Published in the USA
International Journal of Media and Information Literacy
Issued since 2005
E-ISSN 2500-106X
2023. 8(1): 114-121

DOI: 10.13187/ijmil.2023.1.114
https://ijmil.cherkasgu.press

Use of the OSINT-Technologies for Civil Society Institutions

Andrii E. Lebid [a, b, *], Vitalii V. Stepanov [a], Mykola S. Nazarov [a]

[a] Sumy State University, Sumy, Ukraine
[b] Cherkas Global University, Washington, DC, USA

Abstract

The article shows that the use of open data provides new opportunities for improving life and economic growth in communities. Their effective use helps the community to develop, build dialogue and make informed decisions. Data systematization is the basis for monitoring and quality planning at the community level. It has been proven that open data complicates manipulation of the community budget and brings reputational dividends. The asset accounting system is an integral part of automating the processes of collecting, recording, updating and using data on property and other objects of the community. Activists use technology to make authorities more transparent and accountable.

The authors are convinced that open data has naturally reduced the number of requests for public information from city councils, which eases the burden on local authorities and has a sustainable economic effect.

Open data also increases the investment attractiveness of regions. Businesses invest only based on analytics and monitoring of community indicators. Open budget helps to make a choice, as it is a key source of data on the state of the community's financial affairs.

Open data can be used not only to monitor the actions of the authorities, but also to make management decisions. The published data can be used for further community development planning.

Platforms and applications based on open data can improve services in the community. And it does not always require additional resources. To do this, you should first research the market for open data-based tools: what has already been developed and what can be scaled up in your community for free.

In this context, we believe that OSINT technologies are an important tool for monitoring and control, as they help to increase the level of information and media literacy of local residents, as well as their resilience. The importance of using OSINT-technologies and tools for citizens' access to public information, open data and effective citizen participation in communities is shown.

Keywords: open data, OSINT-technologies, public information, basic services, governance, citizen participation, resilience.

1. Introduction

As open data application, the Open Source Intelligence (OSINT) plays a significant role in public control of local and state authorities (Tau, Volz, 2021). Security is another branch to use this tool. Let us sort out how the OSINT works and why it exceeds the military sphere.

The OSINT term comprises search, analysis and use of common information to make certain decisions. The first data processing dates back to the Second World War. In the USA, the Foreign

[*] Corresponding author
E-mail addresses: a.lebid@socio.sumdu.edu.ua (A. Lebid)

Broadcasting Service was established to analyze data from foreign organizations. Since the Internet creation, the key OSINT sources are online ones (including social networks).

The OSINT use exceeds military intelligence. It can concern business processes as well: to analyze counter-agents, competitions or reactions to certain products. Investors and venture funds rely on the OSINT to collect founding and managing data from open sources before the financing project is signed.

Lawyers can resort to the OSINT tools to investigate cases via open data analysis from different social networks and media. The OSINT may be useful in crime investigation: to produce a profile for tracing criminal habits (Adams, 2023). The OSINT contributes to darknet examinations: forums and e-shops are checked to detect illegal commerce. In such a way, we simplify investigations in cybersecurity, cyberterrorism and cyberwars. Here, OSINT may be applied for defense and attack. You may find traffic leaks via these technologies. Besides, the OSINT provides Penetration Tests as an important cybersecurity element.

There are several approaches to the OSINT study. You may attend online courses, read articles and guides, listen to YouTube lectures. The obtained knowledge and skills make it possible to join the OSINT community and conduct civil research.

Obviously, OSINT prospects are going to rise: here, market volume is equal to billions of dollars (OSINT Market Report, 2023). Consequently, the OSINT use will be necessary for business, law, journalism and public to control local and state authorities properly.

2. Materials and methods

To prepare the article manuscript, we analyzed a range of the OSINT tools (sorted by target users, sources, algorithms of data collection and processing, accessibility). Besides, we applied platforms, systems and services that work with open data bases and the OSINT set. The proposed principle of open data collection does not concern the automated systems of information transfer: Social Media and Open Source Intelligence Platform, Intelligence Cloud Platform, OSINT Combine, SocialNet (Social Media Monitoring and Investigations), Open Source Intelligence Monitoring and Alerting, Semantrum, Slidstvo.Info, NashiGroshi etc.

