ПРАВОВІ АСПЕКТИ

У статті досліджено можливості застосування OSINT (розвідки з відкритих джерел) в оперативно-розшуковій діяльності, її значення для отримання й аналізу інформації. Розглянуто основні способи збирання відкритих даних, доцільність їхньої інтеграції з іншими оперативно-розшуковими заходами, а також потенційні напрями розвитку цього інструменту. Окреслено правові аспекти OSINT, зокрема питання достовірності та правового статусу таких оперативних даних. Звернено увагу на виклики, пов'язані з поширенням дезінформації, необхідністю правового регулювання та захисту персональних даних. Наголошено на важливості технологічного прогресу, автоматизації процесів та міжнародної співпраці для впровадження OSINT у правоохоронну діяльність і зміцнення національної безпеки.

Ключові слова: *розвідка з відкритих джерел (OSINT), оперативно-розшукова діяльність, збирання й аналіз інформації, національна безпека, протидія злочинності.*

Постановка проблеми. Сучасні технології значно вплинули на способи збирання, оброблення й аналізу інформації в оперативно-розшуковій діяльності (ОРД). Одним із інструментів у цій сфері є розвідка з відкритих джерел (OSINT – Open-Source Intelligence), яка дає змогу отримувати дані із загальнодоступних ресурсів, зокрема засобів масової інформації, соціальних мереж, публічних реєстрів та супутникових знімків.

Актуальність дослідження зумовлена зростанням ролі OSINT у правоохоронній діяльності. Використання відкритих джерел дає змогу оперативним підрозділам одержувати первинні дані, доповнюючи негласні оперативно-розшукові заходи.

Аналіз останніх досліджень і публікацій. Дослідження стосовно використання OSINT у правоохоронній діяльності набули значного розвитку в останні десятиліття, що зумовлено активним упровадженням цифрових технологій у сферу забезпечення національної безпеки [1]. Науковці S. Szymoniak та K. Foks розглядають OSINT як спосіб збирання інформації, що дає можливість оперативно виявляти загрози, аналізувати злочинні зв'язки та підтримувати ухвалення стратегічних рішень [2].

У міжнародній науковій літературі дослідження OSINT переважно зосереджені на його інтеграції з іншими видами оперативної діяльності, питаннях кібербезпеки та можливостях застосування у боротьбі з тероризмом. Наприклад, у праці A. Ziółkowska OSINT розглядається як елемент розвідувального циклу, що дає змогу отримувати інформацію без використання інсайдерських джерел. Водночас акцентується увага на ризиках, пов'язаних із дезінформацією та необхідністю ретельної верифікації одержаних даних [3].

Українські дослідники А. В. Білобров та П. С. Клімушин приділяють увагу застосуванню OSINT у контексті гібридних загроз, військової розвідки та боротьби з кіберзлочинністю. Окремо розглядається питання правового регулювання OSINT, оскільки в Україні немає спеціального законодавства, що чітко визначає його використання в ОРД [4].

Загалом сучасні дослідження свідчать про високий потенціал OSINT у правоохоронній діяльності, проте науковці наголошують на необхідності вдосконалення методології аналізу, підвищення якості автоматизованих систем оброблення інформації та створення відповідної нормативної бази.

Метою статті є аналіз можливостей та обмежень використання OSINT в оперативно-розшуковій діяльності, дослідження основних способів збирання й аналізу інформації, а також оцінювання правового регулювання цієї діяльності.

Виклад основного матеріалу. Розвідка з відкритих джерел (OSINT) – це процес збирання, аналізу й використання інформації, отриманої із загальнодоступних джерел, для вирішення різних спеціальних завдань. У контексті ОРД OSINT є допоміжним інструментом, який дає змогу оперативним підрозділам швидко одержувати й перевіряти інформацію без залучення складних дозвільних процедур, які обмежують права і свободи громадян.

На відміну від традиційних способів ОРД, OSINT використовує виключно доступні дані, такі, як відкриті бази даних і реєстри, засоби масової інформації (онлайн- та друковані видання), соціальні мережі (SOCMINT), аналітичні звіти та публічні дослідження, супутникові знімки та геопросторові дані (GEOINT). OSINT дає змогу виявляти зв'язки між особами, групами та подіями, оцінювати рівень загроз і відстежувати діяльність підозрюваних осіб без необхідності безпосереднього контакту з ними.

