МІЖНАРОДНЕ ПРАВО. ПОРІВНЯЛЬНЕ ПРАВОЗНАВСТВО

UDC 004.056:341.24
DOI https://doi.org/10.32782/2521-6473.2026-3.27

O. V. Batiuk, Doctor of Law, Professor, Leading Researcher at the Research Laboratory for Force Construction and Operational Employment, National Academy of the National Guard of Ukraine
ORCID: 0000-0002-2291-4247

L. Y. Danylivskyi, Senior Lecturer at the Department of Intelligence at the Kyiv Institute of the National Guard of Ukraine, Major General (Retired)
ORCID: 0000-0003-1995-7980

ENSURING INFORMATION SECURITY THROUGH OSINT TECHNOLOGIES: INTERNATIONAL LEGAL REGULATION

The article provides a comparative analysis of the international legal regulation of the use of Open Source Intelligence (OSINT) technologies in the context of ensuring information security. The peculiarities of developing legal mechanisms for the application of OSINT technologies in the United States of America, Europe, and NATO countries are investigated. Key legal acts regulating access to open-source information, personal data processing procedures, the functioning of cybersecurity systems and the use of open information sources in the activities of state institutions and the security sector are identified.

The fundamental principles of the regulatory framework for using OSINT technologies are analysed, including information openness, the legality of data collection and processing, privacy protection, provision of information security, the proportionality of the use of information resources, informational self-determination and respect for fundamental human rights. It is established that the American approach focuses on developing the analytical potential of open sources of information and supporting national security; the German model is characterised by increased attention to personal data protection and privacy, whereas the Polish regulatory system is aimed at ensuring cyber-resilience and implementing European Union and NATO standards.

It is substantiated that the international experience in the legal regulation of OSINT technologies can be used to improve national approaches to ensuring information security, develop legal mechanisms for regulating open data and increase the effectiveness of countering modern cyber threats and information risks.

Key words: *OSINT, information security, open sources of information, cybersecurity, international legal regulation, personal data protection, open data, cybersecurity, state information security.*

О. В. Батюк, Л. Й. Данилівський. Забезпечення інформаційної безпеки інструментами OSINT технологій: міжнародне нормативно-правове регулювання

У статті здійснено порівняльний аналіз міжнародного нормативно-правового регулювання використання технологій відкритої розвідки Open Source Intelligence, (OSINT) у контексті забезпечення інформаційної безпеки. Досліджено особливості формування правових механізмів застосування OSINT-технологій у Сполучених Штатах Америки, країнах Європи та країнах членах НАТО. Визначено ключові нормативно-правові акти, які регламентують доступ до відкритої інформації, порядок обробки персональних даних, функціонування систем кібербезпеки та використання відкритих джерел інформації у діяльності державних інституцій і безпекового сектору.

Проаналізовано основні принципи нормативного забезпечення використання OSINT-технологій, серед яких відкритість інформації, законність збору та обробки даних, захист приватності, забезпечення інформаційної безпеки, пропорційність використання інформаційних ресурсів, інформаційне самовизначення та дотримання фундаментальних прав людини. Встановлено, що американський підхід орієнтований на розвиток аналітичного потенціалу відкритих джерел інформації та підтримку національної безпеки, німецька модель характеризується підвищеною увагою до захисту персональних даних та приватності, тоді як польська система нормативного регулювання спрямована на забезпечення кіберстійкості та імплементацію стандартів Європейського Союзу і НАТО.

Обґрунтовано, що міжнародний досвід правового забезпечення використання OSINT-технологій може бути використаний для вдосконалення національних підходів до забезпечення інформаційної безпеки, розвитку нормативно-

правових механізмів регулювання відкритих даних та підвищення ефективності протидії сучасним кіберзагрозам і інформаційним ризикам.

Ключові слова: *OSINT, інформаційна безпека, відкриті джерела інформації, кібербезпека, міжнародне нормативно-правове регулювання, захист персональних даних, відкриті дані, кіберстійкість, інформаційна безпека держави.*

Introduction. The rapid digitalisation of society, the global integration of information systems and the active introduction of modern information and communication technologies drive a significant increase in the role of information security as one of the key elements in ensuring national, international and corporate security. In the context of a constant increase in the volume of open data, the development of digital platforms, social networks and electronic services, OSINT technologies are gaining particular relevance, enabling the collection, analysis and verification of open-source information for security needs, analytics, countering cyber threats and making managerial decisions. Modern international security challenges, particularly hybrid threats, cyberattacks, information and psychological operations, disinformation campaigns, illegal use of personal data and an increase in the number of cyber incidents, necessitate the improvement of mechanisms for ensuring information security using innovative tools for monitoring and analysing the information space. In this context, OSINT technologies acquire strategic importance as a tool for the early detection of risks, threat assessment and enhancing the cyber resilience of state institutions, critical infrastructure facilities, business entities and civil society.

At the same time, the active use of OSINT technologies brings to the forefront the issue of international legal regulation of activities in the field of collecting, processing and using open data, ensuring a balance between security needs and the observance of fundamental human rights, in particular the right to privacy, personal data protection and freedom of access to information. The diversity of international legal approaches, the dynamic development of digital legislation and the formation of new international standards in the field of cybersecurity require a comprehensive scientific analysis of the legal mechanisms for regulating the use of OSINT technologies.

The aim of the research is the formation of theoretical and methodological foundations for the legal provision of state information security by means of OSINT technologies through the development of the theoretical foundations of information law and the formulation of proposals for improving information legislation.

