DOI: https://doi.org/10.34069/AI/2023.67.07.8
How to Cite:
Chernysh, R., Chekhovska, M., Stoliarenko, O., Lisovska, O., & Lyseiuk, A. (2023). Ensuring information security of critical infrastructure objects as a component to guarantee Ukraine's national security. *Amazonia Investiga*, *12*(67), 87-95. https://doi.org/10.34069/AI/2023.67.07.8

Ensuring information security of critical infrastructure objects as a component to guarantee Ukraine's national security

Забезпечення інформаційної безпеки об'єктів критичної інфраструктури, як складова гарантування національної безпеки України

Received: May 30, 2023 Accepted: July 2, 2023

Written by:
Roman Chernysh[1]
https://orcid.org/0000-0003-4176-7569
Mariia Chekhovska[2]
https://orcid.org/0000-0001-8135-7770
Olena Stoliarenko[3]
https://orcid.org/0000-0003-3134-3201
Olena Lisovska[4]
https://orcid.org/0000-0002-2272-3053
Andrii Lyseiuk[5]
https://orcid.org/0000-0002-9026-1188

Abstract

The purpose of the article is to define and justify the conceptual foundations of the implementation of the state policy on ensuring the information security of critical infrastructure objects, as a component of guaranteeing the national security of Ukraine. The methodological basis of the study was a set of general scientific and special methods of scientific knowledge: dialectical-phenomenological, systemic analysis and synthesis, structural-functional, deduction and induction, etc. According to the results of the research: the author's definition of the concepts «information security of critical infrastructure objects of Ukraine» and «threats to information security of critical infrastructure objects of Ukraine» was formulated; the elements of the system of threats to the information security of critical infrastructure objects of Ukraine are identified; the factors leading to the emergence of threats to critical infrastructure objects of Ukraine are singled out and groups of basic measures aimed at countering traditional and

Анотація

Метою статті є визначення та обґрунтування концептуальних засад реалізації державної політики із забезпечення інформаційної безпеки об'єктів критичної інфраструктури, як складова гарантування національної безпеки України. Методологічну основу дослідження склала сукупність загальнонаукових та спеціальних методів наукового пізнання: діалектико-феноменологічного, системного аналізу та синтезу, структурно-функціонального, дедукції та індукції тощо. За результатами дослідження: сформульовано авторське визначення понять «інформаційна безпека об'єктів критичної інфраструктури України» та «загрози інформаційній безпеці об'єктів критичної інфраструктури України»; визначено елементи системи загроз інформаційній безпеці об'єктів критичної інфраструктури України; виокремлено чинники, що призводять до виникнення загроз об'єктам критичної інфраструктури України та сформульовано групи основних заходів, спрямованих на протидію традиційним і новим

[1] Phd in Law, Associate Professor, National Academy of the Security Service of Ukraine, Kyiv, Ukraine. WoS Researcher ID: B-7598-2018
[2] Doctor of Economics, Professor, National Academy of the Security Service of Ukraine, Kyiv, Ukraine.
[3] Doctor of Economics, Associate Professor, National Academy of the Security Service of Ukraine, Kyiv, Ukraine.
[4] PhD in Economics, Associate Professor, National Academy of the Security Service of Ukraine, Kyiv, Ukraine.
[5] Phd in Law, Associate Professor, National Academy of the Security Service of Ukraine, Kyiv, Ukraine.

new threats to the information security of critical infrastructure objects of Ukraine are formulated.

Keywords: critical infrastructure objects, information security, forces and means, national security, threats to information security.

загрозам інформаційній безпеці об’єктів критичної інфраструктури України.

Ключові слова: загрози інформаційній безпеці, інформаційна безпека, національна безпека, об’єкти критичної інфраструктури, сили та засоби.

Introduction

The further development of Ukraine, the implementation of the European integration course, the very existence of our state in a period of threats and danger even more than in peacetime, requires the activation of radical reform processes, first of all, in the field of organization and activity of the national security and defense sector, transformation on democratic principles of all the main civil institutions, introduction of new principles of exercise of state power.

