UDC 35.078.3:342
DOI: 10.32518/sals1.2023.49

Соціально-правові студії. 2023. Т. 6, № 1
Social & Legal Studios. 2023. Vol. 6, No. 1

Methodological foundations of information security research

Serhii Yesimov*
PhD in Law, Associate Professor
Lviv State University of Internal Affairs
79000, 26 Horodotska Str., Lviv, Ukraine
https://orcid.org/0000-0002-9327-0071

Vitalina Borovikova
Scientific Researcher
Lviv State University of Internal Affairs
79000, 26 Horodotska Str., Lviv, Ukraine
https://orcid.org/0000-0003-4401-4562

Abstract. The lack of an established approach to methodological research in information security determines the further development of scientific knowledge and changes in paradigms and becomes especially relevant considering the aggression of the Russian Federation and the need to strengthen the information security of Ukraine. The purpose of this study was to identify the principles of information security research methodology. To fulfil this purpose, general philosophical methods of investigating legal phenomena were applied, namely the analysis of corresponding legislation and theoretical solutions. This paper, considering the latest theory of state and law and information law of Ukraine, considering the current legislation and regulatory requirements of the European Union, outlined abstract and logical aspects of the methodological foundations of information security research in the context of digital transformation and Russian information expansion. It was noted that addressing the topic of interdisciplinary research is closely related to a fundamentally new historical situation, which reveals the construction of information relations of a new type between social groups, covering philosophy, political science, sociology, economics, and law. This study considered the activity-based, system-structural, system-functional, informational, integration, predictive, methodological, and paradigmatic scientific approaches to the study of legal phenomena. It was indicated that information security is of particular importance for the design of innovative social systems in the context of digital transformation, which requires further scientific research on the methodology of scientific intelligence in information security. The study was aimed at improving the research methods of information security and protection of individuals, society, and the state from destructive informational influence covered by the object of information security

Keywords: information protection; information destructive influence; interdisciplinary research; principles; digital transformation

Introduction

A natural consequence of the movement of humanity towards a democratic, legal state based on the recognition of the security of the individual, society, and the state as the highest value was the consolidation of the idea of human rights in the public consciousness. It is natural that information security stands out in the complex of tasks of state and legal construction facing society. The development of the information society in Ukraine has led to positive opportunities and adverse consequences manifested in various areas of community functioning, including in the information space. An essential component that ensures the effective genesis of the information community is information security, it belongs to the sphere of influence of national security as one of the main elements. All types of security that form the national security system (economic, military, state, transport, etc.) have an information component, and therefore improving information security is an important area of state activity.

The term "information security" is multifaceted and is considered by modern researchers from the perspective of various approaches. The subject under study is multifaceted. Information security through the lens of philosophy was considered by K.V. Zakharenko (2021), historical events – by

Suggested Citation **Article's History**: Received: 4.01.2023 Revised: 28.02.2023 Accepted: 29.03.2023

Yesimov, S., & Borovikova, V. (2023). Methodological foundations of information security research. *Social & Legal Studios*, 6(1), 49-55. doi: 10.32518/sals1.2023.49.

*Corresponding author

V. Smolianiuk (2021), political realities – by V.O. Babina and I.V. Kudlai (2022), K.V. Zakharenko (2021), jurisprudential areas – by M.V. Baran (2021), O.M. Boiko (2021), international relations – by V.P. Kononenko *et al.* (2021), O.V. Pyrozhyk (2021) and others. Ideologically, all approaches are based on the information security strategy of Ukraine (Decree of the President of Ukraine No. 685/2021…, 2021).

The concept of information security is formed by the set of proportionally balanced rights of society, the state and the individual, the state of protection of the informational interests of the state. The information sphere combines the community of information, subjects, and information infrastructure, which ensure the production, collection, distribution, generation, and application of information as a mechanism of influence on emerging social relations.