Semantrum is an AI platform for media analytics and reputation management (Semantrum, 2023). Semantrum started as a startup in 2014 with a vision to revolutionise the way we work with unstructured data – text and media. Since then, Semantrum has become a recognisable product in the media monitoring market. In 2022, the Semantrum team launched a standalone analytical product – BrandVox. It is a universal tool for working, analysing and managing social media. BrandVox was also successfully launched on the Product Hunt platform, where it was among the top 10 favourite products of the week. And in May 2023, BrandVox was presented on the world-famous AppSumo platform, where it was highly praised by both company experts and users. Today, Semantrum is actively working and developing in the Ukrainian market, as well as expanding its presence in other international markets

In addition, we analysed OSINT tools and services for collecting information, processing data and conducting investigations based on open sources of information - the Molfar platform. A list of 250 tools for analysing people, websites, emails, images, apps, geolocation and traffic. The list is constantly updated: we remove old tools that have stopped working and add new ones with similar or better functions by search category. All these OSINT tools have been tried and tested by Molfar analysts. We recommend the OSINT services and websites presented on this page for conducting open source investigations. There is no perfect OSINT tool, and there never has been. But systematic mastery of a large number of common tools is the key to success (OSINT Tools, 2023).

Registers of legal entities in different countries of the world. A list of 370 registers in 148 countries for the analysis of legal entities. In the work of OSINT analysts, the analysis of legal entities is critical: legal data contains a lot of useful information that can be used to study the relationship between people, companies and projects with each other. When working with registers of legal entities, you should always remember about the imperfection of information aggregators. That is why when researching, for example, a British company, it is worth checking the data on a legal entity in several registers at once. So, you are much more likely to collect the maximum of valuable information for further processing and use (Entities Registers, 2023).

All useful OSINT tools and resources in one place. We have gathered everything that Molfar researchers use conducting investigations. These OSINT tools will definitely be useful in your work. The registers are constantly supplemented and updated. The OSINT tools presented on our website are proven resources, useful enough to recommend them to the entire Molfar OSINT community. However, let's not forget that these tools are external, so the developer company is responsible for the result of their work. Also note that it is normal when some OSINT tools stop working, and we replace them by others

3. Discussion

In civil, publishing, military and other spheres, the OSINT is a conception to search, collect, analyze and apply open source data. That concerns corresponding methods and tools as well. The OSINT emerged because of military reasons when relevant and common information required processing. Via the OSINT, you can find necessary data and benefit from them. Since its emergence, many researches have been conducted to offer and develop new ways of the OSINT use in different branches (Adams, 2023; Semantrum, 2023; Senekal, Kotze, 2019; Gruters, 2018; Hatfield, 2023; Eldridge et al., 2018; Mugavero Benolli, Sabato, 2015; Rønn, Søe, 2019) and others.

Another top trend in the world is artificial intelligence. However, currently there is a lack of sources to trace the OSINT application combined with artificial intelligence. The OSINT methods are reasonable for case investigations because they are accessible and checkable. Previously, the data protection laws were regarded to contain the free press. However, no studies were conducted to assess influence of such reforms on more common OSINT abilities (Semantrum, 2023).

In the information age of research with open source tools, the OSINT got especially important among investigators. Nevertheless, big data led to many challenges in the OSINT use. In particular, big data consist of large amounts of non-structured data that are generated continuously (Senekal, Kotze, 2019).

As the generally accessible information keeps being codified by the USA Department of Defense, we should reconsider the OSINT concept to apply digital data efficiently. For spreading the OSINT idea, some researchers find it reasonable to professionalize the OSINT defense. They offer the OSINT military specialty, define the OSINT recruitment, record the best OSINT experience, standardize the OSINT defense training, involve experts and amend all corresponding acts of the USA Department of Defense (Gruters, 2018).