Provided the spread of information technologies and their active use in the conditions of the Russian-Ukrainian war (Horska et al., 2023, p. 353), the issue of ensuring the sustainable functioning of critical infrastructure facilities is extremely urgent. Therefore, our state should systematically improve conceptual measures of information security, because information threats are much more dynamic compared to economic or political ones. In our opinion, a certain reserve in this countermeasure is the improvement of the organization of the work of special entities to ensure timely and targeted neutralization of information threats (preferably at the stage of preparation for their implementation or at the initial stage).

In modern conditions, «informational potential» becomes one of the most important factors in ensuring national security, along with «economic potential», «military potential», etc. The level of development and security of the information environment actively influence the state of political, economic and other components of national security of Ukraine (Prysiazhniuk, 2014, p. 27).

Methodology

In order to achieve the goals of scientific research, a combination of interrelated and complementary scientific research methods was used.

Thus, the methodological basis of the study was a set of general scientific and special methods of scientific knowledge: dialectical-phenomenological, systemic analysis and synthesis, structural-functional, deduction and induction, and others. In particular, the use of the dialectical and phenomenological method, as well as systemic analysis and synthesis, made it possible to identify the essential features of the implementation of state policy in the field of ensuring information security of critical infrastructure objects, as a component of guaranteeing the national security of Ukraine. Thanks to the use of the structural-functional method, it was possible to identify and generally characterize the forces and means of ensuring information security of critical infrastructure objects of Ukraine. The use of methods of system analysis and synthesis, as well as deduction and induction made it possible to formulate the concept of «threats to the information security of critical infrastructure objects of Ukraine», to systematize them, to single out the factors that lead to their occurrence, and to propose groups of basic measures aimed at countering traditional and new threats to the information security of critical infrastructure objects of Ukraine.

The research also used the work of scientists reflected in scientific articles, which are indexed in the Web of Science scientometric database.

Literature Review

An urgent problem today for ensuring international and national security is prompt response to the emergence of new challenges and threats in various spheres of public life.

Its successful solution in the conditions of global transformations in the world is impossible within the framework of the application of traditional approaches to predicting threats and ensuring the appropriate level of collective and national security.

In these conditions, the awareness and proper assessment of the importance of information and the informational component of the development of modern civilization becomes of primary importance. Understanding the importance of ensuring information security (including critical infrastructure objects), more and more scientists from different countries of the world are paying attention to the study of this issue.

Let's name only some of them, without at all diminishing the achievements and significance of other scientists and researchers. In particular, these are: Doronin I., Dovgan O., Govorukha V., Horbulin V., Krutov V., Lipkan V., Marushchak A., Petryk V., Pocheptsov H., Polevy V., Pylypchuk V., Risman D., Ron T., Tikhomirov O., Tkachuk T., Ukhanova N. and others.

These authors made a significant contribution to the development of legal and organizational regulation of legal relations in the information field. Protest, despite the achievements of Ukrainian and foreign scientists, in view of the ultra-fast pace of informatization, in particular the current stage – digitization, a significant range of issues of the raised issues still remain insufficiently researched and require scientific substantiation for the purpose of further implementation into the practical component.

The rapid development of information technologies and the globalization of the Internet have led to the fact that the information infrastructure of the state has become an object of criminal activity - more vulnerable places for illegal encroachments have appeared.

Criminal and terrorist groups have gained the opportunity to use the global network to achieve their goals.

Because of this, the problem of ensuring the security of the information infrastructure is essential in the state's defense capability, its economic and social development.

The processes of global informatization have led to the fact that modern society is almost completely dependent on the state of security of the information infrastructure.

Results and discussion

According to the provisions of the Law of Ukraine «On the National Security of Ukraine», threats to the national security of Ukraine are phenomena, trends and factors that make it impossible or difficult or may make it impossible or difficult to realize national interests and preserve the national values of Ukraine. In turn, national interests in the specified article are defined as vital interests of man, society and the state, the implementation of which ensures the state sovereignty of Ukraine, its progressive democratic development, as well as safe living conditions and well-being of its citizens (Law 2469-VIII, 2018).

Art. 1 of the Law of Ukraine «On the National Security of Ukraine» also stipulates that the National Strategy is a document that defines the current threats to the national security of Ukraine and the corresponding goals, tasks, mechanisms for the protection of the national interests of Ukraine and is the basis for the planning and implementation of state policy in the field of national security of Ukraine. The specified legal act states that the priorities of the national interests of Ukraine and ensuring national security are:

- defense of independence and state sovereignty;
- restoration of territorial integrity within the internationally recognized state border of Ukraine;
- social development, primarily the development of human capital;
- protection of rights, freedoms and legitimate interests of citizens of Ukraine;
- European and Euro-Atlantic integration.