Розвідка з відкритих джерел часто інтегрується з іншими напрямами збирання оперативних даних, які застосовуються західними партнерами [5], зокрема: HUMINT (Human Intelligence) – агентурна розвідка, що базується на особистих контактах; SIGINT (Signals Intelligence) – перехоплення комунікаційних сигналів; COMINT (Communications Intelligence) – аналіз змісту перехоплених повідомлень; IMINT (Imagery Intelligence) – аналіз зображень, отриманих із супутників або безпілотних систем [6]. Ключова відмінність OSINT від згаданих заходів полягає у відкритому характері одержаної інформації, що робить цю діяльність більш доступною, але водночас менш надійною порівняно зі способами, які передбачають роботу з конфіденційними (інсайдерськими) даними.

Як окремий напрям діяльності OSINT активно розвивається з кінця XX ст. завдяки поширенню цифрових технологій [7]. У 1990-х роках у США його офіційно визнали джерелом стратегічної інформації, а після терактів 11 вересня 2001 р. значення OSINT суттєво зросло, особливо для сфери національної безпеки. У країнах НАТО він використовується для моніторингу воєнних загроз, виявлення терористичних угруповань та боротьби з гібридними загрозами. В Україні цей підхід набув особливої важливості після 2014 р. у контексті інформаційної та військової боротьби з агресією [8]. Інтеграція OSINT до ОРД забезпечує ефективне збирання й аналіз даних, що дає змогу створювати комплексну картину оперативної ситуації або оперативної обстановки в цілому, на ділянці відповідальності.

Використання OSINT в ОРД базується на різних способах збирання, які дають змогу оперативним підрозділам отримувати інформацію з відкритих джерел. Основні методи охоплюють: моніторинг засобів масової інформації – аналіз публікацій у друкованих та онлайн-виданнях для виявлення ознак злочинної діяльності, політичних загроз чи тенденцій у суспільстві; аналіз соціальних мереж (SOCMINT – Social Media Intelligence) – відстеження активності підозрюваних осіб у Facebook, Twitter, Instagram, Telegram та інших платформах для виявлення зв'язків, намірів і місцезнаходження; оброблення відкритих баз даних – використання державних реєстрів, комерційних баз, судових рішень та корпоративної документації для отримання інформації про осіб, компанії та фінансові операції; геопросторовий аналіз (GEOINT – Geospatial Intelligence) – використання супутникових знімків, даних геолокації та картографічних сервісів для встановлення місцезнаходження об'єктів або осіб; веб-скрейпінг (Web Scraping) – автоматизоване вилучення інформації з веб-сайтів, форумів, баз даних та інших онлайн-ресурсів; зворотний пошук зображень – використання інструментів для перевірки достовірності фотографій та ідентифікації осіб або об'єктів; Dark Web OSINT – збирання інформації з ресурсів у «темному» сегменті інтернету [9].

Сучасні технології сприяють значному прискоренню оброблення даних за допомогою спеціалізованих інструментів. Серед найпопулярніших такі: Maltego – платформа для аналізу зв'язків між особами, компаніями, IP-адресами та доменами; Shodan – пошукова система для виявлення відкритих пристроїв та мережевих інфраструктур, що можуть бути вразливими для кібератак; Google Dorking – методика розширеного пошуку в Google для знаходження прихованих або незахищених файлів та сторінок; SpiderFoot – автоматизований інструмент збирання даних про IP-адреси, домени, електронні адреси та цифрові сліди; CheckUserNames – сервіси для перевірки реєстрації користувачів у різних соцмережах і форумах; ExifTool – програма для аналізу метаданих фото- і відеофайлів, що дає змогу отримати інформацію про місце і час зйомки; The Wayback Machine – архіватор веб-сайтів, який допомагає відстежувати зміни сторінок у часі й одержувати доступ до видаленого контенту [10].