Simultaneously, some researchers regard the OSINT as a fundamentally inconsistent conception. That is why it should be rejected in two steps. Firstly, you cast doubt on key criteria used to single out the OSINT as a separate intelligence type among other «conventional» analogues. Secondly, you criticize the OSINT as an outdated concept. It assesses the flow of valuable unclassified information with less advantages, which makes problems for the OSINT itself. Rejecting the OSINT term and resorting to traditional interpretations of open sources, you may benefit conceptually and analytically (Hatfield, 2023).

In the big data age, the potential OSINT value is widely recognized. Today, the progress in this sphere often concerns software to collect, filter, associate and manipulate data automatically. The automation tendency is innovative and necessary. However, technocentric efforts to replace humans with properly developed algorithms (from data collection to their analysis and synthesis) risk restricting rather than enhancing the OSINT potential. Effective OSINT systems should be thoroughly designed to promote complementarity and balance their disadvantages with advantages for the highest benefit (Eldridge et al., 2018).

As a result of modern global dynamics, international intelligence debate shows the revolutionary situation within investigation means. To follow the development pace, these tools should collect and process data via all technological and methodological experiences. Here, intelligence proves to be a key approach for effective reaction to community needs. Actually, the constant interaction between the IMINT, MASINT, SIGINT, GEOINT, HUMINT and OSINT data must provide added value to offer clear, efficient and appropriate products (Mugavero Benolli, Sabato, 2015).

From this perspective, SOCMINT (SOCIAL Media INTelligence) is often regarded as actual and economically effective information. In terms of civil security, use of social network data is mostly unrestricted, which leads to certain ethical challenges for intelligence services. Morality discussions find privacy inviolable in the public space (including the Internet). Therefore, the regular social network shadowing may not only secure but also affect society (Rønn, Søe, 2019).

4. Results

To ensure a proper resilience of local communities, we should develop threat resistance conceptions for people and state in the information sector. Among the main ideas, we can define:

a) media literacy and critical thinking (to understand news broadcasting methods);

b) management of information threats and risks on local, regional and national levels (to detect them and promote Ukrainian narratives via strategical communications);

c) skills at searching, collecting, analyzing, processing and using big data.

Historically, the only effective way of fake prevention is media literacy – ability to sort out information responsibly and objectively. It is systemic coordination between state and civil institutions that is extremely important in this sphere.

One of self-control tools is media hygiene as a means of fake and digital impact resistance. It recognizes negative informational effects via self-study experience (knowledge about media work, alternative news sources and their comparison, etc.).

Here, a key problem is convincing people that they are able to recognize fakes properly for not to become victims. Today, media literacy is developed by state and civil institutions. The former focuses on indefinite recipients, the latter resorts to specific groups of media hygiene (journalists, officials, teachers, public figures).

To prevent informational threats, state authorities should enlighten on media literacy, digital security and system, analytical and critical, thinking (Lebid, Shevchenko, 2020a; Lebid, Shevchenko, 2020b). From this perspective, civil institutions perform a leading role as well: they supervise state and local authorities and raise their performance.

A significant shift occurred in digital security when the conception of external threat resilience emerged and progressed. As a multidisciplinary phenomenon, the resilience issue may concern many aspects of state policy. Informational risks and threats are managed by state strategical communication services.

All these spheres can mutually integrate with the OSINT technologies. Via them, you get more data for proper administrative decisions, forecasts and assessments.

The most important thing for the effective OSINT study is research thinking. Here, it is context understanding, ability to analyze and use of reasonable tools rather than OSINT knowledge that is relevant. Besides, you should consider applying available data within investigations properly.

Before research starts, the OSINT scientist must define achievable purpose with corresponding tasks. It will form a clear strategy, proper OSINT tools and structure of key information search.

Contextual understanding in geolocation is an OSINT core principle. With many geolocation tools, you should understand contextually what tools are necessary to clarify event circumstances and why it is important. If scientists know the advanced search algorithms, they can investigate without specific OSINT tools. Here, gamification is sensible to form and develop geolocation skills. For example, you may resort to the GeoGuessr online game: via Google Street View, you study sites and mark their location. The closer a marked location is to the real place, the more game points you get. This tool is efficient to develop skills of space monitoring and analyzing.