The state of economic, political, military, and other components of a country's security also directly depends on the situation in the information industry. During the improvement and transformation of the legal and political system, the modernization of all spheres of life to enter the European legal space, security issues become particularly important. To find an answer to the difficult tasks facing Ukraine, we need the latest paradigm of the content and degree of information security, especially during martial law, which was introduced after the armed aggression of the Russian Federation against Ukraine. In the science of information law, a certain algorithm for analysing the problems of legal support of information security has developed. It makes provision for the definition of the conceptual framework in the analysed sphere, the place and role of information security in the national security system (Doronin, 2020), the establishment of national interests in this area, coverage of the content of the principles, tasks, and functions of information security, characteristics of the system of legal regulation of public relations in the sphere under study.

In multidimensional research, there is a need not only for a standard scientific abstraction from partial to essential characteristics of legal phenomena, but also for a special combination of their diverse aspects within the framework of a practical task or theoretical construction. To develop methodological tools for analysing information security, it is necessary to factor in the disciplinary research approaches that have developed in this subject area. The purpose of this study was a comprehensive theoretical substantiation of the methodological framework for the information security research in information law, which is necessary to improve the norms of information law in the specified area. Fulfilling this purpose depends on the implementation of tasks that lie in the investigation of the main methodological approaches to information security research in the context of digital transformation. To achieve the purpose of this study, the methods of investigating the objective reality and cognition were used comprehensively and systematically: general scientific and private scientific one, aimed at substantiating the prerequisites and principles of research and determining the hierarchy of priorities and values in information security research.

The methodology of scientific research on information security is the subject of scientific research of the following scientists. A. Althonavan and A. Andronache (2018) reviewed general aspects of the information security research methodology. L.V. Lytvynova (2021), T.P. Afonchenko *et al.* (2020) revealed the essence of interdisciplinary research in law. T.S. Perun (2017), S.H. Onopriienko (2021), T.V. Mikhailina and Yu.V. Gotsulyak (2021) considered the methodology of information security in the context of philosophical approaches. Ye.V. Bilozorov (2021; 2022) studied the methodological and activity approach as a tool for cognition of law. The studies by M.N. Kurko and S.V. Didenko (2021), O.M. Balynska and V.A. Yashchenko (2018), O.H. Danilian and O.P. Dzoban (2019) covered the methodology of modern law. H.M. Hulak (2020), M.V. Kovaliv *et al.* (2022) revealed certain aspects of the study of information protection and protection of individuals, society, and the state from destructive informational influence. M.Yu. Osadchuk (2017), V.B. Hdychynskyi (2019) investigated certain approaches of methodology in law. S. Wendzel *et al.* (2022) revealed certain aspects of the information security research methodology in the context of the modern development of information and communication technologies.

General methodological approaches to ensuring information security

The information security methodology should be considered as the basis of theoretical knowledge methods that form the structure and orientation of research. In this case, the methodological function of science is its role for private or interdisciplinary sciences. The theory of state and law exists as a fundamental science in relation to special sciences, for which knowledge of objectively natural and essential things in the state and law serves as a theoretical basis for developing their own means of cognition. The methodology of legal science for information security research contains certain sections that are closely interrelated. The basis of these sections is the philosophical method, to which the methodological principles of jurisprudence, the main provisions and categories of legal science, which represent the formulation of categories of legal reality, relative to information security in the information space of Ukraine, their value is contained in the dialectical-materialistic method, but is expressed indirectly through generally accepted foundations of jurisprudence.

The philosophical method helped obtain the principles of cognition of legal phenomena, general categories of methodological significance for the information security research. This method is based on materialistic dialectics, the application of its laws and categories to the cognition of state-legal phenomena forms the essence of methodology in jurisprudence, specifically in information law. The essence and content of information security cannot be fully covered as a result of analysis alone, separated from other social and legal events and facts. Information protection and protection against destructive informational influence are objects of information security, interconnected and mutually determined by social relations on which the law acts, through the will of the majority of political forces, the tasks facing the law, the historical prerequisites for the operation of the law, between the public and private interests, which are shared very conditionally. All specified methods were used comprehensively. The study of information security in dynamics, progressive movement helps to objectively establish a true picture of the functional state of the legal security system, to see the transformations generated by the changes that occur in public relations regulated by law.

