UDC 351.746:007 DOI: 10.31673/2412-4338.2023.0101111

Lehominova S.V., Shchavinskyy YU.V., Muzhanova T.M., Dzyuba T.M., Rabchun D.I.
State University of Telecommunications, Kyiv

LEGAL MECHANISMS FOR ENSURING INFORMATION SECURITY IN UKRAINE IN THE CONDITIONS OF HYBRID WAR

Abstract. *The article provides an analysis of legal regulation of information security in Ukraine compared to some foreign countries legislative practices. Based on the analysis, the main problems of legislative regulation of information security are identified, which are common for many countries around the world. These problems include discrepancies in international rules of behavior in cyberspace, which do not allow to apply legal mechanisms for joint action effectively, as well as inconsistency of responsibilities for violations of information security in conditions of hybrid warfare. The authors also identify the peculiarities of legal regulation of information security and ways to solve these problems, which include the development and implementation of legislative provisions regulating activities on the Internet, including the national segment, and special requirements for network providers and other subjects that ensure the functioning of the network in conditions of war. The results of research on normative and legal support for information security in the conditions of hybrid warfare indicate the need to apply a systematic approach to the improvement of legislation in this direction. There is a need for legislative consolidation of special information security mechanisms to implement complex measures aimed at preventing cyberattacks and negative information influences on society; strengthening responsibility for cybercrime, abuse and neglect of information security measures; legislative consolidation of mechanisms for legal regulation of information relations in cyberspace; reinforcing cooperation with the international community to counteract information threats. It is proposed to take into account factors to ensure effective regulatory support in the context of a hybrid war. The necessity of conducting scientific research on the development of proposals for improving domestic legislation on the basis of international agreements and the implementation of their provisions in domestic legislation regarding information security is determined.*

Keywords: *information security, cybersecurity, regulatory and legal support, hybrid warfare* **.**

Легомінова С.В., Щавінський Ю.В., Мужанова Т.М., Дзюба Т.М., Рабчун Д.І.
Державний університет телекомунікацій, Київ

ПРАВОВІ МЕХАНІЗМИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ В УМОВАХ ГІБРИДНОЇ ВІЙНИ

Анотація. *У статті зроблений аналіз вітчизняних досліджень стану та особливостей нормативно-правового забезпечення інформаційної безпеки у порівнянні із зарубіжними країнами. За результатами аналізу визначені основні проблеми законодавчого забезпечення інформаційної безпеки, що є актуальними для багатьох країн світу. Вони полягають у*

розбіжності міжнародних правил поведінки в кіберпросторі, що не дозволяє ефективно застосовувати правові механізми для сумісних дій, вказують на недостатню ефективність посилення норм відповідальності за порушення інформаційної безпеки в умовах гібридної війни. Визначені особливості правового регулювання забезпечення інформаційної безпеки та шляхи вирішення проблем, які полягають у розробленні та впровадженні законодавчих норм, що регулюють діяльність в мережі Інтернет, у тому числі й у національному сегменті, та повинні включати особливі вимоги до провайдерів мережевого зв'язку та інших суб'єктів, які забезпечують функціонування мережі в умовах воєнного стану. Визначена потреба у законодавчому закріпленні особливих механізмів інформаційної безпеки для організації ы здійснення превентивних законодавчих заходів з метою попередження кібератак та інформаційного впливу на суспільство в особливих умовах гібридної війни, які включають особливості функціонування суб'єктів інформаційної безпеки в умовах воєнного стану, посилення співпраці з міжнародною спільнотою у відповідності з міжнародними угодами. Запропоновано врахування факторів для забезпечення ефективного нормативно-правового забезпечення в умовах гібридної війни. Визначена необхідність проведення наукових досліджень з розробки пропозицій щодо вдосконалення вітчизняного законодавства на основі міжнародних угод та імплементації їх положень в національне законодавство щодо забезпечення інформаційної безпеки.