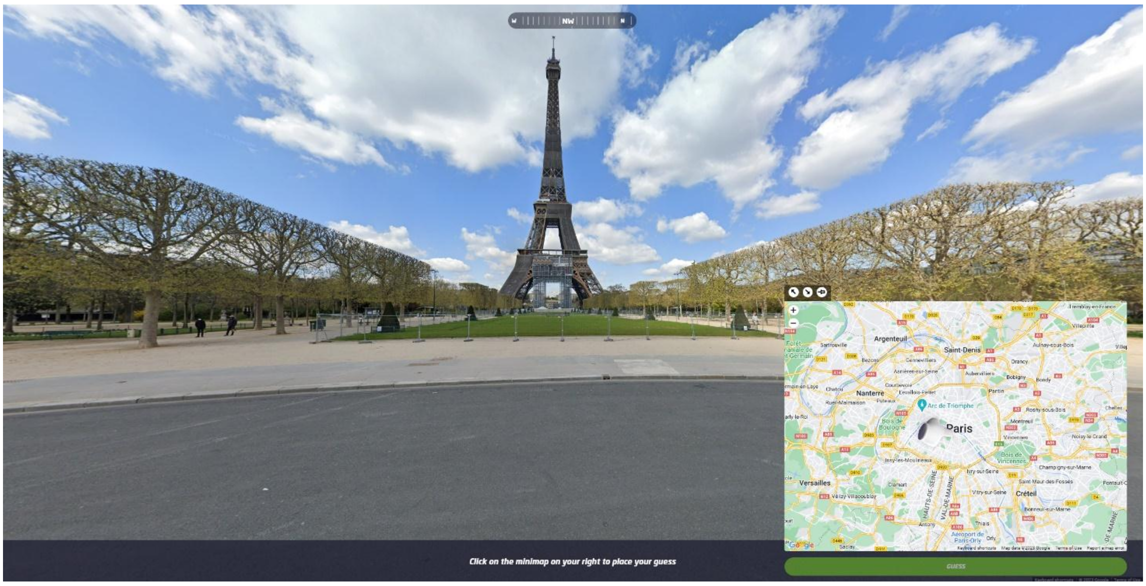
Moreover, other OSINT research means are online communication skills. It significantly simplifies information search when your make a corresponding request to experts or common civilians.

Critical thinking is welcomed for the content media analysis and check (including those in social networks). It is actual because social networks publish much earlier comparing with mass media repost. Such data are valuable for OSINT researchers. However, there may be a lot of fakes for these materials, which requires analyzing them especially critically.

Therefore, research mind set, contextual and critical thinking, OSINT use skills, advanced search algorithms, online communication, etc. produce a real impact for OSINT researchers. The OSINT methodology not only generates new content but also prevents failure within target audiences.

The OSINT work is usually creative. Interested parties not always can interact with the information sphere efficiently, especially in terms of conventional and media wars. The best variant is the OSINT, geolocation and open data use in public, anticorruption, science, etc.

For example, civil society institutions may apply the OSINT techniques for public control of local and state authorities. Here, open data are analyzed to monitor budget costs, to make administrative decisions, etc. The OSINT is reasonable for creating content and realizing communication campaigns (to shift public opinion, inform executive authorities). Also, the OSINT methodology provides security: you can resist the fake information spread properly.



Click on the minimap on your right to place your guess

Fig. 1. Defining geolocation in the GeoGuessr online game (GeoGuessr, 2023)

The main civil society tool is their single opinion that can affect the public attitude itself. Civil society institutions are managed via communication campaign planning. Here, you should consider target audience, purpose and tasks in message boxes, resources, communication channels, etc.

Within the civil sector, message clarity, target audience and opponents' understanding become extremely important. That may be achieved through the OSINT use and open source search.

For the highest performance, we should search, check and arrange open source data by three aspects:

1) public initiative;

2) opponents;

3) allies, stakeholders, change agents.

In terms of management of civil society institutions, it is relevant to collect and accumulate information. Case report is the first document to issue for a public organization or activists in protests or advocacies. Such a paper comprises a challenge, solution and achievement.