When investigating an object, especially one as complex as the socio-legal phenomenon of information security, the methods of scientific cognition become crucial. Their significance is enhanced by the discovery of new types of scientific

rationality. Until recently, the underestimation and even indifference to theoretical and methodological issues inherent in a fairly significant part of the scientific community turns into the category of anachronisms that hinder the growth of scientific knowledge.

Therefore, at present, the imperative requirement of a scientist's self-reflection on the basics of search and research activities, including ideological and axiological aspects, is becoming normative for scientific research. Furthermore, methodology, along with any other category of scientific cognition, is a dynamic cognitive education and cannot be transformed into any system of knowledge about the principles and methods of scientific search. Otherwise, it will turn into a conservative system of complete knowledge and will be unable to perform the functions assigned to it.

From the standpoint of classical scientific rationality in science, including law, the choice of the method of cognition is determined by the specifics of the object of research that is highlighted and investigated, and the focus on solving a certain research problem. The study of an object is optimally effective only if it is carried out according to the requirements of a methodology that factors in the specifics of the object, and therefore, ways, methods, and means of its cognition. Information security research is a new area of theoretical research carried out in the context of various humanitarian, social, socio-political, and technical disciplines, i.e., it is an interdisciplinary study, which requires its own methodological interpretation. The difficulties of methodological analysis are conditioned upon the fact that it is necessary to factor in the changing formats of information technology development, the development of the post-industrial and information society.

Research approaches used within interdisciplinary areas, such as the information environment approach, the systemic approach (presentation of the systematicity of a new type of information society), the integrative approach (the synthesis of various ideas about information interaction and the integration of this concept into the theory of information security), ideas about the level scientific knowledge, which involves the identification of the substantive level (procedural and material in the legal aspect of the presentation of the object of research), the conceptual level (generalization of the object of research in the subject of research), technical and technological levels – do not give rise to a single scientific plane of research. The richness of terminology in information technology, information security, or cyber threats is an advantage. However, when the theoretical legacy varies between different definitions and meanings of the same term, it creates confusion and value is lost (Althonavan & Andronache, 2018).

The essence of the interdisciplinary approach is that this approach does not express a synthesis of various disciplinary principles, methods, and concepts. The interdisciplinary approach as a research methodology includes general principles, general scientific and private scientific methods and concepts that cross the boundaries of particular scientific disciplines and transcend these particular disciplines in terms of their marginal generality. Accordingly, such a research methodology is called an interdisciplinary methodology precisely because it is built on top of particular methodologies. This is what sets the integral system unity, epistemological certainty, methodological integrity, and completeness of the study.

The multidimensional nature of the object of information security research in the context of information security and protection of the individual, society, and the state from destructive informational influence implies study in the cross-section of different fields of knowledge: philosophical (Kononenko *et al.*, 2021), historical (Smolianiuk, 2021), political (Babina & Kudlai, 2022; Zakharenko, 2021), legal (Baran, 2021; Boiko, 2021), international (Kononenko *et al.*, 2021; Pyrozhyk, 2021), and other sciences. Each of the branches of knowledge can contribute to the knowledge of information security as an object of research in its own way.

Social engineering approach to strengthening information security

According to L. Lytvynova (2021), to analyse information security as a dynamic semantic mechanism of influences, scientific intelligence should represent a multi-level open model, consider the dynamic difficulties of genesis and, as a rule, should be investigated through the lens of social development. Information security is a multidisciplinary concept that is part of sociology, communication theory, philosophy, public administration (Panchenko, 2020), information theory, political science, social and general psychology, etc. Consideration of the concept of information security in the context of the protection of information and individuals, society, and the state from destructive informational influence in the scientific research of scientists suggests the dominant trend of modern science, which lies in the scientific analysis of information security within the framework of separate areas of science (Lytvynova, 2021).