Ключові слова: *інформаційна безпека, нормативно-правове забезпечення, гібридна війна, кібербезпека.*

1. Introduction

Formulation of the problem. Because of the global surge of information technologies in all spheres of human, societal, and state activities, information has become a crucial factor, and in the conditions of modern global and regional information confrontations, it is a tool of destructive communicative influences, manipulation, informational expansion, and aggression. In the conditions of a hybrid war, a state that has become the object of aggression inevitably faces a wide range of information threats, the neutralization of which, on the one hand, requires the implementation of extraordinary legal, administrative, organizational, and technical measures, and on the other hand, may be accompanied by a curtailment of democratic rights and freedoms. The information environment becomes a front for conducting hybrid combat operations. As a result, information is subject to various threats, including illegal collection of information, dissemination of disinformation, use of propaganda means, informational and psychological influence of the aggressor country on its own people, the population of the state that is the object of aggression as well as on the international community [1-3].

The list of information threats shows that information security has to combine two aspects: technical and psychological. In the conditions of a hybrid war, it is necessary to ensure protection not only against cyberattacks and malicious software but also from propaganda, fake news and other types of negative information influences, that can be used as means of military aggression.

The peculiarity of normative and legal support of information security in the conditions of a hybrid war is that information security becomes an integral part of national security and requires a systemic approach to ensuring protection against various threats in the cyberspace. In addition, in the conditions of a hybrid war, the development and implementation of legal acts take place in circumstances of instability when the situation on the front line can change suddenly, requiring

constant updating and refinement of legal norms and standards. It is also worth noting that in a hybrid war, the military component consists of technological and psychological aspects, which requires the development of complex measures aimed at ensuring information security. Therefore, regulatory and legal support of information security should ensure solving complex and multifaceted problems, taking into account the characteristics of hybrid warfare. To solve the problems, it is necessary to analyze the state of domestic legal support, conduct scientific research and develop proposals for improving legislative acts in peacetime with the aim of organizing and conducting preventive measures.

2. Analysis of literary data and statement of the problem.

However, as noted by researchers, issues of legislative support for information security are relevant concerns for many countries around the world. Today, most countries have a cyber security strategy. However, these strategies are mostly static documents that do not or only partially can handle the dynamism that characterizes cyberspace [4].

Authors [5-7] point out the discrepancies in legislation regarding information security in different countries, which may lead to difficulties in determining the scope and measures of protection required for a state and its citizens. Insufficient information security laws in some countries leave a lot of information unprotected, which can negatively affect their national security, as well as the security of neighboring states, given the circulation of information in cyberspace.

The author of the paper [5] examines possible cyberthreats and suggests that cyberwar can be as serious a threat to national security as traditional war. He proposes several legal measures to ensure information and cybersecurity and prevent possible cyberattacks, including: establishment of international rules of conduct in cyberspace, which set standards for the use of cyberweapons and other means of cyberattacks; recognition of cyberattacks as crimes at the national legislative level and establishment of appropriate sanctions for their commission.

In the work [6], there are proposed some measures that should provide a legal framework for the use of cryptography and information protection in various areas of activity: development and establishment of cryptographic standards for information protection in various areas, including telecommunications, financial transactions, and others; regulation of the use of cryptography in different countries, including control over the export of cryptographic products and technologies to prevent their use for criminal and terrorist purposes; establishing responsibility for violating the rules of using cryptography, including unauthorized access to protected information.

The author of many articles and books on information security and cybersecurity in his research [7] proposes the following measures of legal regulation:

- development of international treaties and agreements on cybersecurity, which would establish standards and rules of behavior in cyberspace and regulate the interaction of states;
- foundation of specialized international organizations that would coordinate measures to ensure cybersecurity and combat cybercrime;
- development of agreed national laws and policies that would provide protection against cyberattacks and ensure responsibility for cybercrime;
- implementation of cybersecurity measures at the level of corporations and organizations to protect against internal and external threats;
- ensuring the availability of advanced cybersecurity technologies for states and organizations;
- raising the level of cybersecurity at the level of individuals by popularizing knowledge of cybersecurity and safe behavior on the Internet;

- legislative provision of effective cooperation between state agencies, the private sector, and research institutions to identify and respond to cyberthreats.