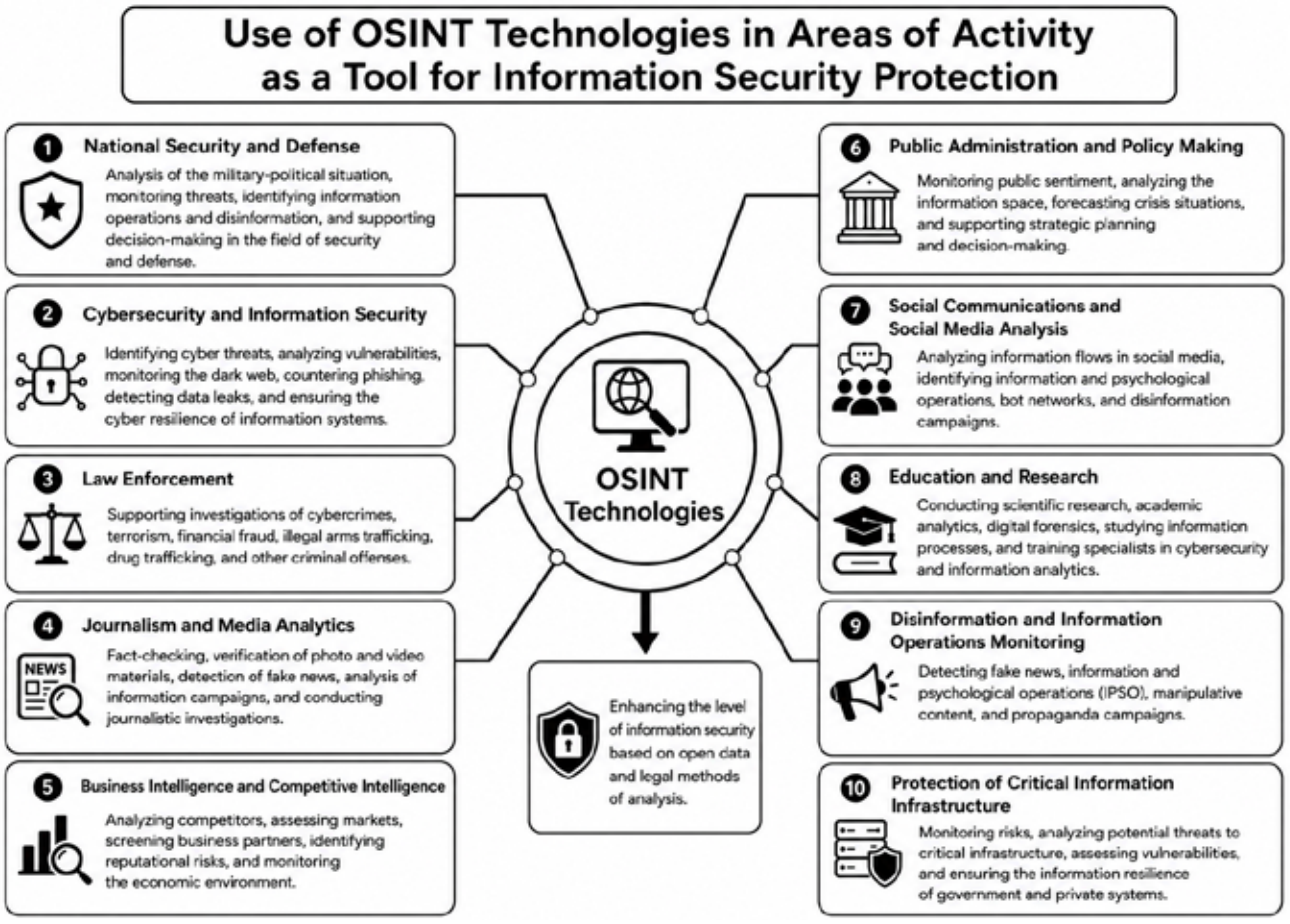

Fig. 1. Use of OSINT Technologies in Areas of Activity as a Tool for Information Security Protection

The outlined aim of the research is connected with solving an important theoretical and practical problem – the development of a conceptual legal framework for ensuring the country's information security and the formation of practical recommendations for improving the mechanisms for its implementation.

The research hypothesis is based on the assumption that ensuring state information security will be effective provided there is properly legalised and the relevant recommendations for improving information legislation are scientifically substantiated.

Literature Review. Numerous scholars have investigated contemporary information security threats, while the issue of ensuring information security using OSINT technologies remains insufficiently explored.

In the scientific article entitled "Information Security: International Legal Aspect", Kovalyov K.E. examines the international legal dimensions of information security. The study presents the results of an analysis of international legal norms regulating the field of information security, as well as relevant foreign practices in this domain. Particular attention is devoted to the significance of the experience of certain foreign states for the development of Ukraine's information security system. Considering the global nature of modern communication networks, the author substantiates the position that effective information security can be ensured exclusively through coordinated international cooperation among states. Furthermore, the research identifies the key priorities and challenges related to information security in Eastern European countries and determines the priority directions for improving the legal framework of information security in Ukraine [1].

In the scientific article entitled "Assessing the Information Security Posture of Online Public Services Worldwide: Technical Insights, Trends, and Policy Implications", Diogo Ribeiro, Vítor Fonte, Luis Felipe Ramos, and Joao Marco Silva investigate the issue of ensuring the security and reliability of electronic public services as a fundamental prerequisite for the effective implementation of Electronic Government (EGOV) initiatives. The study evaluates the state of information security of 3,068 public service platforms operating across all 193 United Nations Member States through non-intrusive technical assessments conducted during 2023–2024. The research focuses on three principal dimensions: the implementation of secure end-to-end communication protocols, the reliability and integrity of digital certificate chains and the exposure of hosting infrastructures to known cybersecurity vulnerabilities. The obtained results demonstrate that, despite some progress in strengthening the protection of online public services, significant deficiencies persist regarding compliance with international cybersecurity standards and best practices. In particular, multiple platforms continue to utilize outdated cryptographic protocols, improperly configured digital certificates and unpatched software vulnerabilities, which substantially increases the risks of cyber threats and unauthorized exploitation by malicious actors. The authors emphasize the necessity of implementing comprehensive cybersecurity policies, conducting proactive security assessments and strengthening mechanisms of regulatory compliance control. Furthermore, the study provides practical recommendations for governmental institutions and system administrators aimed at improving the security of EGOV infrastructures through the elimination of persistent vulnerabilities and the adoption of effective cybersecurity practices [2].

In the scientific article entitled "Implementation of Information Security Management Systems for Data Protection in Organizations: A Systematic Literature Review", Marhad, S. S., Abd Goni, S. Z., and Abdullah Sani, M. K. J. conduct a systematic literature review devoted to the implementation of Information Security Management Systems (ISMS) as an essential mechanism for protecting organizational information resources in the digital environment. The study focuses on identifying the key factors influencing the implementation of ISMS, assessing its impact on data protection processes and analysing the methodological approaches applied in contemporary research. Particular attention is paid to the role of awareness, professional training, and organizational compliance in ensuring the effective functioning of information security systems. The authors emphasize the significance of the ISO/IEC 27001 standard as one of the most widely recognized and effective frameworks for information security management. The results of the study demonstrate that the implementation of ISMS positively affects organizational efficiency, financial performance, corporate reputation and brand reliability. Based on the obtained findings, the researchers substantiate the necessity of applying a comprehensive and systematic approach to information security management within organizations. Furthermore, the study highlights the importance of future scientific investigations aimed at examining ISMS implementation across various organisational environments and industrial sectors in order to develop a more comprehensive understanding of information security practices and their influence on organisational adaptability and resilience [3].