There is an optimal algorithm to produce reports in three steps:

1) primary chronological data array (event description: date, organization, human names, link, etc.);

2) data restructuring;

3) storytelling – chronologies (proven histories).

Finally, you get an arranged document with actual developments and their stakeholders. It may be further applied for communication with different influence agents.

To make an opponents' dossier, you should define and rearrange the data similarly to your own case. Roles and threats of each opponent are explained. The main sources about opponents are journalistic investigations and registers. The most famous investigators are such services as Skhemy – a weekly television programme of investigations and analysis on grand political corruption. Investigative journalism and news exposing high-level corruption (Skhemy, 2023), Slidstvo.Info – is an independent Ukrainian investigative journalism agency specialising in investigations of corruption in government (Slidstvo, 2023), NashiGroshi – an investigative journalism programme exposing corruption schemes of Ukrainian officials (NashiGroshi, 2023), Bihus.Info etc.

Bihus.Info is an independent team of journalists and lawyers (Bihus.Info, 2023). They reveal corruption and shadow schemes. Originally called as Nashi Groshi z Denysom Bihusom (in English: Our Money with Denys Bihus), the project started in 2013. Initially, this video program supplemented articles of the Nashi Groshi news site. However, it focused on own investigation topics with separation from the news reading version. Today, episodes are created by the Bihus.Info team. The staff does not depend on broadcasting channels and has been appreciated by many rating agencies.

«Tysny» (in English: Push) is a Bihus.Info initiative to protect unbiased journalism, monitor criminal proceedings and raise law awareness. Kiltse (in English: Ring) is another project on open state databases with flexible access. They are formal and transparent.

If civil entities do not resist opponents (current corruption), their description is limited to history of topic participation and mentioned investigations. When resistance is an important campaign part, the opponent's dossier can be subdivided into sections: career and official decisions, income sources, affiliations, scandals. That can be significantly supplemented with data from registers as well.

The register search hits are arranged logically – from human's name to his companies, from companies to affiliations and lawsuits. Large amounts of businesses and connections may bring new facts. Appropriate registers for investigation start are Clarity Project (Clarity Project, 2023). The system can search for ProZorro procurements and ProZorro auctions, genera by various criteria; find and display information about bidders and the relationships between them; monitor procurements, customers or participants; assess the risk level of each procurement according to a large list of criteria. The system obtains all published information from open public sources in accordance with the Law.

YouControl – is an analytical system for compliance, market analysis, business intelligence, and investigation. The system generates a full profile for every company in Ukraine based on open data, tracks changes in state registers, and reveals links between affiliates. The unique technology allows you to get relevant (at the time of the request) information about the company or the individual entrepreneur from more than 100 official sources. The Monitoring feature reports changes daily, based on data from official sources (YouControl, 2023).

OpenDataBot is a Ukrainian company that provides access to state data from the main public registers for citizens and businesses. Citizens can access debt and court notifications, data verification to protect against fraud, vehicle and real estate checks. Various IT services are being developed on the basis of Opendatabot to protect companies from raider attacks, control counterparties and take care of employees. These platforms are available through APIs in any CRM/ERP systems (Opendatabot, 2023).

Each owner or beneficiary's company provides several investigation ways. On the one hand, you can watch the company record with its affiliations. On the other hand, you may check the judicial register to find any convicted cases. Here, each subject may lead to new investigation stages since they mostly have subsequent relations with other companies.

Table 1. Databases for prompt verification of public information

№	Resource name/Activity description
1	**Dostup do Pravdy** (Dostup…, 2023) The resource operates as a unified platform for sending electronic requests to information holders in accordance with the Law. All requests and responses to them are published on the website and are available to other users
2	**The State Statistics Service of Ukraine** (SSSU, 2023) On the website of the civil service, you can find official statistical information divided into different categories. In particular, there is data on the general activities of the service, the population of Ukraine, and available statistics. There are also targeted categories for the public, respondents and the media
3	**Open registers and databases** (Open registers, 2023) A separate category of the Access to Truth resource includes a list of open registers where it is advisable to search for information when requests are not needed. Among the links include stacks of public information from various state and official and official agencies
4	**Derzhzakupivli.Online** (Derzhzakupivli, 2023) This resource contains a full range of public information on all public procurement. In addition, users are offered opportunities to participate in procurement and to submit proposals to the state in the form of goods or services.This resource is specialised and provides a range of important and relevant information for users
5	**Scanbe.IO** (Scanbe, 2023) Debtors, real estate, courts, wanted persons, offences, business and professional activities,

