Shevchenko Nataliia, Candidate of Economic Sciences, Associate Professor Senior Researcher at the Research Laboratory for Security Law and OSINT Research Lviv State University of Internal Affairs, Ukraine, ORCID: https://orcid.org/0000-0002-1815-7554

OSINT AS A TOOL FOR ECONOMIC SECURITY ANALYSIS: FROM ENTERPRISES TO THE STATE

Abstract

In the context of the digitalization of economic processes, the growing volume of publicly available information, and the intensification of hybrid, financial, information, and reputational threats, the search for new tools to promptly identify and assess risks to economic security has taken on particular importance. Traditional approaches to economic security analysis, which focus primarily on the internal performance indicators of economic entities and official statistical data, do not always make it possible to identify hidden interconnections, potential conflicts of interest, signs of counterparty misconduct, or financial and reputational risks. In this context, a promising direction is the application of OSINT (Open Source Intelligence) as a system for collecting, verifying, structuring, and analytically processing information from open sources.

The purpose of this article is to justify the role of OSINT as an information and analytical tool for assessing economic security and to identify the specific features of its application at the enterprise, institutional, and state levels. The study systematizes the main sources of open-source information that can be used to assess economic risks, including government registries, financial and statistical information, public procurement data, court decisions, sanctions lists, corporate ties, and media and digital resources. It is proposed to view OSINT not merely as a set of technical methods for searching for information, but as a comprehensive

analytical methodology that facilitates the transition from individual information signals to the identification of risks and threats to economic security.

The report justifies the need to differentiate OSINT research areas according to the level of economic security. At the micro level, OSINT can be used to vet counterparties, owners, and beneficiaries, and to assess financial, legal, reputational, and compliance risks. At the level of institutions and organizations, open data creates opportunities to analyze partnerships, financial ties, personnel relationships, and procurement links, as well as to identify potential conflicts of interest and opaque interdependencies. At the state level, OSINT facilitates the monitoring of strategic economic processes, sanctions risks, critical dependencies, foreign economic ties, and systemic threats. A conceptual sequence for integrating OSINT into the economic security management system is proposed: information collection – verification – structuring – establishing interconnections – identifying risks and threats – assessing the level of economic security – formulating a management decision – preventive response. It is concluded that the systematic use of OSINT can enhance the soundness of management decisions, expand the information base for assessing economic security, and strengthen the preventive nature of its assurance.

Keywords: OSINT, open data, economic security, information and analytical activities, economic risks, threats, security analytics, risk management, enterprise, state.

Statement of the problem. In the context of the digital transformation of the economy, the growth of information flows, and increasing instability in the economic environment, ensuring economic security requires the prompt identification of risks and threats based on reliable and comprehensive information. Traditional approaches to assessing economic security, which rely primarily on internal business performance indicators, official statistics, and

financial reports, do not always allow for the timely identification of hidden interconnections between entities, signs of counterparty misconduct, or reputational, legal, sanctions-related, and other potential threats. At the same time, a significant amount of the information needed for security analysis is already publicly available-in government registries, databases, government information resources, public procurement systems, court decisions, the media, and digital platforms.

The problem lies in the lack of a systematic approach to using open data as a source of information and analytical support for economic security at various levels of its development - from individual enterprises to institutions and the state. This is precisely why there is a growing need for a scientific justification of the role of OSINT (Open Source Intelligence) as a tool not only for searching for open information, but also for its targeted collection, verification, structuring, and analysis to identify economic risks and threats. This necessitates identifying areas of OSINT application within the economic security analysis framework and developing approaches to its integration into the managerial decision-making process.

Analysis of recent studies and publications. The topic of OSINT use in modern security systems is actively being explored in both international and domestic research. One of the practical applications of open-source intelligence is the identification and assessment of organizational risks. D. R. Hayes and F. Cappa (2018) demonstrated the potential of OSINT for conducting risk assessments and identifying organizational vulnerabilities, emphasizing the value of using the information obtained to inform tactical and strategic management decisions [1]. In a study by S. Fantinelli and D. F. Sivilli (2015), OSINT is already considered in the context of organizational activities as a tool for collecting and analyzing information capable of facilitating decision-making, preventive risk analysis, due diligence, and reputation assessment [2].

An important area of scholarly discourse is the development of methodological foundations for transforming open data into analytically meaningful information. S. Khan and D. Wallom (2022) emphasize the organization of processes for collecting, systematizing, and presenting OSINT, viewing it as a process of transforming open data from various sources into information suitable for practical use [3]. A comprehensive review of the current state of OSINT, conducted by A. Yadav, A. Kumar, and V. Singh (2023), demonstrates the expansion of its scope of application and the potential for utilizing vast amounts of publicly available information to address challenges in cybersecurity, national security, threat detection, and crime prevention [4]. At the same time, D. Van Puyvelde and F. Tabárez Rienzi (2025) attribute the growing role of OSINT to a massive increase in the volume of data available online and the expanding capabilities of state and non-state actors to use it to investigate a wide range of security issues [5].