In the scientific article entitled "Information Security Control as a Task of Controlling a Dynamic System", S. Masaev, A. Minkin, Y. Bezborodov and D. Edimichev examine the functioning of a large-scale enterprise as a multidimensional dynamic system within the context of information security management. The enterprise activity is represented through a digital twin model encompassing approximately 1.2 million operational parameters, which enables comprehensive monitoring and analytical assessment of organisational processes. The study focuses on the implementation of a British information security standard based on digital copy technologies, accompanied by the deployment of specialised information security hardware and software solutions, as well as the completion of personnel training programmes aimed at improving cybersecurity competencies. The effectiveness of the implemented measures is evaluated using an integrated performance indicator designed to assess the overall level of information security implementation within the enterprise. The dynamics of this integral indicator are further

utilised to determine the efficiency and practical impact of the introduced British information security standard on organisational security management processes [4].

Methodology. The methodological framework of the study is based on a combination of philosophical (dialectical, metaphysical), general theoretical (epistemological, structural-functional), special (comparative legal, inductive) and cross-sectoral methods of scientific cognition (historical, analytical).

The formal legal method enabled the investigation of the competence of state information security actors, and was also utilised in interpreting legal norms to clarify their essence, content and the legislative intent expressed therein. Structural-functional analysis failitated determining the alignment of the legal acts, underpinning the contemporary system of state information security legal provision with actual public relations in this area and international standards.

Results and discussion. The growing number of cyber incidents, information and psychological operations, disinformation campaigns, information leaks and other forms of hybrid threats necessitates the search for effective mechanisms for detecting, analysing and predicting potential risks in the digital environment. One of the promising tools for ensuring information security is Open Source Intelligence (OSINT) technologies, which are based on the use of open-source information to obtain analytical data, detect threats and support managerial decision-making processes.

OSINT technologies are actively utilised by state authorities, law enforcement agencies, intelligence services, cybersecurity units, analytical centres and the private sector to monitor the information space, detect cyber threats, counter disinformation, ensure cyber-resilience and protect critical information resources.

In the contemporary international environment, the issue of establishing effective legal regulation of OSINT technology use is gaining particular relevance. Various states implement their own approaches to the legal support of activities in the sphere of open-source intelligence, combining the requirements of information security, cyber defence, the openness of state information and legal guarantees for privacy protection. The study of international regulatory experience allows for identifying effective mechanisms for the legal provision for using open sources of information and forming practical approaches to improving the national information security system.

It is worth noting that modern OSINT tools, in particular Maltego, Shodan, SpiderFoot, theHarvester, Recon-ng, Censys, OSINT Framework, SecurityTrails and others, are effective means of collecting, analysing

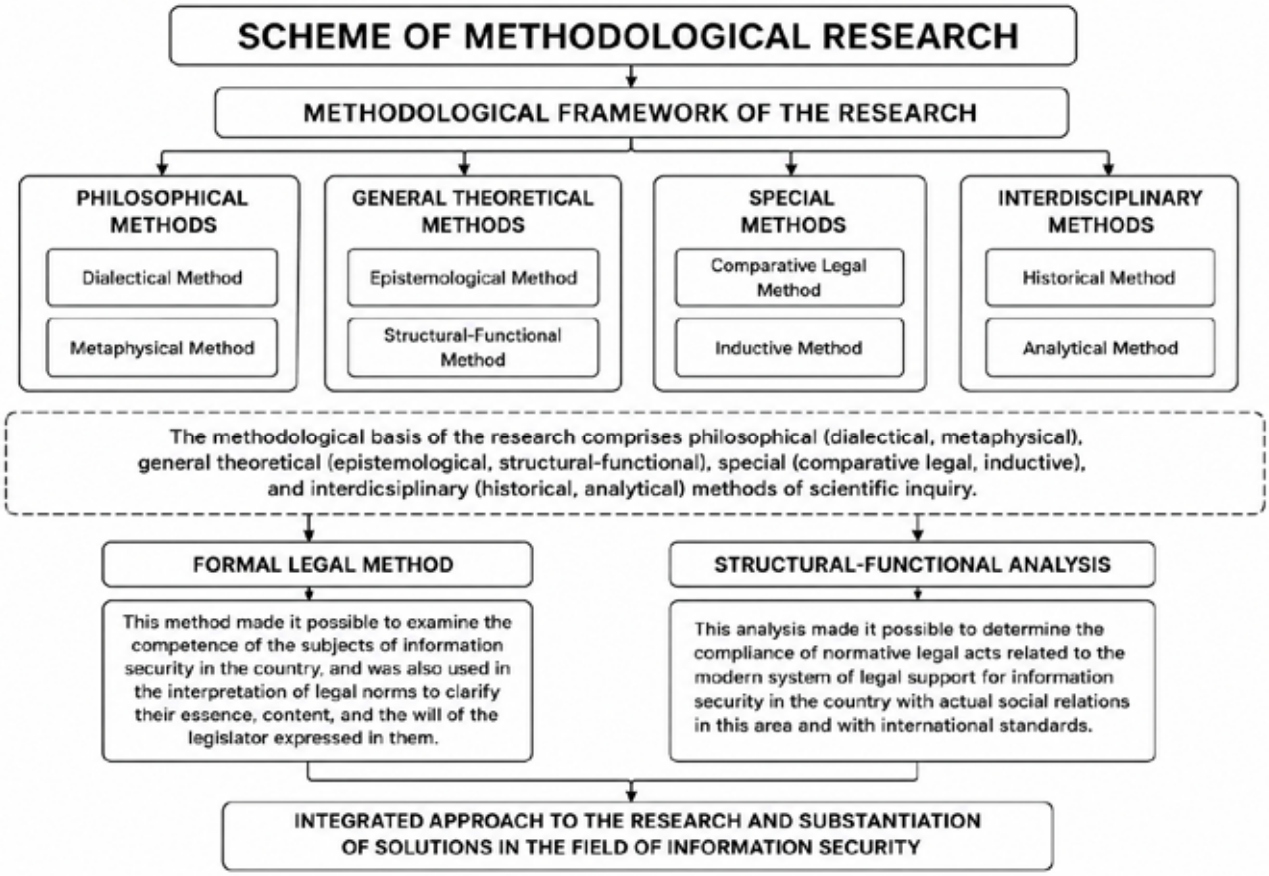

Fig. 2. Scheme of Methodological Research

and visualising data from open sources. Their use contributes to increasing the effectiveness of cyber intelligence, detecting information infrastructure vulnerabilities, monitoring cyber incidents, countering disinformation and ensuring the protection of critical information infrastructure. We consider it appropriate to briefly describe these OSINT tools.

Maltego is one of the most widely used OSINT tools for conducting digital intelligence and visualising connections between entities in the information space. The tool enables the collection and analysis of data from open sources, including domains, IP addresses, email adresses, social networks and organisations. The primary advantage of Maltego is the ability to build graphical diagrams of interconnections between the objects of research, which significantly enhances the effectiveness of analytical activities in the field of information security. The tool is actively utilised for cyber intelligence, digital footprint analysis, cyber threat detection, network infrastructure imvestigation and law enforcement support. In the sphere of information security, Maltego facilitates the timely detection of potential threats and enhances the level of situational awareness.