	etc. This list contains sources that allow you to check any person against open databases. In particular, data on commercial, political, criminal, judicial and other legally dependent affiliation of the subject
6	**Duke Reporters' Lab** (DRL, 2023) The Reporter's Lab is a center for journalism research at the Sanford School of Public Policy at Duke University. This resource has a global database of fact-checking organizations. organizations. It is presented in a convenient form on a world map with points, names and links to the leading fact-checking organizations in different countries. Using this database, you can access information about global events that are analyzed for fact-checking

How may we apply data for communication? Firstly, any opponents' report is necessary for press releases, news columns and social network posts. These reports can provoke active and tense comments, which is typical for protests and advocacies. You should filter such comments via proofs. Secondly, reports can be used to create a Wikipedia article, an opponent's passport, etc.

Case filling, ally and leverage selection are significant as well. Among potential allies, there are activists, journalists, public figures, state and local politicians who share the same initiative values. Their dossiers are usually brief: you do not need to pressure such persons or organizations. Here, the only task is acquaintance and search for cooperation opportunities.

Leverages are state and local subjects responsible for solving problems. They are not active opponents and do not show any motivation to help. It is necessary to have both opponents' and leverage dossiers: lack of motivation makes you influence opponents softly (public addresses and petitions). Leverage dossiers detect pressure points and how to do it properly.

The list of companies is not exhaustive and in no way can be a basis for selecting a monitoring service provider. It is provided solely for information and general impression of the market opportunities. The overview of options is taken from official websites and responses from support services, companies offering demo access. We advise you to to take advantage of this opportunity and test all services to choose the the best solution

5. Conclusion

Therefore, civil organizations actively apply the OSINT techniques to improve business processes. That is achievable via market research when you analyze games, regulators, competitors, customers and suppliers. A more accurate planning enhances business resilience.

Within civil society institutions, OSINT researchers can obtain true and detailed information for administrative decisions. It concerns data on challenges, risks, opportunities and other factors of community development.

Social networks and other sources can track down area brand names and react to current problems of regional development. Civil society institutions get improvement reviews from stakeholders and beneficiaries.

Compliance and security ensure cooperation between partners and counter-agents. Via open data collection, you find out the company reputation and decide whether it is reasonable to cooperate with counter-agents. In social networks and other sources, the OSINT tools are used to detect and prevent potential threats.

Recruitment is also important for civil society institutions. They involve the OSINT technologies to select experts, analysts, volunteers, etc. It can be based on social network profiles, public press releases, publications, etc. You watch them to assess competence, reputation and other influence factors. All these and other activity spheres of civil society institutions are enhanced through the OSINT means.

References

Adams, 2023 – *Adams, S.* (2023). OSINT for Law Enforcement. Electronic Resource: https://cutt.ly/Qwqhpmpn

Bihus.Info, 2023 – Bihus.Info. Anti-corruption journalistic investigations. [Electronic resource]. URL: https://bihus.info/

Clarity Project, 2023 – Clarity Project. Open data analytics system. [Electronic resource]. URL: https://clarity-project.info/about

Derzhzakupivli, 2023 – Derzhzakupivli.Online. [Electronic resource]. URL: https://www.dzo.com.ua/

Dostup..., 2023 – Dostup do Pravdy. [Electronic resource]. URL: https://dostup.pravda.com.ua/

DRL, 2023 – Duke Reporters' Lab. [Electronic resource]. URL: https://reporterslab.org/fact-checking/

Eldridge et al., 2018 – *Eldridge, C., Hobbs, C., Moran, M.* (2018). Fusing algorithms and analysts: open-source intelligence in the age of 'Big Data'. *Intelligence and National Security*. 2018. 33(3): 391-406

