UDC 340+35.078.3
DOI https://doi.org/10.24144/2788-6018.2025.06.1.3

THE PROBLEM OF CLASSIFYING SOURCES OF THREATS TO INFORMATION SECURITY

Honcharov M.V.,
Doctor of Philosophy
ORCID: 0000-0003-4452-1652

Honcharov M.V. The problem of classifying sources of threats to information security.

The article considers scientific approaches to classifying sources of threats to information security.

A synthesized summary of the components of information security in the context of compliance with national security requirements showed possible root causes from which malicious attacks can be made on the established procedure for using information and databases with different levels of technological and legal protection.

A generalization is made about possible and permanent sources of threats to this component as a segment of the complex legal phenomenon «national security». The directions of the predicted root causes of unlawful attacks on the domestic information protection system are distinguished, and tools for timely and effective counteraction to unfriendly and hostile interference in the functioning of the information sphere at all levels of its protection are also indicated.

The sources of threats to information security are detailed, taking into account the human factor, and the directions for implementing preventive measures are determined in order to neutralize unlawful attacks on the information sphere as the basis for communication in all spheres of state life.

The human factor is identified as one of the criteria for sources of threats to information security. A generalized vision of the potentially harmful role of a person who is in possession of information, primarily with limited access, contributed to the development of proposals as part of a complex of preventive measures to prevent the leakage of confidential and other information classified as a state secret.

The main tasks of state information policy are emphasized and the goal of the policy of ensuring information security in Ukraine is clarified, which is the formation of an open information society as a space of an integral state, integrated into the world information space, taking into account national characteristics and interests in ensuring information security at the domestic and international levels.

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 represented 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 state authorities.

Key words: information security of Ukraine, ensuring information security, national security, system, state information policy, sources of threats to information security.

Гончаров М.В. Проблема класифікації джерел загроз інформаційній безпеці.

У статті розглянуто наукові підходи щодо класифікації джерел загроз інформаційній безпеці.

Синтезований підсумок складових інформаційної безпеки у контексті дотримання вимог національної безпеки показав можливі першопричини, з яких можуть завдаватися зловмисні посягання на встановлений порядок користування відомостями і базами даних з різним рівнем технологічного і правового захисту.

Зроблено узагальнення про можливі і перманентні джерела загроз цій складовій як сегменту комплексного юридичного явища «національна безпека». Вирізнено напрямки прогнозованих першопричин протиправних зазіхань на вітчизняну систему захисту інформації, а також зазначено інструменти своєчасної та ефективної протидії недружнім і ворожим втручанням у порядок функціонування інформаційної сфери на всіх рівнях її захисту.

Деталізовано джерела загроз інформаційній безпеці з урахуванням людського фактору, визначено напрямки провадження профілактико-превентивних заходів з метою нейтралізації протиправних посягань на інформаційну сферу як підґрунтя комунікації у всіх сферах життєдіяльності держави.

Одним з критеріїв джерел загроз інформаційній безпеці визначено людський фактор. Узагальнене бачення потенційно шкідливої ролі людини, управненої на володіння інформацією, насамперед з обмеженим доступом, сприяло виведенню пропозицій у складі комплексу профілактико-превентивних заходів з метою недопущення витоку конфіденційних та інших відомостей, віднесених до державної таємниці.

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, інтегрувального в світовий інформаційний простір з урахуванням національних особливостей і інтересів при забезпеченні інформаційної безпеки на внутрішньодержавному та міжнародному рівнях.

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: інформаційна безпека України, забезпечення інформаційної безпеки, національна безпека, система, державна інформаційна політика, джерела загроз інформаційної безпеці.

Problem statement. The international world order and the internal situation in Ukraine, along with the natural tendencies of interaction and development, are subject to the permanent action of destructive instruments of various levels of threats. This situation is visible in all spheres of society. The information component in the organization of social activity is especially sensitive to unlawful encroachments and manifestations. In the context of the above, it is appropriate to cite the world-famous statement of Nathan Rothschild that he who owns information owns the world. This concise expression reflects the entire essence and meaning of the information sphere as a social product, for the possession of which there is a constant open or hidden struggle between interested parties.