Shodan is a specialised search engine for detecting devices and services connected to the Internet. Unlike traditional search engines, Shodan indexes servers, routers, webcams, industrial control systems and other devices with a network connection. The tool allows obtaining information about open ports, protocols used, software and potential vulnerabilities in the information infrastructure. In the sphere of information security, Shodan is widely applied for conducting network audits, assessing the attack surface, monitoring critical infrastructure and detecting unprotected systems. The use of this tool allows for the increase of the effectiveness of cyber defence measures and the timely detection of potential cyber threats.

SpiderFoot is an automated OSINT platform designed for the comprehensive collection and analysis of open-source information. The tool supports integration with a large number of data sources and allows for automatically conducting searches for information about IP addresses, domains, email addresses, network infrastructure and possible data leaks. An important feature of SpiderFoot is the high level of automation in intelligence processes, which significantly reduces the information analysis time. The tool is used in the field of cybersecurity to monitor threats, analyse the digital environment, assess vulnerabilities and conduct cyber intelligence. Due to its comprehensive approach, SpiderFoot contributes to increasing the level of information security of organisations and state institutions.

theHarvester is an OSINT tool designed to collect information about domains, subdomains, email addresses and user names from various open sources. The tool actively uses search engines, DNS services, and specialised databases for automated information collection. theHarvester is widely used during penetration testing, cyber intelligence and the analysis of the information infrastructure of organisations. The tool is of particular importance in the sphere of information security, as it allows to identify potentially vulnerable elements of the network infrastructure and assess the level of openness of information resources. The use of theHarvester contributes to increasing the effectiveness of cyber threat monitoring and ensuring cyber resilience.

Recon-ng is a multifunctional framework for web intelligence and open-source information collection. The tool is built on a modular principle, which allows integrating various analysis mechanisms and the automation of OSINT research processes. Recon-ng supports Whois query execution, domain infrastructure analysis, data breach search, social media information gathering and vulnerability assessment. In the field of information security, the tool is used to conduct cyber intelligence, analyse the digital environment and detect potential risks to information systems. Due to its flexibility and broad functionality, Recon-ng is an effective means of supporting the activities of cybersecurity professionals.

Censys is a platform for monitoring and analysing the global network infrastructure, which allows you to search for hosts, domains, digital certificates and network services in real time. The tool provides a detailed analysis of the configuration of network systems and the detection of potential vulnerabilities in the information infrastructure. In the field of information security, Censys is utilised to assess the level of network security, monitor changes in the digital environment and analyse the attack surface. The tool is an important means of cyber intelligence and supporting information security management processes, especially in the field of protecting critical information infrastructure.

OSINT Framework is a specialised online catalogue of OSINT tools and resources, systematised by areas of activity and categories of information. The platform contains a large number of services for analysing domains, social networks, email addresses, data leaks, geolocation and digital footprints. OSINT Framework is widely utilised by information security specialists to organise intelligence processes, select analysis tools and conduct comprehensive investigations of the information space. Due to its structured nature and the broad spectrum of available resources, the platform contributes to increasing the effectiveness of OSINT analytics and the development of cyber intelligence.

SecurityTrails is an analytical service for researching domain infrastructure and DNS records. The tool allows obtaining information about DNS history, IP addresses, subdomains, digital certificates and other parameters of network infrastructure. In the field of information security, SecurityTrails is used to detect suspicious changes in network configurations, analyse cyber threats and monitor the digital environment. The tool is of significant importance for ensuring the cyber resilience of organisations, as it allows the timely detection of potential risks and anomalies in the operation of information systems.

Have I Been Pwned is a specialised online service for verifying incidents of account compromise and personal data leaks. The tool allows users to check whether their email addresses or accounts have been compromised as a result of cyber attacks or information leaks. In the sphere of information security, the service is utilised to assess the risks of personal data compromise, monitor cyber incidents and increase user awareness regarding digital security threats. The use of Have I Been Pwned contributes to a timely response to data leaks and strengthens the protection of information resources.

Google Dorks is a method of using specialised Google search operators to detect hidden, improperly protected or indexed information in the public domain. The technology allows for finding confidential documents, administration pages, open databases and other resources that may pose a threat to information security. In the field of cybersecurity, Google Dorks is used to conduct OSINT research, analyse the digital footprint of organisations and detect potential vulnerabilities in the information infrastructure. At the same time, the use of this tool requires compliance with the legal norms and the principles of ethical use of open-source information.

We believe that the effective use of OSINT technologies requires the further improvement of international legal regulation, the development of interstate cooperation, the harmonisation of information security standards and the training of highly qualified specialists in the field of cybersecurity and digital analytics. In the current conditions of global digitalisation and the growing number of cyber threats, OSINT technologies are becoming a vital instrument for ensuring the information resilience of the state, protecting national interests and supporting international security.

Of particular scientific interest is the investigation of international legal models regulating the use of OSINT technologies in the United States of America and European countries, including members of the European Union and NATO, which demonstrate different conceptual approaches to ensuring a balance between information openness, national security, cyber resilience and the protection of human rights through the use of OSINT technologies.

The legal foundations for the use of OSINT technologies in the USA are formed through a complex of legislative acts and the activities of state authorities. It should be noted that the key legal acts should include:

The Freedom of Information Act (FOIA, 1966), which ensures the right of citizens to access the information of state authorities, creating a legal foundation for the use of open sources of information.

The Privacy Act (1974), which defines the rules for the processing of personal data by federal authorities and restrictions regarding information collection.

The Federal Information Security Modernization Act (FISMA), which regulates information security requirements for state information systems.

Fig. 3. 10-Best OSINT Tools for Information Gathering

The Intelligence Reform and Terrorism Prevention Act (2004), which facilitates the development of analytical activity mechanisms and the integration of open sources of information into the national security system.

The US Intelligence Community Directives, which determine the use of OSINT in the activities of intelligence agencies.

It is precisely the aforementioned US regulations that determine the fundamental principles: the openness of public information; the legality of collecting open data; privacy protection; the proportionality of information use; cybersecurity and interagency coordination.

The legal foundations for the use of OSINT in the Federal Republic of Germany are based on a high level of personal data protection and observance of fundamental human rights, and are established through a complex of legislative acts, which should include:

The German Constitution (Grundgesetz), the articles of which determine the provisions regarding the protection of human dignity, private life and information self-determination.

The Federal Data Protection Act (Bundesdatenschutzgesetz, BDSG), which determines the procedure for processing personal data.

The General Data Protection Regulation (GDPR / DSGVO), the European personal data protection regulation that directly influences the use of OSINT.

The Act on the Federal Office for Information Security (BSI-Gesetz), which forms the system of cybersecurity and information resilience.

The legislation regarding the activities of intelligence services (BND-Gesetz), which determines the legal and technical limits of information collection and analysis.