As the previous review of legislation and research on information security has shown, such problems are solved in different ways in different countries. In some countries, legislative reforms are being carried out to improve laws on information security and introduce stricter sanctions for their violation. Other countries actively use various technologies and tools of control and protection of important information, such as secure data storage systems and cryptographic solutions.

At the same time, the vast majority of countries actively cooperate with other countries and international organizations in the field of information security, in particular by creating alliances and other forms of international cooperation to exchange information and experience in the fight against cyberthreats. For example, in the US, the National Cybersecurity and Communications Integration Center has been created, which brings together representatives of various government agencies and private companies to coordinate measures for protecting critical information systems. The British Parliament has a Committee on Intelligence and Security, which monitors the activities of intelligence services and ministries in relation to national security. The European Union Agency for Cybersecurity (ENISA) provides advice and support in the field of cybersecurity for the European Union member states [8].

In many countries, mechanisms of self-regulation and interaction between the state and the private sector in the field of information security are also functioning. For example, private companies can use their own security measures to protect corporate data and systems, and collaborate with government agencies to combat cyberthreats. Governments of some countries have adopted legislation aimed at improving the qualifications and effectiveness of specialists responsible for information and cybersecurity, which includes training and education to master information protection competencies.

Thus, solving the problems of legislative support for information security in foreign countries may differ, but their solutions involve a comprehensive approach, which includes the implementation of strict legislative mechanisms, the use of modern technologies, the improvement of specialists' qualifications, coordination between government agencies and the private sector, and international cooperation.

3. The purpose and objectives of the research

The purpose of the article is to determine the legal mechanisms for ensuring information security in the conditions of hybrid warfare. To achieve the goal, it is necessary to complete the following tasks:

to analyze the legislative provision of information security in advanced foreign countries;

to analyze the current state of regulatory and legal provision of information security in Ukraine;

determine the peculiarities of the legal regulation of information security, the need to take into account the factors and propose ways to solve problems in the conditions of hybrid warfare.

4. Research results

4.1. Analysis of legislative provision of information security in advanced foreign countries

The development of information technologies, increasing the importance of information, and expanding the scale of cybercrime have forced countries around the world to address information security at the legislative level. Legal regulation of information security in foreign countries is

typically carried out through national laws and international agreements. The level of detail and scope of legal regulation may vary depending on the specific country.

For example, the United States ensures information security through federal legislation that regulates the protection of information infrastructure systems from cyberattacks and other threats. An important legislative act is the Computer Fraud and Abuse Act of 1986, which defines criminal liability for computer misuse. The US also has laws on the protection of PII (Personally Identifiable Information) and the world-renowned NIST cybersecurity standards. Several agencies responsible for ensuring information security operate in the US, such as the National Cybersecurity Center and the Department of Homeland Security.

In the European Union, information security is regulated by laws related to personal data protection and cyberdefense, such as the General Data Protection Regulation (GDPR) and the Network and Information Security Directive (NIS 2).

In Japan information security is regulated by the Personal Information Protection Act, as well as documents related to cybersecurity in special fields, such as banking and medicine.

The issue of information security is also regulated at the international level. Thus, the United Nations (UN) adopted the Convention on Cybercrime, which was signed by more than 60 countries of the world. This Convention defines the types of cybercrime, regulates rules on jurisdiction, cooperation and other issues related to cybercrime.

4.2. Analysis of regulatory and legal provision of information security in Ukraine

The existing system of normative and legal acts in the field of information security in Ukraine is aimed at regulating the relations between information security subjects, ensuring their legal status, establishing the procedure for the use of forces and means to ensure information security, as well as coordinating and interacting between state bodies and other entities involved in ensuring information security in Ukraine, both at the national and international levels. Domestic regulatory framework on information security consists of Laws of Ukraine, Resolutions of the Verkhovna Rada and the Cabinet of Ministers, decrees of the President of Ukraine, normative documents in the field of technical protection of information, and state standards regarding the creation and functioning of a comprehensive information protection system.

