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 and analyzing information. The main ways of collecting open-source data are considered, including the feasibility of their integration with other operational and investigative measures and the potential directions for this tool development. The legal aspects of OSINT are outlined, in particular, the issues of reliability and legal status of these operational data. Specific attention is paid to the challenges related to the spread of disinformation, the necessity of legal regulation, and the protection of personal data. The article also highlights the importance of technological progress, process automation, and international cooperation for OSINT implementation in law enforcement and the strengthening of national security.

Keywords: *Open-Source Intelligence (OSINT), operational and investigative activities, information collection and analysis, national security, crime prevention.*

Statement of the problem. Modern technologies have significantly influenced the ways of acquiring, processing, and analyzing information within operational and investigative activities (OIA). Open-Source Intelligence (OSINT) in this sphere is one of the tools that allows for obtaining data from publicly available resources, including the mass media, social networks, public registers, and satellite images.

The relevance of the study is determined by the OSINT's growing role in law enforcement. The use of open sources enables operational units to obtain primary data, supplementing covert operational and investigative activities.

Analysis of recent research and publications. Research on the use of OSINT in law enforcement has received significant development in recent decades, owing to the active introduction of digital technologies in the sphere of national security [1]. Scholars S. Szymoniak and K. Foks consider OSINT as a method of gathering information that enables prompt detection of threats, analysis of criminal connections, and support of strategic decision-making [2].

OSINT studies in the international scientific literature mainly focus on its integration with other types of operational activities, cybersecurity issues, and the possibilities of its application in combating terrorism. For example, OSINT is considered an element of the intelligence cycle in the work by A. Ziółkowska, which allows getting information without using insider sources. At the same time, the article focuses on the risks associated with disinformation and the need for thorough verification of the data obtained [3].

Ukrainian researchers A. Bilobrov and P. Klimushyn pay attention to OSINT use in the context of hybrid threats, military intelligence, and the fight against cybercrime. The matter of legal regulation of OSINT is considered separately since Ukraine does not have special laws that clearly define its utilization in OIA [4].

Current studies in general indicate the high potential of OSINT in law enforcement, but scholars emphasize the need to improve the analysis methodology, increase the quality of automated information processing systems, and create an appropriate regulatory framework.

The purpose of the article is to examine the possibilities and limitations of using OSINT in operational and investigative activities, to explore the main methods of collecting and analyzing information, and to assess the legal regulation of this activity.

Summary of the main material. OSINT is the process of gathering, analyzing, and applying information obtained from publicly available sources to solve various special tasks. OSINT is an auxiliary tool in the context of the OIA that allows operational units to quickly receive and verify information without involving complex permitting procedures that restrict the rights and freedoms of the citizens.

In contrast to traditional modes of OIA, OSINT relies exclusively on available data, such as open databases and registries, mass media (online and print publications), social networks (SOCMINT), analytical reports and public research, satellite images, and geospatial data (GEOINT). OSINT provides an ability to identify ties between individuals, groups, and events, assess the level of threats, and track the activities of suspects without the need for direct contact with them.

Open-source intelligence is often integrated with other surveillance collection activities adopted by Western partners [5], namely: HUMINT (Human Intelligence) – agent intelligence based on personal contacts; SIGINT (Signals Intelligence) – interception of communication signals; COMINT (Communications Intelligence) – analysis of the content of intercepted messages; IMINT (Imagery Intelligence) – analysis of images received from satellites or unmanned systems [6]. The key difference between OSINT and the above-mentioned measures is the open nature of the received information, which makes this activity more affordable but at the same time less reliable compared to techniques that involve working with confidential (insider) data.

As a separate line of activity, OSINT has been actively evolving since the end of the XX century due to the spread of digital technologies [7]. It was officially recognized as a source of strategic information in the United States in the 1990s. And after the September 11 terrorist attacks of 2001, the importance of OSINT increased significantly, especially for the national security sphere. It is used in NATO countries to monitor military dangers, detect terrorist groups, and combat hybrid threats. This approach has become especially important in Ukraine after 2014 in the context of the informational and military struggle against aggression [8]. The integration of OSINT into the OIA ensures effective gathering and analysis of data, which gives the opportunity to create a comprehensive picture of the operational situation or the operational environment in general within the area of responsibility.