It is precisely the aforementioned legal acts of the FRGw that determine the fundamental principles: data minimisation, the legality of information processing, privacy protection, informational self-determination and the balance between security and human rights.

It is worth noting that the Republic of Poland is actively developing a regulatory framework for cybersecurity and information resilience, aligning with the standards of the European Union and NATO.

It is advisable to include the following among the main regulatory legal acts of the Republic of Poland that regulate the legal foundations for the use of OSINT technologies in ensuring information security:

The Constitution of the Republic of Poland, which guarantees the right to information and privacy protection.

The Personal Data Protection Act, which implements the European GDPR requirements.

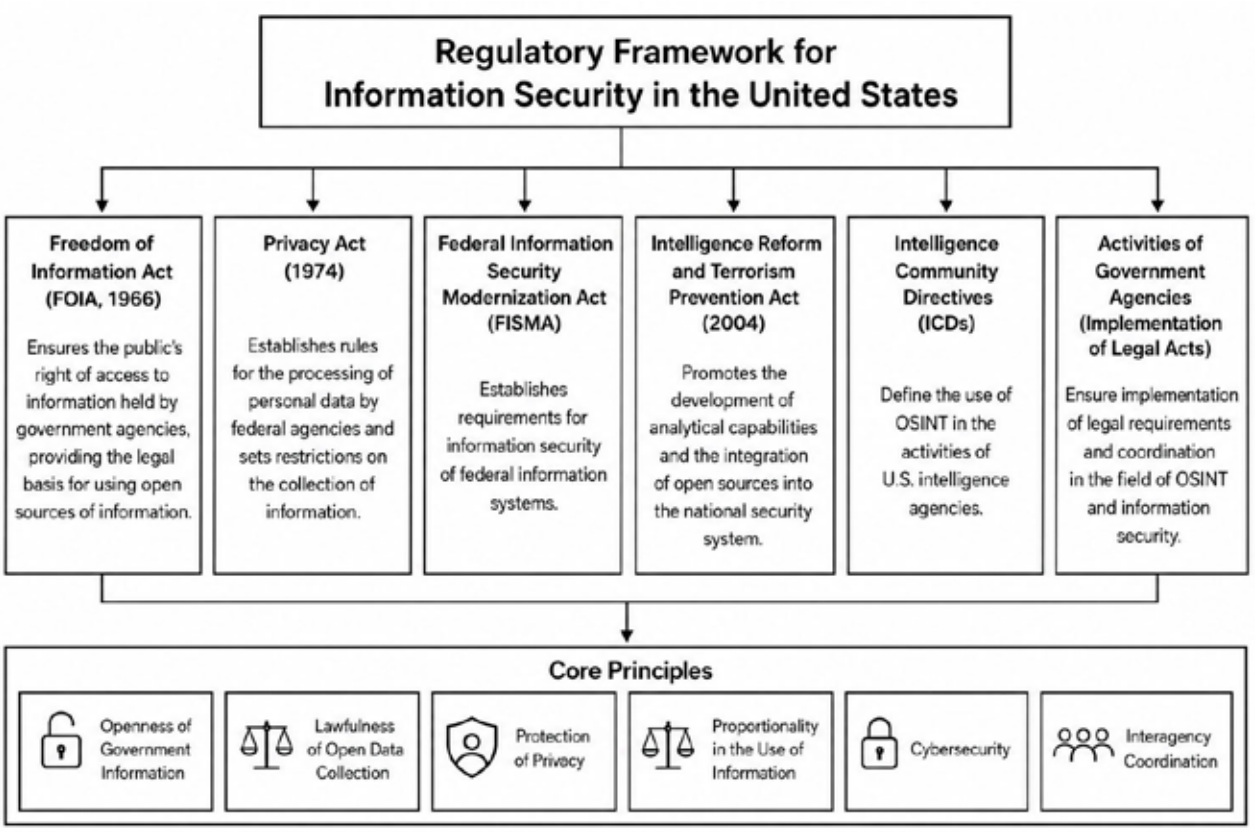

Fig. 4. Regulatory Framework for Information Security in the United States

The National Cybersecurity System Act (2018), which determines the organisational foundations for ensuring cybersecurity.

The Act on Access to Public Information (Ustawa o dostępie do informacji publicznej), which creates a legal foundation for obtaining open data.

As well as a number of legal acts regarding the activities of special services and cyber defense of critical infrastructure in the EU and NATO member states, which should include: Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2 Directive), Directive (EU) 2022/2557 Critical Entities Resilience Directive (CER Directive), Regulation (EU) 2019/881 EU Cybersecurity Act, Regulation (EU) 2024/2847 Cyber Resilience Act (CRA) and Directive (EU) 2016/1148 NIS Directive (first edition).

It is worth noting that the fundamental principles of using OSINT technologies in ensuring information security in the Republic of Poland include: the accessibility of open information, information security, personal data protection, cyber resilience, and compliance with EU and NATO standards.

A comparative analysis of international legal regulation demonstrates that the legal framework for using OSINT technologies in the USA, Germany and Poland is based on a combination of the principles of information openness, personal data protection, cybersecurity and observing fundamental human rights. In this context, the American model is oriented towards the development of the analytical and security potential of open data, the German model towards enhanced privacy protection and informational self-determination and the Polish model towards the integration of cybersecurity mechanisms in accordance with European and Euro-Atlantic standards.

The Swiss Confederation, not being a member state of NATO and the European Union, occupies a distinct position among countries implementing an autonomous approach to establishing an information and cybersecurity system. Despite the absence of formal membership in aforementioned international associations, the state has implemented a series of legal mechanisms oriented towards ensuring a high level of information and personal data protection in accordance with pan-European standards.

An important element of the national system of legal regulation of information security is the Federal Data Protection Act, which has been in force in Switzerland since 1992. This legal act establishes the fundamental principles of processing and protecting information, particularly personal data and categories of so-called "sensitive" information, providing a regulatory foundation for observing the right to privacy and the information self-determination of citizens.