Використання OSINT у правоохоронній діяльності потребує чіткої правової регламентації, оскільки збирання й аналіз інформації з відкритих джерел можуть впливати на права людини. В Україні ОРД регулюється Законом України «Про оперативно-розшукову діяльність» [11], який визначає правові підстави, методи та обмеження збирання інформації. Водночас конкретного нормативного акта, що детально регулював би використання OSINT, досі немає, тому застосування цього методу пошуку здійснюється в межах загального законодавства, зокрема це: Конституція України, яка гарантує право на захист особистої інформації (ст. 32) [12]; Закон України «Про інформацію» [13], що визначає принципи доступу до відкритих джерел; Закон України «Про захист персональних даних» [14], який регламентує оброблення інформації про осіб; Кримінальний процесуальний кодекс України, що встановлює вимоги до доказової бази.

Ці законодавчі аспекти набувають особливої актуальності в умовах триваючої агресії проти України, коли OSINT відіграє дедалі важливішу роль у боротьбі з воєнними злочинами, зміцненні національної безпеки та притягненні правопорушників до відповідальності. Аналіз цифрових доказів (фотографії та відео) дає змогу ідентифікувати агресорів і підтверджувати факти злочинів, однак відсутність чітких правових норм стосовно OSINT ускладнює процес використання таких матеріалів у судових провадженнях. З огляду на це Консультативна місія ЄС в Україні спільно з Bellingcat, GLAN та іншими партнерами організувала для українських правників серію семінарів, зосереджених на методах OSINT, їх відповідності правовим стандартам та практичному застосуванні у судовій системі.

Під час цих заходів особливу увагу приділяли міжнародним ініціативам, таким, як проєкт SIRIUS, що спрощує доступ до цифрових доказів і сприяє транскордонній співпраці. Це свідчить про те, що для впровадження OSINT у правоохоронну діяльність недостатньо лише внутрішнього законодавчого регулювання – необхідна міжнародна підтримка, інтеграція новітніх технологій та обмін досвідом. Саме така співпраця є важливою для боротьби з воєнними злочинами та зміцнення національної безпеки [15].

Розвиток інформаційних технологій значно розширює можливості OSINT в ОРД. Серед перспективних напрямів можна виділити: штучний інтелект і машинне навчання – автоматизація аналізу великих масивів даних, швидка ідентифікація загроз, аналіз поведінкових моделей підозрюваних осіб; розвиток OSINT-інструментів – удосконалення пошукових платформ, геоаналітичних систем та технологій розпізнавання осіб (Face Recognition, NLP-аналіз текстів); інтеграція блокчейн-аналітики – можливість відстеження криптовалютних транзакцій і виявлення фінансових схем відмивання коштів; збільшення відкритих баз даних – розширення державних і міжнародних реєстрів для використання в аналітичних цілях [16].

Попри технологічний прогрес, використання OSINT в ОРД супроводжується низкою викликів: проблеми достовірності інформації – поширення дезінформації, фейкових новин і маніпулятивних матеріалів у відкритих джерелах [17]; обмеження доступу до інформації – посилення захисту персональних даних, обмеження доступу до реєстрів, зростання кількості закритих або зашифрованих платформ; протидія з боку злочинних угруповань – використання анонімних мереж (Tor, I2P), шифрування комунікацій, підроблення цифрових слідів для введення оперативників в оману; юридичні обмеження – відсутність чітких міжнародних стандартів щодо збирання і використання OSINT у ході проведення оперативно-розшукових заходів, проблеми правової легітимності отриманих даних у судовому розслідуванні. Для подолання цих викликів необхідними є комплексне вдосконалення законодавчої бази і впровадження міжнародних стандартів щодо використання OSINT у правоохоронній сфері [18, 19].