Isolated consideration of the same issues within individual disciplines does not give the effect that can be achieved with the interaction of special knowledge. Interdisciplinary synthesis of knowledge is aimed at combining efforts to jointly solve scientific and applied problems for the effective implementation of information security.

Although the term "interdisciplinary approach" in modern scientific discourse does not have clear conceptual boundaries, the phenomenon itself involves the joint study of interdependent aspects of a widespread problem when researchers attempt to build a common perspective (Afonchenko *et al.*, 2020). According to T.S. Perun (2017), to analyse the level of "information security, it is possible to take such categories of dialectics as possibility and reality, form and content, essence and phenomenon, space and time, whole and part, etc. It is also possible to use the laws of dialectics: on the unity and struggle of contradictions; on the transition of quantitative changes to qualitative ones; on negation, etc."

S.H. Onopriienko (2021) notes that the methodological foundations of information security research are based on the multidisciplinary nature of this category. The application of private law and public law procedures to the study of information security allows developing the system and complexity of innovative academic knowledge.

In the context of an interdisciplinary approach, information security research singles out general scientific elements of the method of cognition: deduction and induction, synthesis and analysis, classification and abstraction, modelling and analogy, including such methods as synergistic, instrumental, systemic, etc.; methods (approaches) of learning law characteristic of jurisprudence: normative-analytical, dogmatic, comparative legal.

The use of a systemic and instrumental view of the object of scientific cognition of information security, consideration of its construction from the inside as a monolithic system is

caused by the desire to highlight systemic matter and the nature of the object under study – information, the definition of which is given in the Law of Ukraine "On Information" (1992).

As noted by T.V. Mikhailina and Yu.V. Gotsulyak (2021), the instrumental alliance of methodological knowledge, as opposed to the theoretical worldview, differs in architecture and is formed through the interaction of more accurate, "neutral" in terms of its meaning, methods that perform the functions of "technical" cognitive techniques and tools during research. The functional-instrumental approach to the scientifically argued methodology of conducting cognitive practice requires a combination of inherently diverse knowledge about the legal purpose of information security, legal norms that provide legal opportunities to ensure protection, the originality of the activity of legal entities to generate and use legal methods.

According to Ye.V. Bilozorov (2022), an important method of ensuring the effectiveness of law, overcoming the ossified legal reality, is an effective legal theory. It can be a method of interpreting the phenomena of law due to their dynamism, which should correspond to the relations governed by legal norms.

An idea about the methodology in the field of information protection, as a complex mechanism of interaction of various categories within the practical and theoretical level of law enforcement and law-making activity, was formed from a review using system-structural, activity, system-functional, etc. approaches.

From the standpoint of the study by M. Kurko and S. Didenko (2021), systematic approach occupies a prominent place in the methodology of information security research. A positive point of the system approach in the study of information security is the prospect of considering the dynamics of systems, which provides favourable conditions for comparing heterogeneous items in a single object.

The functional approach allows considering the direction of pressure at the time of implementation of the national policy in the field of security. In this case, as noted by O.M. Balynska and V.A. Yashko (2018), the structural and functional approach allows outlining the internal model (structure) of a person's implementation of any behavioural act at the total level.

From the general system of methodological provisions of jurisprudence regarding research in the information sphere, it is advisable to apply approaches to the study of information security in the context of information security and protection of individuals and society from destructive informational influence: situational, informational, integration, prognostic, methodical, paradigmatic.