The further development of legal guarantees for personal data protection occurred in 2010, when the Federal Supreme Court of Switzerland strengthened the mechanisms for ensuring the information confidentiality by

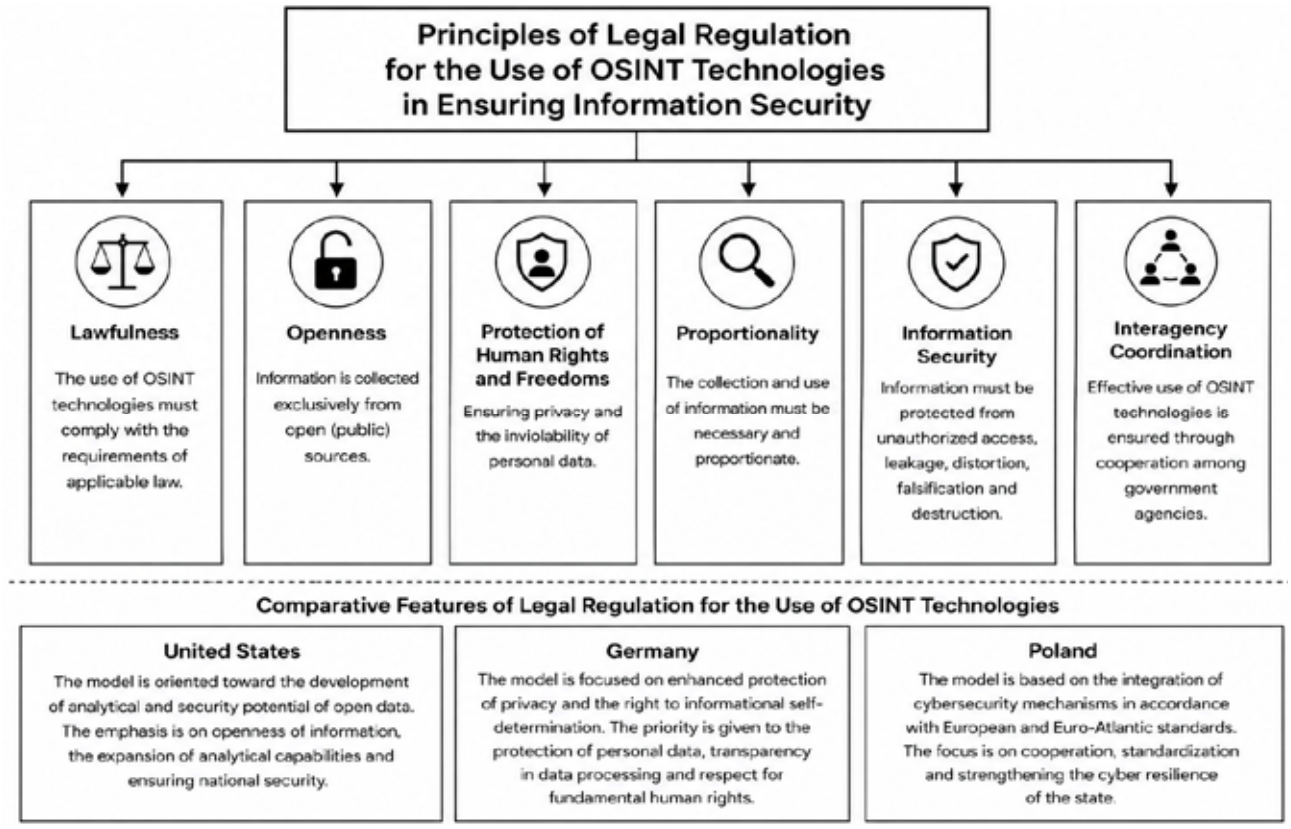

Fig. 5. Principles of legal regulation of the use of OSINT technologies to ensure information security

introducing additional institutional and legal protection instruments. In particular, the activities of authorized bodies in the field of data protection were strengthened, and jurisprudence was established regarding the inadmissibility of the unauthorised collection of information about the IP addresses of file-sharing service users without their consent, including in cases related to copyright protection.

Switzerland's conceptual approaches to ensuring cybersecurity are based on the principles of distributed responsibility and cross-sectoral interaction. The reduction of cyber risks is considered the result of effective cooperation among state authorities, the private sector and civil society, as well as the development of international cooperation. In this context, state intervention in the sphere of cybersecurity is determined by the principle of subsidiarity and is considered appropriate only in the presence of threats to public interests or national security.

Cyber risk management in the Swiss model is considered an integral component of business processes, production activities and managerial mechanisms of organisations of various forms of ownership. Responsibility for the identification, assessment and minimisation of information risks is placed on all levels of management – from administrative and technical personnel to top management. Such an approach implies the formation of a comprehensive cyber risk management system based on the principle of distributed responsibility among state structures, business entities and citizens.

The further development of the national policy in the field of information security received an impetus at the beginning of 2018, when Switzerland began the process of developing specialised information security legislation. The prerequisite for such changes was the recognition of the potentially critical impact of the unlawful use of information and unauthorised interference in information systems on the strategic interests of the state, the functioning of public institutions and the exercise of citizens' rights. It was anticipated that the new legislative mechanism, formed in accordance with international information security standards, would create a unified legal foundation for the coordination, control and implementation of state policy in the sphere of information protection within the powers of the Federal Council of Switzerland.

First of all, the law applies to federal authorities: the Parliament, federal courts, the prosecutor's office, the National Bank, etc. Individuals and enterprises are subjects of the law if they conduct activities involving “sensitive” information on behalf of federal authorities. The Federal Council is also seeking opportunities to deepen cooperation with the cantons, which must be represented in the relevant coordinating body and should participate in the standardisation processes of the respective measures. In particular, the law regulates risk management, classifies information and establishes security principles for the use of IT resources. The information security law is planned to take precedence over freedom of information legislation.

In our opinion, it is also advisable to investigate the experience of ensuring information security using OSINT technologies in European states that are not members of NATO but are also members of the European Union, in particular Austria, Finland and Ireland. First of foremost, it should be noted that EU membership entails for these states the need to comply with pan-European standards in the sphere of information society development, cybersecurity and information protection.

An important stage in the formation of the European information security system was the adoption in 1991 of the Information Technology Security Evaluation Criteria, which defined the main tasks of ensuring information security, namely:

protecting information resources from unauthorised access to ensure the information confidentiality;

ensuring the integrity of information resources by preventing their unauthorised modification or destruction;

maintaining the continuous and stable functioning of information systems by countering "denial-of-service" threats.

The further development of European information security standards occurred in 1996 with the introduction of the Common Criteria for Information Technology Security Evaluation, which became the foundation of the modern certification system for information protection tools.

In Austria, Finland and Ireland, as in other EU member states, significant attention is paid to cybersecurity and countering cybercrime, which is reflected in the European Commission Communication "Towards a General Policy on the Fight against Cybercrime". In the document, cybercrime is defined as a set of criminal offenses committed using electronic communications networks and information systems or directed against such systems. The main forms of cybercrime include:

traditional forms of criminal activity implemented in the electronic environment, in particular fraud and data forgery in electronic communications networks and information systems;

distribution of illegal content via electronic media and digital platforms;

specialised cybercrimes, including attacks on information systems, hacking and other forms of unauthorised interference in the functioning of ICT infrastructure.