Certain aspects of OSINT directly related to economic security are also addressed in recent Ukrainian studies. I. Mihus (2026) substantiates the role of open-source intelligence (OSINT), fact-checking, and cross-verification of data in vetting counterparties and minimizing a company’s financial, legal, reputational, informational, operational, and corruption risks [6]. At the national and international levels, the potential of OSINT is confirmed by a study by M. Sidoruk (2026), which proposes a methodology for using open sources to verify sanctions-evasion schemes, identify hidden corporate ties, and analyze international supply chains [7].

Thus, existing studies provide a solid theoretical and methodological foundation for the use of OSINT in the fields of risk management, cybersecurity, due diligence, sanctions monitoring, and information and analytical activities. At the same time, a comprehensive approach to OSINT specifically as a tool for analyzing economic security—one that ensures interconnection between the micro

level (enterprises), the institutional level (agencies and organizations), and the macro level (the state)—remains under-researched. This necessitates the systematization of OSINT application areas for identifying economic risks and threats, as well as the development of a conceptual approach to its integration into the economic security management system.

Purpose of the article. The purpose of this article is to justify the role of OSINT as an information and analytical tool for ensuring economic security at the enterprise, institutional, and state levels; to systematize the areas of its application for identifying, verifying, and assessing economic risks and threats; and to develop a conceptual approach to integrating OSINT into the system of security-oriented managerial decision-making.

Presentation of the main research material. OSINT (Open Source Intelligence) should be viewed as an information and analytical activity that involves the targeted search, collection, verification, systematization, comparison, and analysis of information obtained from legally accessible open sources, with the aim of generating new analytical knowledge and using it to make informed decisions. Accordingly, OSINT research is a systematic process of studying objects, phenomena, processes, and interrelationships based on open-source information, using specialized search, verification, and analytical methods as well as digital tools. The result is not the mechanical accumulation of open data, but rather the generation of structured analytical information that makes it possible to establish facts and interrelationships, as well as to identify patterns, anomalies, risks, and potential threats.

Within the economic security framework, the role of OSINT research is determined primarily by its ability to expand the information base for risk assessment and managerial decision-making. Open sources make it possible to supplement traditional financial and economic indicators with information on the ownership structure of business entities, their beneficial owners, corporate ties,

legal proceedings, participation in public procurement, sanctions restrictions, reputation, and other factors that may directly or indirectly affect economic security. At the same time, it is fundamentally important to distinguish between the concepts of “open data” and “OSINT”: open data serves as an information resource, whereas OSINT involves the methodology for searching for, verifying, cross-referencing, and analytically interpreting that data.

Given the multi-layered nature of economic security, the main areas of application for OSINT research can be systematically categorized as follows:

1. Vetting counterparties and business partners. OSINT makes it possible to investigate registration details, ownership structure, ultimate beneficial owners, related legal entities and individuals, court cases, debt, sanctions restrictions, and reputation. This facilitates a comprehensive due diligence process and reduces the likelihood of collaborating with unscrupulous or high-risk entities.

2. Identification of corporate and financial risks. Combining information from various open sources allows for the identification of hidden corporate ties, changes in ownership and management, potential conflicts of interest, anomalous transactions, and other indicators that may signal an elevated level of financial or economic risk.

3. Compliance and sanctions monitoring. OSINT research can be used to screen entities and their associated individuals against sanctions lists, analyze corporate and foreign economic ties, and identify factors that may pose sanctions, legal, or reputational risks.

4. Analysis of public procurement and the use of financial resources. Data from electronic procurement systems, combined with information from government registries, court decisions, and other open sources, enables the investigation of relationships among procurement participants, the identification of potential conflicts of interest, signs of anti-competitive behavior, and other risky interconnections.

5. Competitive and market analytics. Open sources can be used to research competitors, market trends, new products and technologies, changes in consumer behavior, business activity, and other external factors. Such analysis enhances a company's ability to adapt its strategy to market changes and respond promptly to new threats.

6. Reputational and Information Security. Monitoring the open information space makes it possible to identify negative information trends, disinformation, reputational threats, and information campaigns capable of influencing the activities of a company or institution and the economic interests of the state.

7. Assessing threats to the state's economic security. At the macro level, OSINT research can be used to analyze foreign economic relations, strategic industries and enterprises, critical economic dependencies, sanctions risks, the transformation of supply chains, and other processes capable of affecting the stability of the national economy. Thus, OSINT is becoming an important tool—not only at the corporate level but also at the state level—for providing information and analytical support for economic security.

The use of OSINT takes on particular significance for Ukraine in the context of a full-scale war, when economic security is shaped by the simultaneous influence of military, financial, energy, logistical, information, and foreign economic threats. Open-source intelligence creates additional opportunities to identify and analyze business entities' ties to the aggressor state, investigate sanctions risks and potential schemes for circumventing restrictions, monitor changes in supply chains, assess risks to critical enterprises, and vet entities involved in the use of public and international financial resources. Therefore, the development of OSINT capabilities and the integration of OSINT research findings into the activities of businesses, institutions, law enforcement agencies, and regulatory bodies can be viewed as a key component of enhancing Ukraine's economic resilience. At the same time, the effectiveness of this approach is

determined not by the amount of available information, but by the ability to verify, synthesize, interpret, and transform it into an analytical foundation for timely, security-oriented decisions.