Entities Registers, 2023 – Entities Registers. [Electronic resource]. URL: https://www.molfar.global/en/useful-apps-registers

GeoGuessr, 2023 – GeoGuessr. Let's explore the world. [Electronic resource]. URL: https://www.geoguessr.com/

Gonçalves Evangelista et al., 2021 – *Gonçalves Evangelista, J., Sassi, R., Romero, M., Napolitano, D.* (2021). Systematic Literature Review to Investigate the Application of Open Source Intelligence (OSINT) with Artificial *Intelligence. Journal of Applied Security Research*. 16(3): 345-369.

Gruters, 2018 – *Gruters, P., Gruters, K.* (2018). Publicly Available Information: Modernizing Defense Open Source Intelligence. *Special Operations Journal*. 4(1): 97-102.

Hatfield, 2023 – *Hatfield, J.* (2023). There Is No Such Thing as Open Source Intelligence. *International Journal of Intelligence and CounterIntelligence*. 36(3).

Lebid, Shevchenko, 2020a – *Lebid, A., Shevchenko, N.* (2020). Cultivating the skills of systems thinking in the context of fostering the basic and professional competencies associated with media education and media literacy. *International Journal of Media and Information Literacy*. 5(1): 60-68.

Lebid, Shevchenko, 2020b – *Lebid, A., Shevchenko, N.* (2020). Cultivation of the skills of design thinking via the project-based method as a component of the dual model of learning. *European Journal of Contemporary Education*. 9(3): 572-583.

Mugavero Benolli, Sabato, 2015 – *Mugavero Benolli, R., Sabato, S.* (2015). Challenges of Multi-Source Data and Information New Era. *Journal of Information Privacy and Security*. 11(4): 230-242.

NashiGroshi, 2023 – NashiGroshi. [Electronic resource]. URL: https://nashigroshi.org/

Open registers, 2023 – Open registers and databases. [Electronic resource]. URL: https://cutt.ly/ZwqDfgAp

Opendatabot, 2023 – Opendatabot. API with analytics and data. [Electronic resource]. URL: https://opendatabot.ua/

OSINT Market Report, 2023 – Open-Source Intelligence (OSINT) Market Report. Global Market Insights, 2023. 52 p.

OSINT Tools, 2023 – OSINT Tools. [Electronic resource]. URL: https://www.molfar.global/en/useful-apps

Rønn, Søe, 2019 – *Rønn, K., Søe, S.* (2019). Is social media intelligence private? Privacy in public and the nature of social media intelligence. *Intelligence and National Security*. 34(3): 362-378.

Scanbe, 2023 – Scanbe.IO. [Electronic resource]. URL: https://scanbe.io/

Semantrum, 2023 – Semantrum. AI platform for media analytics and reputation management. Electronic Resource: https://www.promo.semantrum.net/

Senekal, Kotze, 2019 – *Senekal, B., Kotze, E.* (2019). Open source intelligence (OSINT) for conflict monitoring in contemporary South Africa: Challenges and opportunities in a big data context. *African Security Review*. 28(1): 19-37.

Shere, 2020 – *Shere, A.* (2020). Now you [don't] see me: how have new legislation and changing public awareness of the UK surveillance state impacted OSINT investigations? *Journal of Cyber Policy*. 5(3): 429-448.

Skhemy, 2023 – Skhemy: koruptsiia v detaliakh. [Electronic resource]. URL: https://www.radiosvoboda.org/skhemy

Slidstvo, 2023 – Slidstvo.Info. [Electronic resource]. URL: https://www.slidstvo.info/

SSSU, 2023 – SSS of Ukraine. [Electronic resource]. URL: https://www.ukrstat.gov.ua/

Tau, Volz, 2021 – *Tau, B., Volz, D.* (2021). Defense Intelligence Agency Expected to Lead Military's Use of 'Open Source 'Data. *The Wall Street Journal*. Dec. 10.

YouControl, 2023 – YouControl. Online analytical system. [Electronic resource]. URL: https://youcontrol.com.ua/