Implementation of these priorities will be ensured in the following areas:

- restoration of peace, territorial integrity and state sovereignty in the temporarily occupied territories in the Donetsk and Luhansk regions of Ukraine on the basis of international law;
- implementation of international legal, political and diplomatic, security, humanitarian and economic measures aimed at ending the illegal occupation of the Autonomous Republic of Crimea and the city of Sevastopol by the Russian federation;
- continuation of the implementation of defense and deterrence measures, active use of negotiating formats and consolidation of international pressure on the Russian federation as a guarantee of preventing the escalation of the conflict on the part of Russia, reducing tension and ending armed aggression by the Russian federation;
- use of all available mechanisms of the UN, the Council of Europe, the OSCE, and other international organizations to consolidate international support for Ukraine in countering Russian aggression, restoring Ukraine's territorial integrity and state sovereignty;

- development of relations with the United States of America, the United Kingdom of Great Britain and Northern Ireland, Canada, the Federal Republic of Germany, the French Republic, neighboring and other states, as well as with international organizations to ensure international security and counter common challenges and threats, minimizing their impact on Ukraine;
- full implementation of the Association Agreement between Ukraine, on the one hand, and the European Union, the European Atomic Energy Community and their member states, on the other hand, and modernization of its parameters where necessary, based on the results of a comprehensive review of the achievement of the goals of the Agreement in accordance with Article 481, with the aim of acquiring full membership of Ukraine in the European Union;
- development of a special partnership with the North Atlantic Treaty Organization with the aim of gaining full membership of Ukraine in NATO;
- strengthening the capabilities of the Armed Forces of Ukraine, other bodies of the security and defense sector;
- sustainable development of the national economy and its integration into the European economic space;
- the development of Ukraine's human capital, in particular through the modernization of education and science, health care, culture, and social protection;
- protection of the individual, society and the state from offenses, in particular corruption, ensuring the restoration of violated rights, compensation for the damage caused;
- ensuring environmental safety, creating safe conditions for human life, in particular in territories affected by hostilities, building an effective civil defense system;
- strengthening the capabilities of the national cyber security system to effectively counter cyber threats in the modern security environment;
- development of public-private partnership (Decree of the President of Ukraine 392/2020, 2020).

In accordance with the provisions of the Information Security Strategy, global challenges and threats are defined as:

- increase in the number of global disinformation campaigns;
- the information policy of the Russian federation is a threat not only to Ukraine, but also to other democratic states;
- social networks as subjects of influence in the information space;
- insufficient level of media literacy (media culture) in conditions of rapid development of digital technologies.

National challenges and threats are defined as:

- informational influence of the Russian federation as an aggressor state on the population of Ukraine;
- the information dominance of the Russian federation as an aggressor state in the temporarily occupied territories of Ukraine;
- limited opportunities to respond to disinformation campaigns;
- lack of formation of the strategic communications system;
- imperfect regulation of relations in the field of information activities and protection of journalist's professional activities
- attempts to manipulate the consciousness of Ukrainian citizens regarding the European and Euro-Atlantic integration of Ukraine;
- access to information at the local level;
- insufficient level of information culture and media literacy in society to counteract manipulative and informational influences (Decree of the President of Ukraine 685/2021, 2021).

According to the provisions of the National Security Strategy, the main task of the development of the cyber security system is to guarantee the cyber resistance and cyber security of the national information infrastructure, in particular in the conditions of digital transformation (Decree of the President of Ukraine 392/2020, 2020).

Having analyzed the above, we state that information security, cyber security and state security are components of national security. That is, on the one hand, they are independent components of the state's national security, and on the other hand, they are integrated components of any other security: military, economic, political, etc.

All components of the structure of national security are interconnected, but it is appropriate to note that some types of security are not only independent, but also those that have corresponding dimensions in other directions of the life of society. Among such «integrative» types, according to Pirozhkov S., information security occupies an important place (Pirozhkov, 2016).