Research of situations that arise in legal practice includes the need to use them in processes related to strengthening information security. A detailed review of various opinions on this topic and the formation of a general understanding of situations related to the strengthening of information security is contained in the literature sources (Hulak, 2020; Kovaliv *et al.*, 2022).

The information approach to research in the field of information security is present as a necessary epistemological category. The implementation of the information approach in information security contributes to the development of techniques and methods for analysing objects that provide an opportunity to demonstrate the informative value of features in quantitative terms.

In the context of the study by M.Yu. Osadchuk (2017), integration approach provides an opportunity to analyse the mechanism of the process of strengthening information security as a system that determines the establishment of information security and protection from destructive informational influence at two levels: private and general. The private level, which determines the procedure for establishing individual facts, is a priority for ensuring information security and affects the development and use of administrative legal techniques in relation to them.

Natural law paradigm of information security

The methodological approach as an element of the natural law paradigm determines the probable structure and procedure of actions to obtain the desired result, is observed within the framework of the legal ordering of information rights.

The methodological method, approach is an independent element of the epistemological toolkit of modern legal science; although it requires complex use simultaneously with other methodological elements, it is advisable to use it to investigate strengthening information security in the context of a paradigmatic approach (Bilozorov, 2021).

During information security research, it is advisable to use an evolutionary approach, which is possible through the formulation of theses that should underlie the evolutionary approach to the study of law:

- any phenomenon of objective reality arises as necessary, considering the already existing phenomena that change (evolve) over time, do not exist by itself, but are connected with others, forming objective patterns (mechanisms), as well as interrelated and subject to evolutionary change;
- categories (in this case, "information security"), being a reflection of the phenomena of objective reality in the human mind, can evolve independently within the limits set by objective reality;
- categories (components of the information security object) can give rise to new categories, which, in case of certain favourable circumstances, can become phenomena of objective reality;
- conscious and unconscious higher nervous activity as a phenomenon of objective reality is included in objective laws, as well as human-created phenomena of objective reality, specifically, such as information security;
- the objective regularities are the most "rational" (elementary) and represent the simplest algorithms, in this connection, the evolutionary process is carried out in the simplest and easiest way, as can be seen in the transformation of information security to protection against information that creates a destructive informational influence on a person, society, and the state;
- the basis of evolution is adaptability, so evolutionary change can represent, from the standpoint of a person, not only progress, but also regression (in this case, this refers to the fact that information security measures restrict human rights in the information space);
- given that social norms are a phenomenon of objective reality in this regard, they are subject to evolutionary changes, are included in objective laws (mechanisms). It is impractical to evaluate evolutionary processes from the perspective of compliance with social norms;
- it is necessary to assess the consequences of evolutionary processes occurring in society from the standpoint of

compliance with social norms, since they are one of the tools for influencing these processes, allowing them to be adjusted in the direction desired by society.

According to V.B. Hdychynskyi (2019), the system of concepts and ideas about law reflects the true reality, determined by the choice of the object of scientific research by members of the scientific legal community and is based on legal values, stereotypes, norms of legal ethics, principles, guidelines, a set of views, etc.

The analysis of the doctrine and industry legislation within the framework of the paradigm approach from the perspective of information security helps to consider industry regulation from a different perspective and outline both the way to implement and specify security measures and identify factors that justify the choice of certain legal protection tools.

The principal functions of legal science are generally recognized as practically applied, predictive, educational, theoretical, and cognitive (Danilian & Dzoban, 2019). The paradigm implements general ideas about the future. The paradigmatic approach to research in the field of information security is directed towards the study of legal reality in dynamics and can be applied to characterize various, including equivalent, variants of the genesis of the practice and legislation of the application of law (Wendzel *et al.*, 2022). The predictive and methodological functions of law are interdependent. The use of a paradigmatic approach within the framework of theoretical legal research on information security should be selective in nature and factor in the priority institutions of law for socio-economic development, in this case Ukraine.