Assessing possible directions of unlawful interference in the legitimate information field, Yu.E. Maksymenko [1, p. 3] indicates that the development of the above-mentioned information tools and technologies causes a negative effect, since there is a significant increase in violations of the procedure for using information, namely, illegal collection of information, unauthorized access to information resources, destruction or damage to databases by launching virus programs, theft of information from archives, banks, libraries, etc. Significant losses are caused by illegal leakage of information or its illegal copying.

The state of the development of the problem. The state of the development of this problem. Many scientists and researchers have paid attention to the study of this issue: Bilenchuk P.D., Bilko S.S., Hnatiuk S.L., Hryhorchuk M.V., Dzyoban O.P., Dovgan O.D., Zolotar O.O., Kosilova O.I., Kudin S.V., Lipkan V.A., Loginov O.V., Novitska N.B., Tkachuk T.Yu., Tikhomyrov O.O., Frantsuz. A.Y., Tsymbalyuk V.S., Shevchenko A.Ye., Yarema O.G. and others.

The purpose of the article is to study scientific approaches to classifying sources of threats to information security.

Presentation of the main material. The significant level of harm from the deformed information field and data array is discussed in the scientific work of G. Sashchuk [2]. The scientist warns that the destructive impact of information attacks can change the morality and worldview not only of an individual person, but also encroach on the reorientation of the entire society or a significant part of it in its own interests. Such attacks impose other people's interests, carry out a hidden aggressive action on the basic moral values of the individual and society, which, due to the presence of aggressive content, harms the information environment and national security. In connection with the above, there is an urgent need to introduce effective mechanisms of protection against encroachments on state sovereignty and territorial integrity through unlawful interference in the information sphere of Ukraine.

At the same time, while exercising their subjective right to freedom of expression, free expression of beliefs and views, Part 3 of Article 34 of the Constitution introduces restrictions on the free interpretation of the right to possess and use information (such a right may be limited by law in order to prevent unlawful interference in the sphere of interests that threaten national security, encroach on the territorial integrity of the state, and also pose threats to public order and security, incite to commit offenses and crimes against other persons and their constitutional rights, threaten their reputation, pose threats to the established procedure for the circulation of information, etc.).

So, it is from illegal actions regarding the possession and use of information that the initial dangers in this area arise, which are defined as sources of threats to information security.

An Internet resource without reference to authorship provides a definition of the concept of «sources of threats» – these are conditions and factors that are hidden in themselves and under certain conditions, by themselves or in various combinations, reveal hostile intentions, harmful properties, and a destructive nature [3].

Considering the sources of threats to information security from the standpoint of a social nature, it is necessary to realize their level of scaling (external intervention or internal origin) as a tool for influencing public opinion, its formation and affirmation, or the intention to harm the information system as a material, protected object, which is regulated by relevant legal norms and provisions of subordinate regulatory legal acts.

In our opinion, the external signs of the manifestations of sources of threats to information security include: the activities of foreign disinformation centers and the transfer of this information to the maximum number of consumers; attempts by individual countries to gain an advantage in the information space in order to distort, distort or damage databases and other information in order to obtain dominant positions on international information platforms; measures aimed at seizing the latest technological tools as a means of potentially seizing the initiative in specific areas (defense, commercial, etc.); terrorist threats and subversive activities of foreign organizations; technological expansion by foreign commercial and other structures against the background of the weakening of Ukraine's influence on the global information network due to Russian military aggression; dissemination of strategic information that harms the national security of Ukraine, obtained by various means, including spy satellites, etc.; cyberwarfare and information warfare as sources of threats that harm all spheres of society through the use of tools to destroy, distort, or steal information, primarily national security.

The internal characteristics of the sources of threats to information security are somewhat different from those that encroach on the established information field of Ukraine from beyond the territorial borders of the state, since their origins are associated with the imperfection, ineffectiveness, and sometimes obsolescence of legitimized instruments that ensure the organization of information regulation and protection within the country. Such sources should include: problems of economic development, in connection with which there is insufficient financial support for measures to ensure information security; an uncompetitive level of informatization of the main industries, which is a consequence of the general state of the economy; gaps in the sphere of regulatory and legal regulation of relations in the information environment, which is a factor in increased malicious interest in mastering information for the purpose of enrichment or causing other harm; weakened attention to studying the personal data of candidates before appointment to positions related to information management, primarily with limited access, as well as effective control over employees holding these positions; the spread of criminal connections among persons authorized to access and manage information, their bribery, blackmail and other actions aimed at inducing them to criminal cooperation and violation of professional duty; insufficient coordinating and organizing role of the central government body responsible for implementing policy in the field of information security; insufficient development of the information environment, which is the basis for abuses in the field of information security.