The issue of ensuring state interests and state security in the field of obtaining and using information is currently quite relevant. Information security is ensured by the implementation of a unified state policy in the field of national information security, a system of economic, political and organizational measures adequate to existing and potential threats to national interests (personal, public and state) in the information sphere.

At the same time, in our opinion, the national special services with their information and analytical potential should play a significant role in this complex system (Shilin, Shmotkin, Chernysh, Chekhovska & Konyk, 2023; Shilin, Shmotkin, Chernysh, Konyk & Botvinkin, 2022; Chernysh, Prozorov, Tytarenko, Matsiuk & Lebedev, 2022; Kostenko, Strilchu, Chernysh & Buchynska, 2021).

To ensure and maintain the necessary level of state security in the information space, a system of legal norms regulating relations in the information sphere is being developed and implemented. It provides for the determination of the key areas of activity of state administration bodies, the creation or reorganization of bodies and forces that ensure information security, as well as the formation of a mechanism for monitoring their activities.

The point of view of Lipkan V. deserves attention, noting that the process of forming key elements of the information security system has not yet been completed. Taking into account the general lack of formation of the national security system, the uncertainty of the state information policy is appropriate in this context. Moreover, the imperfection of regulatory and legal regulation of the studied processes negatively affects the quality of public administration in the specified area (Lipkan et al., 2006).

In our opinion, the issue of ensuring information security of critical infrastructure objects, as a component of ensuring Ukraine's national security, should be considered systematically and comprehensively - in the context of ensuring cyber security, state security and information security. These components act as integrated components of national security and are positioned as priority functions of the state.

Information security of objects of critical infrastructure of Ukraine is a systematic provision of the state of complete security of their information field. Control over the use of information resources and the ability to effectively take certain actions in relation to them is information sovereignty, and one of the main tools of such control is countering destructive informational influences.

The rapid development of the global information space and the use of information and communication technologies in all spheres of life contribute to the expansion of the information society in Ukraine and determine the importance of information security problems. In such conditions, one of the main tasks of the state is to create a comprehensive system for assessing threats of an informational nature and corresponding response in order to ensure state security in the information sphere (Decree of the President of Ukraine 449/2014, 2014).

Threats to the information security of critical infrastructure objects of Ukraine can be formulated as a system of conditions and factors that lead or may lead to damage to important state, public and personal interests due to technical influence on information resources and infrastructure.

The system of threats to the information security of critical infrastructure objects of Ukraine may include the following categories:

- threats to the security of information and related infrastructure, which include risks related to misuse, unauthorized access, damage or loss of information, as well as attacks on information infrastructure (cyber-attacks or computer viruses);
- threats to the safety of subjects of the information direction and social ties between them from actions (influences) of an informational nature, which include manipulation of information with the aim of influencing the consciousness and behavior of citizens, forming the desired impression and manipulation of social ties with the aim of influencing the public order;
- threats to the current order of realization of the rights and interests of subjects of the information sector, which include actions aimed at violating laws, rights and freedoms, in particular in the field of information (distribution of misinformation, discrediting, obstacles to access to information or restriction of freedom of speech).

At the same time, we agree with the opinion of Khmelevskyi R. that even detailed lists of threats cannot be comprehensive and stable. This is explained by the fact that the sources of threats can be diverse: a person, technical means, models, algorithms, software and technological processing schemes, the external environment, etc. (Khmelevskyi, 2016, p. 69).

Having analyzed the system of threats to information security of critical infrastructure objects of Ukraine, we come to the conclusion that the technical aspect is not central to the structure of information security of critical infrastructure objects of Ukraine. Taking into account the above classifications, it is advisable to ensure not only the security of information data from destruction, distortion or blocking, but also general information security. This will be facilitated by the priority development of an appropriate system of regulatory and legal regulation of countering threats to these interests and streamlining the law-making process in the field of analysis, generalization, use and dissemination of information.