The methodological matrix of information security research includes:

- principles: the principle of consistency, according to which the formulation of the basic concept (information security of a person in the information age) is based on identifying a variety of system connections of all structural and functional components of individual-personal, socio-psychological, socio-group, social, and civil existence of a person in the information age;
- the principle of evolution, according to which information security, having a systemic quality, has the ability to self-develop, including vectors of social dynamics;
- the system principle of integrity, according to which information security in the context of digital transformation constitutes an integral system of interrelated properties of its constituent elements;
- the principle of multifactoriality and multifacetedness, according to which information security in the conditions of digital transformation is expressed in the aggregate unity of individual-personal, social-psychological, professional-activity, spiritual-creative, moral, aesthetic, social-group qualities of a person.

When investigating information security objects in the context of digital transformation and countering Russian information expansion, the legislator should foremost factor in the social conditionality of legal regulation, the value of certain public relations, their role, and significance for the entire system of public relations in the information space. Improving the level of information security will be effective if it is socially determined. Therefore, the study of social conditionality of information security should be considered the primary factor, the basis for effectiveness. Even though the norms of information law, which determine the areas of strengthening information security, as the norms of all other branches of law, are consolidated in the legislation as a result of conscious human activity, their origins should be sought in the laws of social development. This guides the researcher.

The direct basis of the methodology of information security research is the social need to protect a certain group of public relations. The study of Information Security is reduced to objective laws in social development, when there is a need to protect public relations that have become particularly significant and valuable to society at the appropriate time stage.

The concept of social Predestination is overly broad and comprises many objective factors, which together are indicators of the need to investigate information security in the context of digital transformation and the influence of factors of information confrontation with aggressors.

Conclusions

Information security, as a component of national security, requires further comprehensive theoretical justification of the methodological basis to improve the norms of information law, which relate to increasing the degree of protection of information security, considering the specific features of the present. The considered methodological approaches to the study of information security in the conditions of armed aggression of the Russian Federation and the process of forcing digital transformation lead to new approaches to the research methods of information protection, protection of the individual, the state, and society from informational harmful effects outlined by the object of information security.

Methodology, by its very nature, is not just a sustainable system of scientific cognition, since this would mean termination of its development. The dynamism of this cognitive formation is beyond doubt, it is determined by the specificity of the object and is considered by factoring in the social development. A multidisciplinary and multifaceted approach to the scientific analysis of information security allows forming a complex, systemic mechanism of influence on the sphere of information protection from destructive influence.

The proposed model of an effective system theory of protection of information security objects contributes to the improvement of measures to ensure this group of public relations and can be used in the field of theoretical and practical law-making and law enforcement processes.

At the same time, the variety of objective factors of the concept of social conditioning and terminology in the field of information technology, information security (cyber threats) is both an advantage and an obstacle for the further genesis of the proposed methodological foundations of information security research and may become the subject of further scientific research.

Acknowledgements

None.

Conflict of interest

None.

References

[1] Afonchenko, T.P., Brileva, V.A., Vorobeva, E.M., Gorypa, T.A., Deykalo, E.A., Zapadnyuk, E.A., Zlotnikov, A.G., Isaychikova, N.I., Konnova, E.V., Konovalova, Zh.Ch., Kopytkova, N.V., Mozhaeva, L.E., Nabatova, A.E., Pasovets, E.Yu., Senkova, T.V., Sinitsa, I.M., Tomashevskiy, K.L., Usova, E.I., Esmantovich, I.I., & Yaroshevich, E.A. (2020). *Interdisciplinary research in the field of human rights* (2nd ed.). Minsk: Ekoperspektiva.

[2] Althonavan, A., & Andronache, A. (2018). Shifting from information security towards a cybersecurity paradigm. In *ICIME 2018: Proceedings of the 2018 10th International conference on information management and engineering* (pp. 68-79). New York: Association for Computing Machinery. doi: 10.1145/3285957.3285971.