The use of OSINT in the OIA is based on various kinds of compilation that enable operational units to obtain information from open sources. The primary methods include the following: mass media monitoring – analyzing publications in print and online media to detect signs of criminal activity, political threats, or tendencies in society; social media analysis (SOCMINT – Social Media Intelligence) – tracking the activity of suspects on Facebook, Twitter, Instagram, Telegram, and other platforms to identify connections, intentions, and locations; open database processing – the use of public registers, commercial databases, court decisions, and corporate documentation to get information about individuals, companies, and financial transactions; geospatial analysis (GEOINT – Geospatial Intelligence) – the use of satellite images, geolocation data, and mapping services to determine the location of objects or individuals; Web Scraping – automated extraction of information from websites, forums, databases, and other online resources; reverse image search – the use of tools to verify the authenticity of photos and identify persons or objects; Dark Web OSINT – gathering information from resources in the "dark" segment of the Internet [9].

Modern technologies facilitate significant speed-up of data processing with the help of specialized instruments. Among the most popular are the following: Maltego – a platform for analyzing connections between individuals, companies, IP addresses, and domains; Shodan – a search engine for identifying open devices and network infrastructures that may be vulnerable to cyberattacks; Google Dorking – an advanced search methodology on Google to find hidden or unprotected files and pages; SpiderFoot – an automated tool for collecting data about IP addresses, domains, email addresses, and digital footprints; CheckUserNames – services for checking user registration in various social networks and forums; ExifTool – a program for analyzing metadata of photo and video files, providing information about the place and time of the shooting; The Wayback Machine – a website archiver that helps to track changes in pages over time and access deleted content [10].

The application of OSINT for law enforcement requires clear legal regulation, as the collection and analysis of information from open sources may affect human rights. OIA in Ukraine is regulated by the Law of Ukraine "About Operational and Investigative Activity" [11], which defines the legal grounds, methods, and limitations of information gathering. At the same time, there is still no specific normative act that would thoroughly

regulate the use of OSINT, so this search method utilization is carried out within the scope of general legislation, namely: the Constitution of Ukraine, which guarantees the right to protection of personal information (Art. 32) [12]; the Law of Ukraine "On Information" [13], which specifies the principles of access to open sources; the Law of Ukraine "On Personal Data Protection" [14], which regulates the processing of information about individuals; the Criminal Procedure Code of Ukraine, which sets requirements for the evidence base.

These legislative aspects are especially relevant in the context of the ongoing aggression against Ukraine, when OSINT plays an increasingly important role in combating war crimes, strengthening national security, and bringing offenders to justice. The analysis of digital evidence (photos and videos) enables the identification of aggressors and confirms the facts of crimes, but the absence of clear legal provisions regarding OSINT complicates the process of using such materials in judicial proceedings. With this in mind, the EU Advisory Mission Ukraine, together with Bellingcat, GLAN, and other partners, organized a series of seminars for Ukrainian legal professionals focused on OSINT methods, their compliance with legal standards, and practical application in the judicial system.

Special attention at these events was paid to international initiatives, such as the SIRIUS project, which facilitates access to digital proof and promotes cross-border cooperation. This indicates that domestic legislative regulation alone is not enough to implement OSINT in law enforcement – international support, integration of the latest technology, and exchange of experience are needed. It is this kind of cooperation that is important for combating war crimes and strengthening national security [15].

The development of information technology significantly expands the capabilities of OSINT for the OIA. The promising areas include artificial intelligence and machine learning – automation of big data analysis, rapid identification of threats, behavioral analysis of suspects; development of OSINT tools – improvement of search engines, geo-analytical systems, and face recognition technologies (NLP text analysis); integration of blockchain analytics – the ability to track cryptocurrency transactions and detect money laundering schemes; growth of open databases – expansion of state and international registers to be used for analytical purposes [16].

The use of OSINT in the OIA is accompanied by several difficulties despite technological progress: problems of information accuracy – the spread of disinformation, fake news, and manipulative materials in open sources [17]; restrictions on access to information – enhanced protection of personal data, restrictions on access to registries, an increase in the number of closed or encrypted platforms; opposition from criminal groups – the use of anonymous networks (Tor, I2P), encryption of communications, falsification of digital traces to mislead operatives; legal constraints – the absence of clear international standards for the acquisition and use of OSINT in the course of operational and investigative activities, problems of legal legitimacy of the obtained data in a judicial inquiry. A comprehensive improvement of the legislative framework and introduction of international standards for OSINT application in law enforcement are necessary to overcome these challenges [18, 19].

