

METHODOLOGY OF RESEARCHING PROBLEMS OF REGULATORY AND LEGAL PROCUREMENT OF INFORMATION SECURITY

МЕТОДОЛОГІЯ ДОСЛІДЖЕННЯ ПРОБЛЕМ НОРМАТИВНО-ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Honcharov A., Candidate of Legal Sciences, Associate Professor,
Associate Professor at the Department of Intellectual Property and Private Law
National Technical University of Ukraine "Ihor Sikorsky Kyiv Polytechnic Institute"

Honcharov M., Postgraduate at the Department of Theoretical and Legal Disciplines
Educational and Scientific Institute of Law of State Tax University

The article deals with the conceptual problems of normative and legal provision of information security. It has been established that the regulatory and legal provision of information security in general, as well as at the elemental level, is characterized by scientificity, systematicity and has many aspects.

Regulatory and legal support is a scientifically based, consistent system of legal and other means by which civil society and the state influence information relations (implementation of information security, self-regulation) and relations directly related to the development of information security, based on the sequence of tasks and pursued goals that arise before society.

Attention is focused on the main tasks of the state information policy and the purpose of the information security policy of Ukraine is clarified, which is the formation of an open information society, as the space of an integrated state.

The specific nature of the information security research methodology consists in the integration of scientific knowledge about the ways and means of knowing the legal reality, the laws of its development and their adequate reflection in the formation of the conceptual apparatus.

Ensuring information security can be considered as a system of theoretical-methodological, normative-legal, information-analytical, managerial, intelligence, counter-intelligence, operational-research, personnel, scientific-technical, resource and other measures aimed at ensuring the conscious purposeful influence of the subject of management on threats and dangers, under which state, international and non-state institutions create the necessary and sufficient conditions for the realization and progressive development of information interests, the effective functioning of the information security system.

The state policy of ensuring information security should be based on scientific and methodological developments, systematized and combined into a single concept. It can be presented as a set of national goals, interests and values; strategies and tactics of management decisions and methods of their implementation, which are developed and implemented by the state authorities.

Key words: regulatory and legal provision of information security, national security, state information policy, information security of Ukraine.

У статті розглянуто концептуальні проблеми нормативно-правового забезпечення інформаційної безпеки. Встановлено, що нормативно-правове забезпечення інформаційної безпеки в цілому, так і на елементному рівні характеризується науковістю, системністю та має багато аспектів.

Нормативно-правове забезпечення є науково обґрунтована, послідовна система правових і інших засобів, за допомогою яких громадянське суспільство та держава здійснює вплив на інформаційні відносини (реалізація інформаційної безпеки, саморегулювання) і відносини, безпосередньо пов'язані з розробкою інформаційної безпеки, виходячи з черговості завдань і переслідуваних цілей, що виникають перед суспільством.

Акцентовано увагу на основних завданнях державної інформаційної політики та з'ясована мета політики забезпечення інформаційної безпеки України, це формування відкритого інформаційного суспільства, як простору цілісної держави.

Специфічна природа методології дослідження інформаційної безпеки полягає в інтеграції наукових знань про способи та засоби пізнання правової реальності, закономірностей її розвитку та їх адекватного відображення у формуванні понятійного апарату.

Забезпечення інформаційної безпеки можна розглядати як систему теоретико-методологічних, нормативно-правових, інформаційно-аналітичних, управлінських, розвідувальних, контррозвідувальних, оперативного-розшукових, кадрових, науково-технічних, ресурсних та інших заходів, спрямованих на забезпечення свідомого цілеспрямованого впливу суб'єкта управління на загрози та небезпеки, за якого державні, міжнародні та недержавні інституції створюють необхідні й достатні умови для реалізації та прогресивного розвитку інформаційних інтересів, ефективне функціонування системи забезпечення інформаційної безпеки.

Державна політика забезпечення інформаційної безпеки повинна базуватися на наукових і методологічних розробках, систематизованих і об'єднаних в єдину концепцію. Вона може бути представлена як сукупність національних цілей, інтересів і цінностей; стратегії та тактики управлінських рішень і методів їх реалізації, що розробляються та реалізуються державною владою.