The need for such development of the system of regulatory and legal support is determined by certain factors. First, in the conditions of the functioning of the legal state and civil society, the main functions of state authorities, which are entrusted with the main responsibility for national security, should be regulated by legal norms aimed at ensuring civil constitutional rights and freedoms. Legislation in this direction should be aimed at the normative consolidation of the tasks of countering threats to the national security of Ukraine, the means and methods of their implementation, ensuring the conciliatory policy of the authorities. Secondly, Ukraine’s course for integration into the international community significantly expands the possibilities of consolidating the conceptual foundations of state information security through participation in the development and improvement of international legal norms in this area, the formation of an international system for ensuring information security on a global scale and within the framework of an individual country. Thirdly, the implementation of guarantees of civil rights and freedoms, protection of state interests of our country involves a significant increase in the role of authorities in regulating relevant social relations, the presence of a transparent and understandable state policy (Pocheptsov, 2015).

The main factors that lead to the emergence of threats to the objects of critical infrastructure of Ukraine include the following:

- lack of a complete system of information and analytical support of state authorities and management;
- destruction of intellectual potential, unpreparedness of the education system to support the processes of anticipatory development of the state;
- low general level of information infrastructure development, which does not exclude the possibility of expansion of foreign companies in the market of information services;
- the destruction of the national information space and the possibility of its use in anti-state interests;
- insufficient professional, intellectual and creative level of domestic producers of information products and services, their lack of competitiveness in the global information market;
- informational expansion of leading foreign states, development and use by them, international or domestic criminal organizations of various modern methods of direct subversion;
- poorly controlled activities of individual political forces, media and individuals, aimed at destroying moral values, undermining the moral and physical health of the nation; using mass media from positions contrary to the interests of citizens, political and public organizations, and the state;
- loss of trust in the government by a significant part of the population due to the spread of slander, the use of «dirty» political technologies, especially during election campaigns;
- competitive struggle for ownership of mass media, the process of their monopolization and concentration of informational and political power; manipulation of public opinion (through disinformation, distortion of data, suppression of true information, etc.) (Petryk et al., 2018, p. 26-27).

The system of ensuring information security of critical infrastructure objects of Ukraine as a component of the system of ensuring national security is generally characterized by appropriate forces and means. In this context, it is possible to consider the **forces** as the subject composition of the information security system of critical infrastructure objects of Ukraine, i.e., people, organizations, structures, special bodies that carry out information protection; **means** – as technologies and various technical, software, linguistic, legal and organizational resources. They include telecommunications channels used to collect, form, analyze, transmit or receive information data, as well as measures aimed at strengthening said security.

In the modern information society, each subject plays an important role in ensuring the information security of critical infrastructure objects of Ukraine. Thanks to synergistic features, any of the subjects can simultaneously be an object of information security and a source of possible threats or a channel of their spread. Therefore, the success of ensuring information security of critical infrastructure objects of Ukraine depends not only on special state structures, but also on each subject of information relations, which must protect itself in the information sphere. At the same time, the state acts as a special subject of ensuring information security, as it has the ability to direct administrative action and uses legal means to regulate information relations. In addition, it should be taken into account that the state plays a special role among the subjects of information security of critical infrastructure objects of Ukraine. After all, only it has a wide potential, which includes not only economic, political and ideological means of indirect influence, but also direct managerial action. This means that the state can use legal means to regulate information relations and directly influence the provision of information security (Tikhomirov, 2023).

Taking into account the provisions of Article 17 of the Constitution of Ukraine (Law 254к/96-ВР, 1996), ensuring information security is considered one of the most important functions of the state, along with the protection of Ukrainian sovereignty and territorial integrity. State activity in this direction is carried out through relevant authorities. In particular, the circle of subjects responsible for ensuring state security and implementing a set of other measures of a similar direction has been defined. These entities include military formations, special services and law enforcement agencies, the content and procedure of which are determined by law.

According to the provisions of Article 12 of the Law of Ukraine «On National Security of Ukraine», the national security and defense sector consists of four interrelated elements: security forces; defense forces; defense industrial complex; citizens and their associations who can voluntarily participate in ensuring the security of the state. The functions and competence of elements of the security and defense sector are established by the current legislation of Ukraine (Law № 2469-VIII, 2018).

Lipkan V. proves that, taking into account the functionality of the subjects, the information security system is formed from the strategic, tactical and operational levels of security management. The researcher attributes the National Security and Defense Council of Ukraine and the Cabinet of Ministers of Ukraine to the subjects of the higher, strategic level, respectively, the central bodies of the executive power are the subjects of the lower, tactical level, and the local bodies of the executive power are located at the operational level (Lipkan, 2009). Agreeing with Lipkan V., it should be noted at the same time that the Security Service of Ukraine and intelligence agencies «drop out» of the three-level system.