[3] Babina, V.O., & Kudlai, I.V. (2022). Information policy and its role in the resolution of interstate conflicts. *Politicus*, 6, 53-58. doi: 10.24195/2414- 9616.2022-6.9.

[4] Balynska, O.M., & Yashchenko, V.A. (2018). *Methodology of modern legal science*. Lviv: Lviv State University of Internal Affairs.

[5] Baran, M. (2021). Information security as a subject of administrative and legal regulation. *Social & Legal Studios*, 3, 50-56. doi: 10.32518/2617-4162-2021-3-50-56.

[6] Bilozorov, Ye.V. (2021). Methodological approach as a tool of knowledge of law. *Current Problems of State and Law,* 90, 32-37. doi: 10.32837/apdp.v0i90.3204.

[7] Bilozorov, Ye.V. (2022). Jurisprudence activity based theory: General characteristics. *Uzhhorod National University Herald. Series: Law*, 70, 19-23. doi: 10.24144/2307-3322.2022.70.2.

[8] Boiko, O.M. (2021). Personal data collection and information security: Administrative and legal aspect. *European Perspectives*, 2, 56-62. doi: 10.32782/EP.2021.2.10.

[9] Danilian, O.H., & Dzoban, O.P. (2019). *Educational and methodological manual for the discipline "Organization and methodology of scientific research" for postgraduate students (applicants for higher education degree of Doctor of Philosophy)*. Kharkiv: Pravo.

[10] Decree of the President of Ukraine No. 685/2021 "On the Decision of the National Security and Defense Council of Ukraine dated October 15, 2021 "On Information Security Strategy". (2021, December). Retrieved from https://zakon.rada.gov.ua/laws/show/685/2021#Text.

[11] Doronin, I.M. (2020). *National security of Ukraine in the information age: Theoretical and legal research* (Doctoral thesis, Scientific Research Institute of Informatics and Law of the National Academy of Law Sciences of Ukraine, Kyiv, Ukraine).

[12] Hdychynskyi, V.B. (2019). Subject-disciplinary character of legal paradigms in law-making. *Journal of Eastern European Law*, 61, 49-54.

[13] Hulak, H.M. (2020). *Information protection methodology. Aspects of cyber security*. Kyiv: Publishing House of the National Academy of the Security Council of Ukraine.

[14] Kononenko, V.P., Novikova, L.V., & Kopytska, P.O. (2021). Policy of international organizations on information security. *Uzhhorod National University Herald. Series: Law*, 65, 353-358. doi: 10.24144/2307-3322.2021.65.64.

[15] Kovaliv, M.V., Yesimov, S.S., & Yarema, O.H. (2022). *Information law of Ukraine*. Lviv: Lviv State University of Internal Affairs.

[16] Kurko, M., & Didenko, S. (2021). Problematics of research of administrative and legal support of the education system in Ukraine: Theoretical and methodological aspects. *Analytical and Comparative Jurisprudence*, 4, 162-167. doi: 10.24144/2788-6018.2021.04.28.

[17] Law of Ukraine No. 2657-XII "On Information". (1992, Otober). Retrived from https://zakon.rada.gov.ua/laws/show/2657-12#Text.

[18] Lytvynova, L. (2021). Interdisciplinary approach in the study of communicative culture in public administration. *Derzhavne Upravlinnya: Udoskonalennya ta Rozvytok*, 2. doi: 10.32702/2307-2156-2021.2.36.

[19] Mikhailina, T.V., & Gotsulyak, Yu.V. (2021). Crisis of methodology of modern legal research. *Uzhhorod National University Herald. Series: Law*, 65, 26-30. doi: 10.24144/2307-3322.2021.65.4.

[20] Onopriienko, S.H. (2021). Methodological bases for studying information security in the law of nation-al security and military law. *Analytical and Comparative Jurisprudence*, 4, 185-188. doi: 10.24144/2788-6018.2021.04.32.