Висновки

Розвідка з відкритих джерел стала важливим інструментом оперативно-розшукової діяльності, який не лише доповнює негласні оперативно-розшукові заходи, а й дає змогу значно прискорити аналітичні процеси. Правоохоронні органи активно використовують для швидкого виявлення правопорушників, аналізу їхніх зв’язків, відстеження фінансових операцій та моніторингу загроз у сфері національної безпеки такі автоматизовані платформи, як Maltego, Shodan та Google Dorking. Проте OSINT залишається допоміжним інструментом, що потребує інтеграції з іншими оперативно-розшуковими заходами для забезпечення достовірності отриманих даних. Широке застосування OSINT вимагає належного правового врегулювання, адже в Україні досі немає спеціального законодавства, яке б чітко визначало межі використання OSINT, що створює ризики і для захисту персональних даних, і для допустимості таких матеріалів у судовій практиці. Подальший розвиток цієї сфери залежить як від технологічних досягнень, зокрема впровадження штучного інтелекту та новітніх аналітичних інструментів, так і від здатності державних органів пристосувати правову базу до сучасних викликів, серед яких протидія дезінформації та забезпечення міжнародної координації у сфері цифрової розвідки.

Напрямом подальших досліджень буде розроблення методики збирання, оброблення та обов’язкових аналізу й перевірки інформації за методом OSINT.

Перелік джерел посилання

1. Зоренко Д. С., Лех Р. В., Кулик Д. О., Червяков О. І. Використання інструментів та методів OSINT для отримання пошукової інформації : практ. порадник. Харків : ІПЮК для СБУ, 2023. 36 с.

2. Szymoniak S., Foks K. Open-Source Intelligence Opportunities and Challenges – A Review. *Advances in Science and Technology Research Journal*. 2024. Vol. 18. № 3. P. 123–139. DOI: https://doi.org/10.12913/22998624/186036.

3. Ziółkowska A. Open-source intelligence (OSINT) as an element of military recon. *Security and Defence Quarterly*. 2018. Vol. 19. № 2. P. 65–77. DOI: https://doi.org/10.5604/01.3001.0012.1474.

4. Білобров А. В., Клімушин П. С. Використання технологій OSINT для отримання інформації. *Протидія кіберзлочинності та торгівлі людьми* : зб. матеріалів Міжнар. наук.-практ. конф., м. Харків, 27 трав. 2020 р. Харків, 2020. С. 135–137. URL: https://surli.cc/scziio (дата звернення: 03.03.2025).

5. Van Puyvelde D., Tabárez Rienzi F. The rise of open-source intelligence. *European Journal of International Security*. 2025. P. 1–15. DOI: https://doi.org/10.1017/eis.2024.61.

6. Тищук В. В. Окремі аспекти забезпечення прав людини під час використання безпілотних літальних апаратів для охорони державних кордонів. *Актуальні проблеми правоохоронної діяльності в умовах воєнного стану* : зб. тез доп. ІІ наук.-практ. конф., м. Хмельницький, 3 січ. 2024 р. Хмельницький, 2024. Т. 1. С. 180–182.

7. Evangelista J. R. G., Sassi R. J., Romero M., Napolitano D. Systematic Literature Review to Investigate the Application of Open-Source Intelligence (OSINT) with Artificial Intelligence. *Journal of Applied Security Research*. 2020. Vol. 16. № 3. P. 345–369. DOI: https://doi.org/10.1080/19361610.2020.1761737.

8. Molfar. OSINT інструменти для розвідки на основі відкритих джерел. URL: https://molfar.com/useful-apps (дата звернення: 03.03.2025).

9. Задерейко О., Долінко К. GEOINT: можливості геопросторової розвідки. *Кіберпростір в умовах війни та глобальних викликів XXI століття: теорія та практика* : матеріали Міжнар. наук.-практ. конф., м. Одеса, 24 листоп. 2023 р. Одеса, 2023. С. 118–122. URL: https://surl.li/urjlru (дата звернення: 03.03.2025).

10. Sayer P., Brenner B. 21 best free security tools. CSO. 2021. URL: https://surl.li/cclhlb (дата звернення: 03.03.2025).

11. Про оперативно-розшукову діяльність : Закон України від 18.02.1992 р. № 2135-XII. *Відомості Верховної Ради України.* 1992. № 22. Ст. 303. URL: https://zakon.rada.gov.ua/laws/show/2135-12#Text (дата звернення: 03.03.2025).

12. Конституція України : офіц. текст. URL: https://surl.li/yqohub (дата звернення: 03.03.2025).