Conclusions

The results of the study of the genesis of the regulatory and legal regulation of organizational and practical measures to ensure the information security of Ukraine give grounds to believe that in the modern conditions of information confrontations, the information security of critical infrastructure objects of Ukraine is insufficiently protected from internal and external threats (Chernysh, Pogrebnaya, Montrin, Koval & Paramonova, 2020a; Chernysh, Pogrebnaya, Montrin, Koval & Paramonova, 2020b). Therefore, the protection of their information sovereignty, the formation of a powerful and effective information security system, the development and implementation of effective strategies and tactics for countering information threats should be the priority tasks of state authorities, special services and law enforcement agencies (including taking into account russian armed aggression) and non-state institutions.

Taking into account the above, we come to the conclusion that in modern conditions it is possible to formulate the following groups of basic measures aimed at countering traditional and new threats to the information security of critical infrastructure objects of Ukraine and eliminating the factors that lead to their occurrence:

– **political and diplomatic measures** – political and diplomatic efforts to strengthen international cooperation, conclude international treaties and agreements, build alliances and partnerships with other countries in order to ensure collective security in the information sphere;

- **military measures** – strengthening of the country's defense capabilities, development of military infrastructure, modernization of military forces and implementation of military operations to protect the state security of Ukraine in the information sphere;
- **legal (legislative) measures** – development and adoption of normative legal acts aimed at regulating the field of information security, including the fight against terrorism, cyber threats, cyber-crime, etc.;
- **informational and psychological measures** – conducting informational campaigns, appropriate psychological influence on the public, formation of a positive image of the country, fight against disinformation and propaganda, formation of a «culture of information consumption» among the population;
- **economic measures** – development of economic sectors, attracting investments, ensuring economic stability, combating financial threats in the information sphere;
- **scientific and technological measures** – scientific research, development of technologies and innovations, which are aimed at identifying, forecasting and countering new threats in the information sphere, including cyberespionage and cyberattacks on critical infrastructure objects;
- **organizational (administrative and procedural) measures** – development and implementation of effective organizational structures, procedures and policies that contribute to ensuring information security. May include creation of specialized information security departments, determination of information access control procedures, regular review and updating of security systems, etc.;
- **physical measures** – physical protection of information infrastructure, data storage facilities (primarily critical infrastructure facilities), restriction of physical access to confidential information and installation of video surveillance and control systems;
- **technical (hardware and software) measures** – application of special hardware and software for information protection, data encryption, detection and recovery after incidents, data backup and other technical means to ensure state security in the information sphere.

The implementation of the mentioned measures will contribute to the creation of a comprehensive system (takes into account various threats and uses various methods for their prevention and localization) of ensuring information security of critical infrastructure objects of Ukraine, as a component to guarantee Ukraine's national security.

Bibliographic references

Chernysh, R., Prozorov, A., Tytarenko, Y., Matsiuk, V., & Lebedev, O. (2022). Legal and organizational aspects of destructive information impact counteracting: the experience of Ukraine and the European Union. Amazonia Investiga, 11(54), 169-177. https://doi.org/10.34069/AI/2022.54.06.16

Chernysh, R., L. Pogrebnaya, V., I. Montrin, I., V. Koval, T., & S. Paramonova, O. (2020). Development of Internet communication and social networking in modern conditions: institutional and legal aspects. Revista San Gregorio, 1(42), Url: http://revista.sangregorio.edu.ec/index.php/REVISTASANGREGORIO/article/view/1572

Chernysh, R., Pogrebnaya, V. L., Montrin, I. I., Koval, T. V., & Paramonova, O. S. (2020). Formation and application of communication strategies through social networks: legal and organizational aspects. International Journal of Management, 11(6), 476-488. Available online at https://doi.org/10.34218/IJM.11.6.2020.041

Decree of the President of Ukraine 392/2020. On the decision of the National Security and Defense Council of Ukraine. On the National Security Strategy of Ukraine. Dated September 14, 2020, URL: https://www.president.gov.ua/documents/3922020-35037 (In Ukranian).