Conclusions

Open-source intelligence has become an important instrument of operational and investigative activities, not only supplementing covert operational and investigative measures but also significantly accelerating analytical processes. Law enforcement authorities are actively using automated platforms like Maltego, Shodan, and Google Dorking to quickly identify offenders, analyze their connections, track financial transactions, and monitor national security threats. However, OSINT remains an auxiliary tool that requires integration with other operational and investigative measures to ensure the accuracy of the acquired data. The widespread application of OSINT demands proper legal regulation, as Ukraine still lacks special legislation that would clearly determine the boundaries of OSINT usage, which poses risks both to the protection of personal data and to the admissibility of such materials in judicial practice. Further development of this sphere depends both on technological advances, in particular, the introduction of artificial intelligence and the newest analytical instruments, and on the ability of state bodies to adapt the legal framework to modern challenges, including countering disinformation and ensuring international coordination in the digital intelligence sector.

The direction of future research will be the development of a methodology for gathering, processing, and mandatory analysis and verification of information using the OSINT technique.

References

1. Zorenko D. S., Lekh R. V., Kulyk D. O., Cherviakov O. I. (2023). *Vykorystannia instrumentiv ta metodiv OSINT dlia otrymannia poshukovoi informatsii* [Using OSINT tools and methods to obtain search information: a practical guide]. Kharkiv : IPYUK dlia SBU [in Ukrainian].

2. Szymoniak S., Foks K. (2024). Open-Source Intelligence Opportunities and Challenges – A Review. *Advances in Science and Technology Research Journal*, vol. 18, no. 3, pp. 123–139. DOI: https://doi.org/10.12913/22998624/186036 [in English].

3. Ziółkowska A. (2018). Open-source intelligence (OSINT) as an element of military recon. *Security and Defence Quarterly*, vol. 19, no. 2, pp. 65–77. DOI: https://doi.org/10.5604/01.3001.0012.1474 [in English].

4. Bilobrov A. V., Klimushyn P. S. (2020). *Vykorystannia tekhnolohii OSINT dlia otrymannia informatsii* [Using OSINT technologies to obtain information]. Proceedings of the International scientificand practical conference *"Protydiia kiberzlochynnosti ta torhivli liudmy"* (Ukraine, Kharkiv, May 27, 2020). Kharkiv, pp. 135–137. Retrieved from: https://surli.cc/scziio (accessed 3 March 2025) [in Ukrainian].

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

6. Tyshchuk V. V. (2024). *Okremi aspekty zabezpechennia prav liudyny pid chas vykorystannia bezpilotnykh litalnykh aparativ dlia okhorony derzhavnykh kordoniv* [Certain aspects of ensuring human rights during the use of unmanned aerial vehicles to protect state borders]. Proceedings of the 2nd Scientificand practical conference *"Aktualni problemy pravookhoronnoi diialnosti v umovakh voiennoho stanu"* (Khmelnytskyi, January 3, 2024). Khmelnytskyi, iss. 1, pp. 180–182 [in Ukrainian].

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

8. Molfar (2025). *OSINT instrumenty dlia rozvidky na osnovi vidkrytykh dzherel* [OSINT tools for intelligence based on open sources]. Retrieved from: https://molfar.com/useful-apps (accessed 3 March 2025) [in Ukrainian].

9. Zadereiko O., Dolinko K. (2023). *GEOINT: mozhlyvosti heoprostorovoi rozvidky* [GEOINT: geospatial intelligence capabilities]. Proceedings of the International scientificand practical conference *"Kiberprostir v umovakh viiny ta hlobalnykh vyklykiv XXI stolittia: teoriia ta praktyka"* (Ukraine, Odesa, November 24, 2023). Odesa, pp. 118–122. Retrieved from: https://surl.li/urjlru (accessed 3 March 2025) [in Ukrainian].

10. Sayer P., Brenner B. (2021). 21 best free security tools. CSO. Retrieved from: https://surl.li/cclhlb (accessed 3 March 2025) [in English].

11. *Zakon Ukrainy "Pro operatyvno-rozshukovu diialnist" № 2135-XII* [Law of Ukraine about Operational and Investigative activity no. 2135-XII]. (1992, February 18). *Vidomosti Verkhovnoi Rady Ukrainy*. Retrieved from: https://zakon.rada.gov.ua/laws/show/2135-12#Text (accessed 3 March 2025) [in Ukrainian].

12. *Konstytutsiia Ukrainy* [Constitution of Ukraine]. Retrieved from: https://surl.li/yqohub (accessed 3 March 2025) [in Ukrainian].