[21] Osadchuk, M.Yu. (2017). Integrative approach in the light of classical scientifical rationality. *State and regions. Series: Law*, 2, 9-13.

[22] Panchenko, O.A. (2020). *Government control of the information security in the era of turbulence* (Doctoral thesis, National University of Civil Defense of Ukraine, Kharkiv, Ukraine).

[23] Perun, T. (2017). Methodological approaches for conducting investigation of mechanisms of information security in Ukraine. *Journal of Lviv Polytechnic National University. Series: Legal Sciences*, 865, 303-307. doi: 10.23939/law2017.865.303.

[24] Pyrozhyk, O.V. (2021). On the need for Ukraine to use the positive experience of the United States in building an information security system. *Bulletin of the Penitentiary Association of Ukraine*, 2, 64-73. doi: 10.34015/2523-4552.2021.2.07.

[25] Smolianiuk, V. (2021). National security of independent Ukraine: Comprehension of the essence. *Political Studies*, 1, 163-186. doi: 10.53317/2786-4774-2021-1-10.

[26] Wendzel, S., Caviglione, L., Mileva, A., Lalande, J., & Mazurczyk, W. (2022). Guest editorial: Information security methodology and replication studies. *it – Information Technology*, 64(1-2), 1-3. doi: 10.1515/itit-2022-0016.

[27] Zakharenko, K.V. (2021). *Institutional dimension of information security of Ukraine: Transformational challenges, global contexts and strategic landmarks* (Doctoral thesis, National Pedagogical Drahomanov University, Ivan Franko National University of Lviv, Lviv, Ukraine).

Методологічні основи дослідження інформаційної безпеки

Сергій Сергійович Єсімов

Кандидат юридичних наук, доцент
Львівський державний університет внутрішніх справ
79000, вул. Городоцька, 26, м. Львів, Україна
https://orcid.org/0000-0002-9327-0071

Віталіна Станіславівна Боровікова

Науковий співробітник
Львівський державний університет внутрішніх справ
79000, вул. Городоцька, 26, м. Львів, Україна
https://orcid.org/0000-0003-4401-4562

Анотація. Відсутність усталеного підходу до методологічних досліджень у галузі інформаційної безпеки зумовлює подальший розвиток наукового знання та зміни парадигм і набуває особливої актуальності з огляду на агресію рф та необхідність посилення інформаційної безпеки України. Мета статті – визначити основи методології дослідження інформаційної безпеки. Для реалізації мети застосовано загальнофілософські методи дослідження правових явищ, зокрема аналіз відповідного законодавства та теоретичних розідок. У статті з врахуванням новітньої теорії держави і права та інформаційного права України, зважаючи на чинне законодавство та нормативні вимоги Європейського союзу, окреслено абстрактно-логічні аспекти методологічних основ дослідження інформаційної безпеки в умовах цифрової трансформації та російської інформаційної експансії. Зазначено, що звернення до теми міждисциплінарних досліджень тісно пов'язане з принципово новою історичною ситуацією, яка виявляє побудову інформаційних відносин нового типу між соціальними групами, охоплюючи філософію, політологію, соціологію, економіку та право. Розглянуто діяльнісний, системно-структурний, системно-функціональний, інформаційний, інтеграційний, прогностичний, методичний, парадигмальний наукові підходи щодо дослідження правових явищ. Указано, що інформаційна безпека має особливе значення для проєктування інноваційних соціальних систем в умовах цифрової трансформації, що вимагає подальших наукових досліджень методології наукових розвідок у сфері інформаційної безпеки. Дослідження спрямоване на вдосконалення методів дослідження захисту інформації та захисту особи, суспільства та держави від інформаційного деструктивного впливу, що охоплюється об'єктом інформаційної безпеки

Ключові слова: захист інформації; інформаційний деструктивний вплив; міждисциплінарні дослідження; принципи; цифрова трансформація