Decree of the President of Ukraine 449/2014. On the decision of the National Security and Defense Council of Ukraine. On measures to improve the formation and implementation of state policy in the field of information security of Ukraine. Dated May 1, 2014. URL: http://www.zakon5.rada.gov.ua/laws/show/n0004525-14 (In Ukranian).

Decree of the President of Ukraine 685/2021. On the decision of the National Security and Defense Council of Ukraine. On the Information Security Strategy of Ukraine, Dated December 28, 2021, URL: https://zakon.rada.gov.ua/laws/show/685/2021#n7 (In Ukranian).

Horska, K., Dosenko, A., Iuksel, G., Yuldasheva, L., & Solomatova, V. (2023).

Internet platforms as alternative sources of information during the russian-Ukrainian war. Amazonia Investiga, 12(62), 353-360. https://doi.org/10.34069/AI/2023.62.02.36

Khmelevskyi, R. (2016). Research on the assessment of threats to information security of objects of information activity. Modern information protection, 4, 65-70. URL: http://journals.dut.edu.ua/index.php/dataprotect/article/view/1250 (In Ukranian).

Kostenko, S., Strilchu, V., Chernysh, R., & Buchynska, A. (2021). The threats to national security of Ukraine and Poland in assisting to the development of the crypto-asset market: LEGAL ASPECT. Management Theory and Studies for Rural Business and Infrastructure Development, 43(2), 225-236. Retrieved from https://ejournals.vdu.lt/index.php/mtsrbid/article/view/1436

Law 2469-VIII. On the National Security of Ukraine. Bulletin of the Verkhovna Rada of Ukraine, dated June 21, 2018, No. 31, Art. 241. Url: https://zakon.rada.gov.ua/laws/show/2469-19#Text (In Ukranian).

Law 254к/96-ВР. Constitution of Ukraine. Bulletin of the Verkhovna Rada of Ukraine, dated June 28, 1996, No. 30, Art. 141. Url: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text (In Ukranian).

Lipkan, V. (2009). National security of Ukraine: education. manual. Kyiv: Condor. 280 p.

Lipkan, V., Maksymenko, Yu. E., & Zhelikhovskyi, V.M. (2006). Information security of Ukraine in the conditions of European integration: training. manual Kyiv: KNT. 280 p. URL: https://www.dut.edu.ua/ua/lib/1/category/1181/view/1350 (In Ukranian).

Petryk, V., Bed, V.V., & Prysiazhniuk, M.M. (2018). Informational and psychological conflict: a textbook. The second edition translated, supplemented and revised. 386 p. URL: https://acortar.link/qeae3o (In Ukranian).

Pirozhkov, S. (2016), The civilizational choice of Ukraine: a paradigm of understanding and a strategy of action: a national report. Institute of Political and Ethnonational Studies named after I.F. Curacao of the National Academy of Sciences of Ukraine. Kyiv: NAS of Ukraine, 284 p. URL: https://acortar.link/7WKbpG (In Ukranian).

Pocheptsov, H. (2015). Modern information wars. Kyiv: Pub. house «Kyiv-Mohyla Academy». 497 p. URL: https://acortar.link/3yoWvK (In Ukranian).

Prysiazhniuk, M. (2014). Course of lectures on the educational discipline «Information security of the state». Center for educational, scientific and periodical publications. 244 p. Url: https://academy.ssu.gov.ua/uploads/p_57_92823860.pdf (In Ukranian).

Shilin, M., Shmotkin, O., Chernysh, R., Chekhovska, M., & Konyk, T. (2023). Theoretical and legal basis for the implementation of state policy on national security of Ukraine. Amazonia Investiga, 12(64), 57-64. https://doi.org/10.34069/AI/2023.64.04.5

Shilin, M., Shmotkin, O., Chernysh, R., Konyk, T., & Botvinkin, O. (2022). Formation and formulation of state policy to ensure national security: theoretical and legal aspects. Amazonia Investiga, 11(57), 152-161. https://doi.org/10.34069/AI/2022.57.09.16

Tikhomirov, O. (2023). Human rights: information dimension: monograph. Odesa: Yuridyka Publishing House. 304 p. URL: http://ippi.org.ua/sites/default/files/tihomirov_o.o._prava_lyudini_print.pdf (In Ukranian).