13. *Zakon Ukrainy "Pro informatsiiu" № 2657-XII* [Law of Ukraine about Information activity no. 2657-XII]. (1992, October 2). *Vidomosti Verkhovnoi Rady Ukrainy*. Retrieved from: https://zakon.rada.gov.ua/laws/show/2657-12#Text (accessed 3 March 2025) [in Ukrainian].

14. *Zakon Ukrainy "Pro zakhyst personalnykh danykh" № 2297-VI* [Law of Ukraine about Protection of Personal Data activity no. 2297-VI]. (2010, June 1). *Vidomosti Verkhovnoi Rady Ukrainy*. Retrieved from: https://zakon.rada.gov.ua/laws/show/2297-17#Text (accessed 3 March 2025) [in Ukrainian].

15. EUAM UKRAINE (2024). *Instrumenty OSINT u prahnenni do spravedlyvosti v Ukraini* [OSINT tools in the pursuit of justice in Ukraine]. Retrieved from: https://surl.li/yswqnc (accessed 3 March 2025) [in Ukrainian].

16. Dokrell V. (2024). *Adaptatsiia do novykh vyklykiv OSINT: instrumenty ta metody v umovakh hlobalnykh zmin* [Adapting to new OSINT challenges: tools and methods in the face of global change]. *You control*. Retrieved from: https://surli.cc/tjllgk (accessed 3 March 2025) [in Ukrainian].

17. Tyshchuk V. (2024). *Sproby kryminalizatsii poshyrennia dezinformatsii v Ukraini* [Attempts to criminalize the spread of disinformation in Ukraine]. Proceedings of the International scientificand practical

conference *"Viina v Ukraini: zrobleni vysnovky ta nezasvoieni uroky"* (Ukraine, Lviv, February 22-23, 2024). Lviv, pp. 903–908 [in Ukrainian].

18. Bocharov S. V. (2021). *Osoblyvosti poperedzhennia zahroz u prykordonnii sferi diialnosti v umovakh zabezpechennia kolektyvnoi bezpeky* [Peculiarities of threat prevention in the border area of activity in the context of ensuring collective security]. *Hraal nauky*, no. 7, pp. 119–121. DOI: https://doi.org/10.36074/grail-of-science.27.08.2021.019 [in Ukrainian].

19. Bocharov S. V., Kireieva O. S. (2024). *Osoblyvosti zabezpechennia natsionalnoi bezpeky Ukrainy shliakhom poperedzhennia zahroz derzhavnii bezpetsi u prykordonnii sferi* [Peculiarities of ensuring the national security of Ukraine by preventing threats to state security in the border area]. *Aktualni pytannia u suchasnii nautsi*, no. 9 (27), pp. 288–302. DOI: https://doi.org/10.52058/2786-6300-2024-9(27)-288-302 [in Ukrainian].

The article was submitted to the editorial office on 5 March 2025

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

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 їх 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.

Розвідка на основі відкритих джерел OSINT (Open-Source Intelligence) – концепція, методологія і технологія добування й використання військової, політичної, економічної та іншої інформації з відкритих джерел без порушення законів. Використовується для ухвалення рішень у сфері національної безпеки і оборони, розслідувань тощо.

Традиційні способи оперативно-розшукової діяльності передбачають низку гласних і негласних методів та використання спеціальних засобів для здобуття інформації. Зі свого боку, OSINT застосовує виключно доступні дані, такі, як відкриті бази даних і реєстри, засоби масової інформації (онлайн- і 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, не потребуючи безпосереднього контакту з ними.

Звернено увагу на виклики, пов'язані з поширенням дезінформації, необхідністю правового регулювання, а також 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.*

BOCHAROV Serhii – PhD in Military Sciences, Lecturer at the Department of Special Disciplines, Bohdan Khmelnytskyi National Academy of the State Border Guard Service of Ukraine.
https://orcid.org/0000-0002-3824-4022

TYSHCHUK Viktor – PhD in Law, Associate Professor at the Department of Special Disciplines, Bohdan Khmelnytskyi National Academy of the State Border Guard Service of Ukraine.
https://orcid.org/0000-0001-5811-5909

BIELAI Serhii – Doctor of Science in Public Administration, Professor, Deputy Head of the Educational and Scientific Center for the Organization of the Educational Process – Head of the Scientific-Methodological Department, National Academy of the National Guard of Ukraine
https://orcid.org/0000-0002-0841-9522