Ключові слова: нормативно-правове забезпечення інформаційної безпеки, національна безпека, державна інформаційна політика, інформаційна безпека України.

Formulation of the problem. In the conditions of intensification of reforms in Ukraine, we are observing certain difficulties in the implementation of state functions in some spheres of life. The sphere of national security, information relations, etc. is no exception. At the same time, state-building and law-making processes in Ukraine in recent years demonstrate the need to draw the attention of representatives of domestic science to the issue of ensuring information security of the individual, community, society and the state.

The methodologically dominant issue of the paradigm of information security, which structures scientific, theoretical and practical information about the object under study, remains debatable, as is the question of the genesis and development of the structure of information security elements, their systematic classification and typology, optimal system orga-

nization and effective functioning in the conditions today's jurisprudence does not know the practice of law enforcement, the harmonization of structural and elemental connections, the forecast of changes in the structure and its elements.

It is necessary to find a scientifically weighted solution to the issue of the paradigm of information security as a methodological priority problem of the general theory of security. According to O. P. Dziobany, O. Yu. Panfilov, R. A. Chemchekalenko, the subject of systematic information security research is the identification of types of connections and, above all, system-forming connections of integrity, separation of the objective structure of a given system formation and its character [1, c. 172].

This is especially important during the implementation of the Law of Ukraine "On the Basic Principles of Ensuring

Cyber Security of Ukraine” and the Doctrine of Information Security of Ukraine for research where general scientific means of cognition perform heuristic functions, with the help of which a system of new scientific knowledge about one or another sphere of security is built; ensuring its communication links with other types of security; transformation of the conceptual apparatus of one sphere of security into another, which expands the possibilities of interpretation of research results [2].

The purpose of the article is to study the methodological foundations of regulatory and legal support of information security.

Analysis of recent research and publications. Many domestic and foreign scientists and researchers paid attention to the study of this issue. In particular, research into the essence of information security was reflected in the works of Ukrainian scientists: O. O. Zolotar, A. Yu. Nashinets-Naumova, O. A. Baranova, O. O. Tikhomirova, O. A. Zayarny, T. S. Perun and others.

Presenting main material. The structure of modern knowledge about security is characterized not so much by a collection of individual facts, theories and methods of their study, but by a complex approach to the study of “interfaces”, which presupposes the use of scientific tools of various fields of security in the course of researching complex problems related, for example, to the means of ensuring information security at the regional, or in general, at the state level, which is due to the internal relationship, that is, the interpenetration and mutual influence of different methods of knowledge and general methodological dominance [3].

The implementation of the above expands the possibilities of using systemic, structural-functional, informational, logical, model, probabilistic and other general scientific methods in the formation of the appropriate conceptual apparatus.

Using M. S. Kelman’s approaches to methodology, in this connection questions arise, on the one hand, about the use of general knowledge about security in the study of social problems, the study of which in logical and epistemological aspects can lead to obtaining both new and deepening of previously acquired knowledge, and, on the other hand, in the development and adoption of management decisions on security issues [4, c. 313].

At the same time, it is advisable to agree with A.B. Kaczynskii that a comprehensive study of the patterns of occurrence of socially dangerous factors and their impact on nature, society and man in the structure of general scientific knowledge is difficult to overestimate, since the results depend on social assessment and active state policy in the field of ensuring information security [5, c. 123].

It becomes clear that the problem of information security should be included among similar problems of social practice with full reason, the theoretical and applied solution of which requires, first of all, a rather broad, general scientific understanding in the formal and logical system of judgments: – first, a theoretical and applied solution to the problem ensuring information security has a clear focus on the development and implementation of scientific methods of managing social practice in the field of organizing information security; – secondly, the scientific toolkit for researching the problem of ensuring information security requires a mandatory transition from purely theoretical constructions to the analysis of empirical material, and then to the level of general scientific understanding, which captures the general scientific knowledge of “security” in an organic unity with the specific knowledge of “information security”; – thirdly, in the field of theoretical and methodological provision of information security, there is a synthesis of natural, technical and humanitarian knowledge, which includes the general provisions of all elements of social systems for the purpose of their preservation, normal functioning and development.