13. Про інформацію : Закон України від 02.10.1992 р. № 2657-XII. *Відомості Верховної Ради України*. 1992. № 48. Ст. 650. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення: 03.03.2025).

14. Про захист персональних даних : Закон України від 01.06.2010 р. № 2297-VI. *Відомості Верховної Ради України.* 2010. № 34. Ст. 481. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення: 03.03.2025).

15. EUAM UKRAINE. Інструменти OSINT у прагненні до справедливості в Україні. 2024. URL: https://surl.li/yswqnc (дата звернення: 03.03.2025).

16. Докрелл В. Адаптація до нових викликів OSINT: інструменти та методи в умовах глобальних змін. *You control*. 2024. URL: https://surli.cc/tjllgk (дата звернення: 03.03.2025).

17. Тищук В. Спроби криміналізації поширення дезінформації в Україні. *Війна в Україні: зроблені висновки та незасвоєні уроки* : зб. тез доп. Міжнар. наук.-практ. конф., м. Львів, 22-23 лют. 2024 р. Львів, 2024. С. 903–908.

18. Бочаров С. В. Особливості попередження загроз у прикордонній сфері діяльності в умовах забезпечення колективної безпеки. *Грааль науки*. 2021. № 7. С. 119–121. DOI: https://doi.org/10.36074/grail-of-science.27.08.2021.019.

19. Бочаров С. В., Кіреєва О. С. Особливості забезпечення національної безпеки України шляхом попередження загроз державній безпеці у прикордонній сфері. *Акуальні питання у сучасній науці.* 2024. № 9 (27). С. 288–302. DOI: https://doi.org/10.52058/2786-6300-2024-9(27)-288-302.

Стаття надійшла до редакції 05.03.2025 р.

UDC 351.746:004.738.5

S. Bocharov, V. Tyshchuk, S. Bielai

USE OF OSINT IN OPERATIONAL AND INVESTIGATIVE ACTIVITIES: TOOLS AND LEGAL ASPECTS

The article examines the possibilities of applying OSINT (Open-Source Intelligence) in operational and investigative activities and its significance for acquiring, processing, and analyzing information to ensure public and national security. The main methods of collecting open-source data are considered, including using social networks, government registries, mass media, satellite imagery, and specialized OSINT tools. The feasibility of integrating OSINT with other intelligence-gathering disciplines, such as HUMINT, SIGINT, and IMINT, is assessed, as this enhances the reliability of obtained data and expands analytical capabilities.

Particular attention is paid to the legal aspects of OSINT use in law enforcement, including the legality of acquiring, storing, and utilizing open-source information during operational and investigative activities. The key challenges related to data accuracy, legal status, and potential risks are analyzed, such as information manipulation and legal restrictions on collecting personal data. The necessity of developing a regulatory framework that would govern the use of OSINT within operational and investigative activities while maintaining a balance between its effectiveness and human rights compliance is emphasized.

The article also highlights the importance of implementing technological innovations, particularly data collection and analysis automation through artificial intelligence and blockchain analytics. It concludes that the effective use of OSINT in law enforcement is only possible through a balanced integration of modern technologies, legal regulation, and international cooperation.

Keywords: *open-source intelligence (OSINT), operational and investigative activities, information collection and analysis, national security, crime prevention.*

БОЧАРОВ Сергій Володимирович – доктор філософії в галузі воєнних наук, викладач кафедри спеціальних дисциплін факультету правоохоронної діяльності, Національна академія Державної прикордонної служби України імені Богдана Хмельницького
https://orcid.org/0000-0002-3824-4022

ТИЩУК Віктор Володимирович – доктор філософії в галузі права, доцент кафедри спеціальних дисциплін факультету правоохоронної діяльності, Національна академія Державної прикордонної служби України імені Богдана Хмельницького
https://orcid.org/0000-0001-5811-5909

БЄЛАЙ Сергій Вікторович – доктор наук з державного управління, професор, заступник начальника навчально-наукового центру організації освітнього процесу – начальник науково-методичного відділу, Національна академія Національної гвардії України
https://orcid.org/0000-0002-0841-9522