The presented author's classification of external and internal threats in the field of information security is not exhaustive and we consider it as an occasion for further scientific discussion.

When classifying sources of threats to information security, it is necessary to distinguish two categories of factors: subjects (actions or inaction of a person) and objective manifestations (hackers, criminals, competitors, corrupt officials, representatives of state authorities and local governments authorized to access information). The unified goal of the practical results of the emergence and application of illegal and prohibited actions in the field of information security is the task of causing material damage and moral harm to the object of the encroachment, which is public relations in the information sphere. A deeper understanding of the role of the subject of information relations as a source of threats to information security can be found in the scientific work of V.A. Nekhay. The scientist notes that potential triggers of illegal use of information content by a person can be: unauthorized access to information stored in the system; denial of actions related to information manipulation; introduction into software projects and products of «logical seals» that are triggered when certain conditions are met or after the end of a certain period of time and partially or completely disable a computer system; development and distribution of computer viruses, and others [4].

A group of scientists, including Yu.E. Maksymenko, V.M. Zhelikhovsky, V.A. Lipkan [5, p. 130], distinguish «threats of breach of confidentiality». In their opinion, such dangers include: «leakage» of information with an established procedure for use, unauthorized access to information resources, violation of integrity, modification, damage, replacement of data, as well as committing actions that hinder access to information or use of information resources.

The expressed judgments found support in the scientific work (terminological reference book, dictionary on information security) of such scientists as V.M. Bogush, V.G. Kryvutsa and A.M. Kudin [6, p. 123].

We find certain aspects as manifestations of sources of dangers for the information field of Ukraine in the work of V. Petryk, who defines threats to national security in the information sphere as a set of conditions and factors that pose a danger to the vital interests of the state, society and the individual due to the possibility of negative information influence on the consciousness and behavior of citizens, as well as on information resources and information and technical infrastructure [7].

From the above judgment, we conclude that the root causes of alarming signs of unlawful interference in the established procedure for using information can be harmful information influence embedded in the produced content, hostile media resources implemented in the domestic information space, which instill treacherous and capitulating clichés in the human mind, impose negative stereotypes of thinking for our environment, etc.

A team of scientists consisting of K.A. Kononenko, B. Parakhonsky and G. Yavorskaya came to an understanding that there is a close mutual connection between the sources of origin and methods of detecting internal and external threats and it is this order of interdependence that is threatening to the state of national security [8, p. 30].

L.V. Borisova and V.V. Tulupov [9, p. 40] carried out a theoretical and practical analysis of the draft Concept of International Information Security. According to the conclusions of scientists, which are in line with the views of other scientists, it is necessary to distinguish the cross-border sphere as one of the sources of threats to information security. Such threats will occur when moving intellectual resources across the border, namely, exporting information that has a unique scientific and technological nature and is owned by specialists, analytical and other information on forecasting development trends in other states to obtain unauthorized access to confidential information and databases.

Theoretical, legal and methodological analysis of the complex of factors that directly or indirectly affect the sphere of information security showed that as a component of national security, this sphere, in accordance with the modern development of its theory, is based on the following basic elements in a generalized form: national interests - threat - protection. That is, as the scientist notes, the sources of threats are the basis for the application of protection mechanisms in accordance with the identified root cause and the level of potential damage.

B.A. Kormych sees the sources of threats to information security in the insufficient protection of special technical means and the imperfection of the technologies used. In this regard, the scientist states that the main actions for collecting, transmitting and distributing information are carried out using special technical means and technologies. In accordance with the development of science and technology, these information means and technologies have become one of the most important components of information processes, along with the information itself and the subjects of information relations [10, p. 322].

All of the above encourages the combination of efforts of all subjects included in the structure of national security of Ukraine in order to achieve the highest possible level of protection of data arrays from unlawful encroachment on their integrity and the procedure for working with them. In this regard, it is advisable to listen to N.S. Onishchenko, who notes: «the conditions of existence can act as a stimulus for the development of abilities and increasing the capacity of the subject, which, in turn, gives him the opportunity to influence the conditions of his existence in order to improve them. Such conditions can also include potential threats, the level of which does not destabilize the activity of the subject, but on the contrary encourages development. Then the «minimum» task for the state becomes the creation of general minimum conditions that will ensure the self-development and self-realization of individuals» [11, p. 115; 12, p. 105].