As noted by I. P. Aristova, considering the methodology of the science of “information law”, the first epistemologi-

cal basis: a scientist who is engaged in research in the field of information law must take into account, in particular, the existence of one of the regularities of the development of science as a whole – the interaction and interconnectedness of all fields science We draw attention to the importance of the interaction of all branches of legal science, as it allows researching the subject of one of the branches of legal science (for example, the science of “information law”) using the techniques and methods of other legal sciences [6, c. 12].

Based on the research of O. D. Dovgan, the legal provision of information security can be defined as an integral system of legal regulation of social relations, which has its own subject of legal regulation [7, c. 75].

The conceptual design of the modern information security system contains a certain complexity due to its multifaceted nature and involves the development of both theoretical and methodological issues, as well as the regulatory and legal mechanism, main directions, forms and methods of implementing relevant innovations.

Here it is important to adhere to the combination of theoretical and applied aspects of the study of the problem of regulatory and legal provision of information security so that, on the basis of establishing its role, functional significance and place in the general structure of problems of national security provision, to develop and clarify the relevant conceptual categories, to substantiate proposals for improving legislation and practice its application.

When considering the problem of the organization of ensuring information security, its structural classification, which is relatively conditional and is built in accordance with certain goals and objectives, becomes important. In this aspect, it is advisable to divide information security depending on the sources of the threat into two types – security of a technical nature, caused by the technology of information and communication processes, and security caused by social factors.

Today, as T. Yu. Tkachuk points out, the strategic information confrontation is a dangerous component of the war waged by Russia against Ukraine, and the line between the two components is very blurred. Moreover, the main threat to the information security of our country today remains the threat of the enemy’s influence on the information infrastructure, information resources, on society, the consciousness and sub-consciousness of the individual in order to impose his own system of values in vital spheres of social and state activity [8, c. 185].

However, such a division seems very expedient and useful from a practical point of view, as it allows for a clear classification of certain conceptual approaches to solving the problems of ensuring information security in general. In addition, such a division is necessary to realize that when ensuring information security of a technical nature, completely different methods, forms and methods are needed than when ensuring information security, which is caused by social factors.

Currently, threats to information security are of a social nature and are concentrated in the domestic political, economic, social, ecological, informational and spiritual spheres of our society. As mentioned above, information security is an integral, organic part of national security. It follows from this that the coincidence of certain types of threats is completely justified for them. This applies to terrorism, corruption, etc. These factors pose a threat to national security, at the same time they pose a danger to information security as a whole.

It should be noted that different interpretations of such a key concept as ensuring information security are expressed in the legal literature. We proceed from the fact that ensuring information security is a complex socio-legal mechanism, which should be understood as the formation and implementation of state policy regarding the creation and maintenance of the necessary level of security of security objects through the implementation of regulatory, organizational, managerial and other measures nature, measures, adequate threats to

the vital interests of the individual, society and the state in the information sphere.

The specific nature of the information security research methodology consists in the integration of scientific knowledge about the ways and means of knowing the legal reality, the laws of its development and their adequate reflection in the formation of the conceptual apparatus. The integrative approach is the relationship of the main structural elements of administrative and legal science: the object of scientific knowledge (legal reality), the subject of scientific knowledge (regularities of development), principles and methods of scientific research (methods of knowledge), rules and techniques of legal knowledge (means cognition), categorical and conceptual apparatus.

The main element of the methodology is a system of special legal methods: systemic, synergistic, hermeneutic, historical-legal, comparative-legal and formal-legal.

Summarizing, it is appropriate to note that from the point of view of the methodology of legal science, the information security paradigm has a structure made up of elements: law enforcement methodology, legislation of Ukraine, systematization of legal norms, interpretation of legal norms, mechanism of law application, state legal policy in the field of information security, culture and ethics the application of legislation that establishes restrictions on the rights and freedoms of a person and a citizen, the strategy and tactics of the subjects of information security, the effectiveness of the application of legislation, law enforcement examination of acts of departmental regulatory and legal provision of information security.