Given the multilayered nature of economic security, the use of OSINT research should be tailored depending on the subject of analysis and the nature of potential threats. Unlike the approach in which OSINT is primarily viewed as a universal tool for searching for and processing open-source information, this study proposes structuring its application across three interrelated levels: the enterprise, the institution, and the state. This approach allows us to trace the transformation of OSINT analysis subjects from individual counterparties, owners, and business transactions to complex corporate, financial, institutional, and foreign economic relationships. At the same time, as the level of analysis changes, so does the nature of the threats: from local financial, fraudulent, and reputational risks to a company to systemic threats to the state's economic security.

The proposed systematization of the three levels of OSINT research in the context of ensuring economic security is presented in Table 1.

Table 1. Levels of OSINT research in economic security analysis

Level of OSINT Research	**Key Objects of Analysis**	**Risks and Threats Identified**
Enterprise level	Counterparties, owners and beneficial owners, financial performance, court cases, public procurement, corporate relationships, media environment	Fraud, fictitious business activities, unreliable counterparties, conflicts of interest, financial and reputational risks
Institutional level	Partners, funding sources, personnel and related parties, procurement activities, institutional relationships, regulatory environment	Corruption risks, conflicts of interest, non-transparent relationships, misuse of financial resources, compliance and financial threats
State level	Markets and industries, companies of strategic importance, sanctions, foreign economic relations, international supply chains, strategic and critical resources	Systemic economic threats, sanctions evasion, critical economic dependencies, threats to strategic industries and national economic resilience

Source: developed by the author.

The approach presented here demonstrates that the functional purpose of OSINT varies depending on the level of economic security. At the enterprise level, OSINT is primarily applied in a preventive manner and is aimed at reducing information uncertainty when interacting with counterparties, investors, suppliers, and other participants in business relations. Combining information on owners and beneficiaries, financial condition, legal cases, procurement, corporate ties, and contextual information allows for the creation of a more comprehensive profile of an entity and the timely identification of factors that could negatively impact the enterprise's economic security.

At the institutional level, the scope of OSINT research is expanding to encompass not only individual entities but also the network of their interconnections. Particular importance is attached to the analysis of funding sources, partnerships, personnel and corporate ties, procurement activities, and the regulatory environment. This creates an information foundation for identifying potential conflicts of interest, corruption and compliance risks, non-transparent use of financial resources, and other threats that may affect the stability and effectiveness of an institution's operations.

At the national level, OSINT takes on strategic importance, as the focus of research shifts to markets, industries, strategic enterprises, international corporate networks, sanctions, foreign economic relations, supply chains, and critical resources. In this context, open-source analysis can be used not to identify a single risk, but rather a set of interrelated factors capable of creating systemic threats to the country's economic stability. Thus, there is a logical expansion of the scope of OSINT research following the pattern "entity → system of interrelationships → the country's economic system".

Conclusions. The study demonstrated that OSINT should be viewed not only as a technology for searching for information in open sources, but also as a comprehensive information and analytical tool for ensuring economic security. Its

use involves the systematic collection, verification, systematization, comparison, and analytical interpretation of open data, which makes it possible to identify hidden connections, risks, and potential threats and to form an information basis for making security-oriented management decisions. The paper proposes systematizing OSINT research across three interrelated levels—the enterprise, the institution, and the state—for each of which key objects of analysis and characteristic risks and threats are identified. This approach allows us to trace the transformation of OSINT from a tool for verifying counterparties, owners, and financial and reputational risks at the micro level to a means of identifying opaque connections, corruption and compliance risks at the institutional level, and systemic economic threats, sanctions risks, and critical dependencies at the state level.

References

1. Hayes, D. R., & Cappa, F. (2018). Open-source intelligence for risk assessment. Business Horizons, 61(5), 689–697. https://doi.org/10.1016/j.bushor.2018.02.001

2. Fantinelli, S., & Sivilli, D. F. (2015). Open source intelligence's methodology applied to organizational communication. Mediterranean Journal of Social Sciences, 6(2), 233. https://doi.org/10.5901/mjss.2015.v6n2p233

3. Khan, S., & Wallom, D. (2022). A system for organizing, collecting, and presenting open-source intelligence. Journal of Data, Information and Management, 4, 107–117. https://doi.org/10.1007/s42488-022-00068-4

4. 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

5. Van Puyvelde, D., & Tabárez Rienzi, F. (2025). The rise of open-source intelligence. European Journal of International Security, 10(4), 530–544. https://doi.org/10.1017/eis.2024.61

6. Mihus, I. (2026). Information and analytical support for partner verification in the enterprise economic security system based on international standards. Economics and Management, 1, 35–41. https://doi.org/10.32782/2312-7872.1.2026.5

7. Sidoruk, M. I. (2026). Методика інформаційно-аналітичного документування відкритих джерел у процесі верифікації схем обходу санкцій [Methodology of information and analytical documentation of open sources in the process of verifying sanctions evasion schemes]. Вісник Харківської державної академії культури, 69, 177–187. https://doi.org/10.31516/2410-5333.069.15