In our opinion, state builders urgently need to work at the «maximum» in order to create such safe conditions in the field of information and information technologies that attackers would not be tempted to test the effectiveness of preventive and preventive mechanisms of state coercion.

Conclusions. Thus, the current stage of Ukraine's development in the field of information security requires a strengthening of the role of the state, in particular in terms of organizing and controlling the activities of all subjects of the information sphere from the standpoint of assessing the legality of their use of information. The analysis shows that the problem of classifying sources of threats to information security remains one of the most urgent and at the same time complex. The significant diversity of threats, their dynamism, technological evolution and the growth of the influence of the human factor determine the need to create a systemic, multi-level and adaptive classification. The absence of a universal classification model complicates the development of effective mechanisms for countering and predicting new risks.

A generalization of existing approaches shows that the optimal classification system should take into account the source of the threat, its motivation, methods of implementation, the scale of influence and the level of organization. Prospects for further research are related to the formation of unified criteria for assessing threats and the creation of flexible classification models capable of promptly responding to changes in the modern information space.

Therefore, effective provision of national security of Ukraine in the field of information protection involves the development of scientifically based state policy and long-term strategy, as well as constant monitoring of potential and actual threats. Only with a comprehensive approach and the implementation of effective tools can stable and secure conditions for the functioning of the state's information environment be created.

REFERENCES:

1. Maksymenko Yu.E. Theoretical and legal principles of ensuring information security of Ukraine: dissertation ... candidate of legal sciences: 12.00.01: theory and history of state and law; history of political and legal doctrines. Kyiv, 2007. 236 p.
2. Sashchuk G. Information security in the system of ensuring national security. URL. http://troubleshooter.com.ua/ru/inform-bezopasnost/52-informatsijna-bezpeka-v-sistemi-zabezpechennya-natsionalnoji-bezpeki.
3. Types of threat sources. URL: https://stud.com.ua/21603/ekonomika/vidi_dzherel_zagroz.
4. Nehai V.A. Information security as a component of economic security of enterprises. Scientific Bulletin of the International Humanitarian University. Series: Economics and Management. 2017. Issue. 24 (2). P. 137–140. URL: file:///C:/Users/%D0%90%D0%BD%D0%B4%D1%80%D0%B5%D0%B9/Downloads/Nvmgu_eim_2017_24(2)__30.pdf.
5. Lipkan V.A., Maksymenko Yu.E., Zhelikhovsky V.M. Information security of Ukraine in the conditions of European integration: a manual. Kyiv: KNT, 2006. 280 p.
6. Bogush V.M., Kryvutsa V.G., Kudin A. M. Information security: Terminological training manual. Kyiv: OOO «DVK», 2004. 508 p.
7. Petryk V. The essence of information security of the state, society and the individual. URL: http://www.justinian.com.ua/article.php?id=3222.
8. Current challenges and threats to regional security: conclusions for Ukraine; [ed. by K.A. Kononenko: analytical assistants B. Parakhonsky, G. Yavorska]. Kyiv: NISD, 2014. 48 p.
9. Borisova L.V., Tulupov V.V. Information security as a determining component of the national security of Ukraine. Law and security. 2013. No. 1 (48). P. 39–42. URL: http://repositsc.nuczu.edu.ua/bitstream/123456789/6805/1/Pib_2013_1_9.pdf.
10. Kormych B.A. Organizational and legal foundations of the information security policy of Ukraine: dissertation for the degree of Doctor of Laws: 12.00.07. Kharkiv, 2004. 542 p.
11. Onishchenko N.S. Perception of law in the conditions of democratic development: problems, realities, prospects: monograph. [editor-in-chief Yu.S. Shemshuchenko]. Kyiv: LLC Publishing House «Yurydychna Dumka», 2008. 320 p.
12. Honcharov M.V. Theoretical and legal foundations of information security regulation in Ukraine: dissertation ... candidate of law: 12.00.01: theory and history of state and law; history of political and legal doctrines. Irpin, 2023. 215 p.