At the same time, the main challenges for ensuring the information security of the specified states, as well as the European Union as a whole, remain:

lack of unified approaches to ensuring the security of information infrastructure at the national level, which negatively affects the effectiveness of the implementation of state policy in the sphere of cybersecurity;

insufficient level of partnership between the public and private sectors in the sphere of information security at the pan-European level;

limited capabilities for early detection of and response to cyber incidents, due to the uneven development of monitoring, reporting and international information exchange systems between EU Member States;

lack of a coordinated international approach to prioritising the implementation of critical information infrastructure protection policy.

In this regard, the experience of Austria, Finland and Ireland regarding the use of OSINT technologies within the information security system is of significant scientific and practical interest for Ukraine, especially in the context of developing the national cybersecurity system, improving the mechanisms for monitoring the information space and enhancing the protection level of critical information infrastructure.

It is worth noting that Ireland's National Cybersecurity Strategy for 2019–2024 aimed to improve the state's capacity to manage and respond to cyber incidents, particularly those with national security implications; to identify and enhance the resilience of critical national infrastructure, ensuring service continuity and incident readiness; to strengthen public sector IT systems and protecting citizens' data and services; to enhance education and prepare the workforce for careers in cybersecurity and related fields; to raise cybersecurity awareness and responsibility in the business sector while stimulating research and innovation; to actively participate in international cyber policy efforts and promote a secure, open and stable cyberspace; and to raise cyber hygiene awareness and competences among the general public.

The strategy was developed through a broad stakeholder engagement process that included a high-level steering group and five sector-specific engagement groups, as well as a period of public consultation. The collaborative efforts were aimed at ensuring that the strategy reflected the real needs and problems of the state, its institutions and citizens.

In order to ensure an appropriate level of cybersecurity, the Government of Ireland has identified the following priorities: strengthening the capacity and operational activities of the National Cyber Security Centre; expanding the legal and policy framework to protect both legacy and emerging digital infrastructures; developing a skilled workforce through formal education, internships and public-private partnerships; deepening cooperation between the public and private sectors and exchanging information to manage cyber threats in real time; integrating cyber policy into international diplomacy and governance discussions; fostering an ecosystem where research, entrepreneurship and policy development intersect to create security-oriented innovations; implementing national campaigns to provide citizens with the knowledge and tools to protect themselves online.

Thus, the National Cyber Security Strategy of Ireland demonstrates a comprehensive approach to national security, critical infrastructure protection, public sector IT systems, private business engagement, cyber skills development, raising public awareness and international cooperation. The strategy acknowledges that digital systems underpin everything from financial markets to public services and individual freedoms. Therefore, it is absolutely important to respond to this issue with the participation of the whole society.

The policy framework outlined in this strategy acknowledges the interconnected nature of cyber threats, ranging from individual-level fraud to complex attacks on national infrastructure. It encompasses not only the technical aspects of cybersecurity, but also the social, economic, legal and diplomatic dimensions.

Recommendations. The analysis of international legal acts and strategic documents in the field of information security involving the use of OSINT technologies enables the identification of priority directions for state policy and international cooperation in the specified sphere. The main ones include:

increasing user awareness of potential threats regarding potential threats associated with the use of information and communication networks and digital services;

establishing a European system of early warning and rapid notification regarding new cyber threats and information security incidents;

ensuring appropriate technological support and the development of modern information protection tools;

promoting market-oriented standardisation and certification in the sphere of information security and cybersecurity;

improving legal regulation in the field of personal data protection, providing telecommunication services and countering cybercrime.

strengthening the system of state information security provision through the implementation of effective and interoperable information protection mechanisms, as well as stimulating the use of electronic digital signatures in the provision of public electronic services;

developing international cooperation in the sphere of ensuring information security and cyber resilience.

Based on the conducted analysis, it is appropriate to outline the primary directions of international activity in the field of ensuring international information security with OSINT technologies, namely:

establishing favourable organisational, legal and technological conditions at the national and international levels for the development, production and implementation of modern information security tools, including the integration of OSINT technologies into cyber threat analysis and forecasting systems;