Each of the named elements of the information security paradigm can be presented in a self-sufficient form of an original special legal doctrine. Legal methodology plays a fundamental role in the development of our ideas about information security, its structure and elements, improvement of the mechanism of influence of law on social relations with the aim of harmonizing the social environment and strengthening security in various applied aspects.

Gradual penetration into the essence of legal phenomena determines the planned complication of the cognitive process, strengthens its methodological power at various stages

of the socio-political and economic development of the state.

The epistemological experience of mastering legal reality shows that for the development of information security, as a segment of the legal life of an individual, society and the state, not only the positive results of scientific research, but also the ways that stimulate the search for truth and lead to such results are of significant importance.

Therefore, during the research of regulatory and legal provision of information security, one should not limit oneself only to one's own methods of jurisprudence, one should use a wide arsenal of modern scientific methodology. In particular, it is advisable to apply dialectical, structural-functional, systemic-structural, comparative-legal, historical and other methods of scientific knowledge, which make it possible to comprehensively investigate the regulatory and legal provision of information security and realize the possibilities of comparative-legal, concrete-sociological, historical and logical analyzes [9, c. 115–116].

Such a complex application of methods makes it possible to investigate problems in the unity of their social content and legal form, to carry out a systematic analysis of the specified issues [10, c. 305].

Conclusions. Analysis of the consideration of the original methodological foundations of the concept and content of information security allowed us to draw the following conclusions: the original methodological foundations of the study of the concept and content of information security are based on a system of special legal methods: systemic, synergistic, hermeneutic historical-legal, comparative-legal and formal-legal.

Ensuring information security can be considered as a system of theoretical-methodological, normative-legal, information-analytical, managerial, intelligence, counter-intelligence, operational-research, personnel, scientific-technical, resource and other measures aimed at ensuring the conscious purposeful influence of the subject of management on threats and dangers, under which state, international and non-state institutions create the necessary and sufficient conditions for the realization and progressive development of information interests, the effective functioning of the information security system.

BIBLIOGRAPHY

1. Дзьобань О. П., Панфілов О. Ю., Чемчекаленко Р. А. Методологічний контекст дослідження проблеми інформаційної безпеки. *Зовнішня торгівля: економіка, фінанси, право*. 2014. № 2. С. 171–180.
2. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України»: Указ Президента України від 25.02.2017 р. № 47/2017. URL: <http://zakon3.rada.gov.ua/laws/show/47/2017> (дата звернення: 02.02.2023).
3. Про основні засади забезпечення кібербезпеки України: Закон України від 18.01.2018 р. № 2268-VIII / *Відомості Верховної Ради України*. 2017. № 45. Ст. 403. URL: <https://zakon.rada.gov.ua/laws/show/2163-19#Text> (дата звернення: 02.02.2023).
4. Кельман М. С. *Юридична наука: проблеми методології*. Тернопіль: ТЗОВ «Терно-граф», 2011. 492 с.
5. Качинський А. Б. Безпека, загрози і ризик: наукові концепції та математичні методи. Київ: Національна академія служби безпеки України, 2004. 471 с.
6. Арістова І. В. Методологія науки «інформаційне право». *IT право: проблеми і перспективи розвитку в Україні*: зб. матеріалів науково-практичної конференції. 18 листопада 2016 р. Львів, 2016. С. 11–18.
7. Довгань О. Д., Ткачук Т. Ю. Правове забезпечення інформаційної безпеки держави як підгалузь інформаційного права: теоретичний дискурс. *Інформація і право*. 2018. № 2 (25). С. 73–85.
8. Ткачук Т. Ю. Сучасні загрози інформаційній безпеці держави: теоретико-правовий аналіз. *Підприємництво, господарство і право*. 2017. № 10. С. 182–186.
9. Перун Т. С. Адміністративно-правовий механізм забезпечення інформаційної безпеки в Україні: дис. ... канд. юрид. наук: 12.00.07. Львів, 2019. 268 с.
10. Перун Т. С. Методологічні засади дослідження механізму забезпечення інформаційної безпеки в Україні. *Вісник Національного університету «Львівська політехніка»*. Серія: *Юридичні науки*. 2017. № 865. С. 303–307.