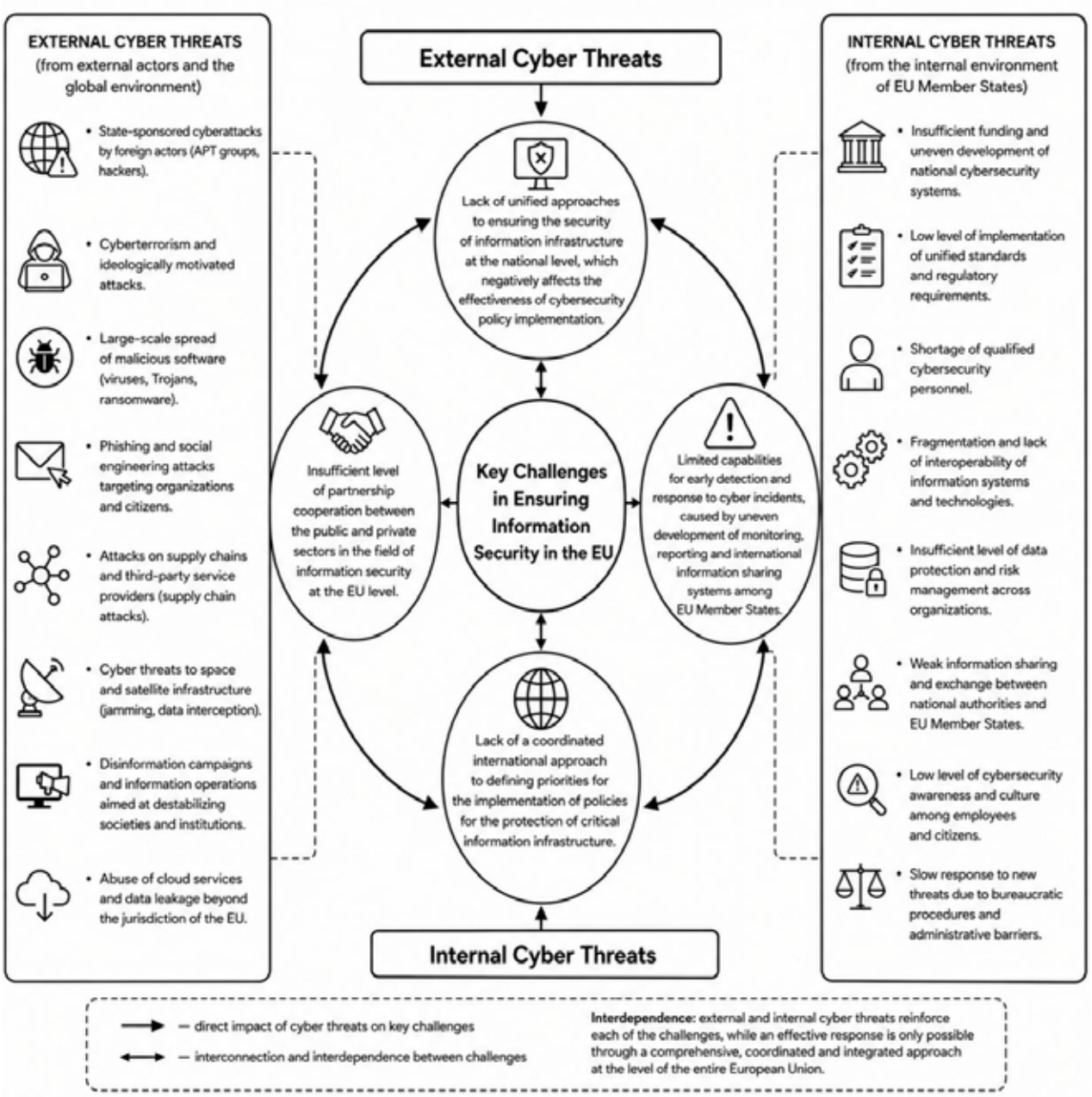

Fig. 6. Key Challenges in Ensuring Information Security in the EU

organising measures for effective international cooperation in the field of information and communication technologies, the exchange of analytical data and the use of open-source information for the timely detection of risks and threats to international security;

coordinating international efforts in the field of countering cybercrime, information terrorism, disinformation campaigns and other forms of illegal activity in the information space involving the application of OSINT technologies for monitoring the digital environment and detect potential threats;

ensuring the protection of information and communication systems from destructive influence, as well as minimising the potential consequences of cyber attacks on information resources and critical infrastructure objects through the use of modern open data analytics methods and early warning systems;

improving personnel provision, methods of professional training of specialists and the development of scientific research in the field of information security, cybersecurity and OSINT-analysis, which will contribute to establishing a high level of professional competence in the sphere of digital security;

implementing international initiatives aimed at preventing conflicts in the information space, countering information and psychological operations and destructive information influence, particularly through the use of OSINT-technologies to detect and analyse information threats;

protecting information, information resources and their processing facilities in order to ensure the effective functioning of complex information systems at all levels of management, including the application of OSINT tools to monitor vulnerabilities and assessing the level of information resilience;

conducting comprehensive scientific research on the use of information and communication technologies, in particular OSINT, in modern conflicts, as well as analysing the application of international law norms to the activities of states in the global information space.

Conclusions. At the current stage of development of the digital society, information and communication technologies (ICT) acquire strategic importance not only for ensuring the socio-economic development of states but also for the implementation of military, political, intelligence and information-psychological operations. The rapid development of digital technologies and the growing dependence of state and non-state institutions on the information environment determine the transformation of approaches to ensuring information security and increase the relevance of using modern analytical tools for the detection, monitoring and forecasting of threats.

In this context, Open Source Intelligence (OSINT) technologies are of particular significance, which provide the capability to collect, systematise, analyse and verify open-source information in order to timely detect risks, assess information threats and support managerial decision-making processes in the field of information security. The application of OSINT technologies allows for increasing the efficiency of monitoring the digital space, detecting signs of information and psychological influence, destructive information campaigns, cyber incidents and other forms of hybrid threats.

The complexity of attribution of incidents in cyberspace, the speed of disinformation spread, the high level of anonymity of information operations and the lack of universal international response mechanisms create the prerequisites for inadequate threat assessment and increase the risks of destabilising individual sectors of state administration and national security. Under such conditions, OSINT technologies act as an important tool for information and analytical support of the cyber defense system and the formation of situational awareness regarding potential information risks.

We believe that among the main contemporary challenges to information security, the detection and analysis of which can be ensured by OSINT-technologies, it is appropriate to highlight:

Firstly, the growing use of ICT in military conflicts, intelligence activities and political confrontation, which necessitates the continuous monitoring of the open information space to detect signs of potential threats.

Secondly, the risks of conducting cyber attacks on critical infrastructure facilities and associated information systems, which requires the application of OSINT tools for early detection of digital threats and cyber risk analysis.

Thirdly, the use of information and communication technologies for criminal or terrorist purposes, including the coordination of unlawful activity, the dissemination of extremist content and the preparation of destructive actions, which brings to the forefront the need to monitor open information resources.

Fourthly, the use of digital platforms for information and psychological influence, disinformation campaigns, propaganda and manipulative information operations aimed at undermining public confidence in state institutions and critically important systems.

Fifthly, the continuous improvement of tools and methods for conducting cybercriminal activities, which requires the development of analytical approaches to detecting new models of cyber threats and mechanisms for their forecasting.

Sixthly, the presence of complex transnational information risks associated with the activities of criminal groups, destructive network communities and other non-state actors using digital technologies to implement unlawful activities.

Seventhly, the use of OSINT-technologies in the information security system allows for increasing the effectiveness of detecting information threats, ensuring a timely response to potential cyber incidents and establishing mechanisms of state information resilience. At the same time, the development of open-source intelligence technologies requires the improvement of international legal regulation and the establishment of unified approaches to ensuring a balance between information security, personal data protection and the observance of fundamental human rights.

Eighthly, in contemporary conditions, international cooperation in the sphere of developing legal mechanisms for regulating ICT and the use of OSINT technologies acquires strategic importance for maintaining international security and preventing destabilising processes in the global information space. The improvement of international legal mechanisms and the development of information analytics tools are important prerequisites for establishing a resilient information security system in the context of contemporary digital transformations.

Bibliography:

1. Ковальов К. Інформаційна безпека: міжнародно-правовий аспект. *Інформація і право.* 2023. № 4(47) С. 159–167. DOI: https://doi.org/10.37750/2616-6798.2023.4(47).291624

2. Diogo Ribeiro, Vítor Fonte, Luis Felipe Ramos, Joao Marco Silva Assessing. Assessing the information security posture of online public services worldwide: Technical insights, trends, and policy implications. *Government Information Quarterly.* 2025. Vol. 42, 102031. Pp. 1–12. https://doi.org/10.1016/j.giq.2025.102031

3. Marhad S. S., Abd Goni S. Z., & Abdullah Sani M. K. J. Implementation of Information Security Management Systems for Data Protection in Organizations: A systematic literature review. *Environment-Behaviour Proceedings Journal*. 2024. 9(SI18). pp. 197–203. https://doi.org/10.21834/e-bpj.v9iSI18.5483

4. Масаєв С. Н., Мінкін А. Н., Безбородов Ю. Н., Едімічев Д. А., Салал Ю. К. Контроль інформаційної безпеки як завдання управління динамічною системою. *Журнал фізики: Серія конференцій, том 1679, Кібернетика та IT.* 2020. № 1679(3). С. 1–6. IOP Publishing. URL: https://doi.org/10.1088/1742-6596/1679/3/032012

Дата першого надходження статті до видання: 10.07.2026
Дата прийняття статті до друку після рецензування: 27.07.2026
Дата публікації (оприлюднення) статті: 15.09.2026