Information security within the framework of information legislation is considered from the perspective of protecting the vital interests of individuals, society, and the state, and emphasizing the threats to these interests and the mechanisms for eliminating or preventing such threats by legal methods. Domestic legislation that regulates the issues of information security reflects various aspects of the state policy of information security as a mechanism for achieving the necessary conditions for life activities of society and functioning of the state in the information space. The Constitution of Ukraine declares ensuring information security as the responsibility of all Ukrainian people [9].

Constitutional provisions became decisive for the development of a package of normative and legal acts necessary for the effective ensuring information security in Ukraine, which takes into account the main requirements of international treaties and agreements ratified by the Verkhovna Rada of Ukraine. National interests of Ukraine in the information sphere, threats to their implementation, directions, and priorities of state policy in the information sphere are determined in the Doctrine of Information Security of Ukraine approved by the Decree of the President of Ukraine on February 25, 2017 [10].

Some aspects of information security are outlined in the Law of Ukraine "On National Security of Ukraine," which defines the direction of the state policy of national security and defense to ensure

information and cybersecurity of Ukraine, as well as the tasks of the Security Service of Ukraine in ensuring information and cybersecurity of the state [11].

The Law of Ukraine "On Information" [12] is important for ensuring information security of Ukraine, because it establishes Ukraine's information sovereignty, enshrines the right to information and access to it, defines the system of relations and obligations in this field, and provides for disciplinary, civil, administrative, or criminal liability for violations of information legislation.

In the Law of Ukraine "On State Secrets" are clearly described the key principles of protection of state secrets for the purpose of national and information security of Ukraine, in particular public relations regarding classification of information as a state secret, classification and declassification of its physical media, compliance with the law on state secrets [13].

The issues of information protection in the systems of information processing and transmission, relations between subjects of information protection, the powers of state bodies in this field are regulated the Law of Ukraine "On Protection of Information in Information and Telecommunication Systems" [14].

Important legal acts that regulate the ensuring state information security include mandatory regulatory and technical documents - State Standards of Ukraine (DSTU), as well as regulatory acts of ministries, departments, and other government bodies. These include, among others, DSTU 3254-95 "Radio communication. Terms and definitions", DSTU 3560-97 "Space and satellite radio communication. Terms and definitions", DSTU 4361:2004 "Digital cellular radio communication systems. Terms and definitions" and so on.

Thus, the existing system of regulatory acts in the field of information security of Ukraine is aimed at regulating the coordination and interaction of government bodies and other entities ensuring the information security of Ukraine at both national and international levels. However, the level of implementation of these legal acts remains insufficient due to the imperfection of legislation in terms of monitoring compliance with requirements, low level of safety culture among the population and organizations.

Analysis of the Law of Ukraine "On Critical Infrastructure", which defines the legal and organizational principles of creating and functioning the national critical infrastructure protection system, has shown that despite the importance of information tools in modern wars and conflicts, the Law does not pay sufficient attention to legislative consolidation of the definition of critical information infrastructure objects. As noted in [15], the information component is considered only as "information services" and "electronic communications", which belong to vital functions and/or services, the violation of which leads to negative consequences for the national security of Ukraine.

There are also some inconsistencies in other normative legal acts. According to the results of studies [15-16], certain shortcomings have been identified in the Law of Ukraine "On Basic Principles of Cybersecurity of Ukraine." In particular, it does not define the criteria for classifying organizations (regardless of ownership form) as critical information infrastructure objects. As a result, information systems, information and telecommunications networks, and automated management systems belonging to these organizations are not mentioned, based on the Procedure for forming the list of critical information infrastructure objects, which was approved by the Resolution of the Cabinet of Ministers of Ukraine dated October 9, 2020, No. 943 "Certain Issues of Critical Information Infrastructure Objects." Such vagueness slows down the identification of critical information systems and reduces the level of effectiveness of ensuring information security.

4.3. Peculiarities of legal regulation of information security in conditions of hybrid warfare

The conditions of hybrid warfare require the state to develop and implement effective legal mechanisms to ensure information security. Legislative acts that regulate information security issues in the conditions of hybrid warfare should determine the legal basis for the special functioning of the cybersecurity system and the powers of the state authorities, regulate legal relations in the field of cybersecurity under these conditions, enshrine enhanced standards and rules for collecting, processing, storing, and transmitting information, and also establish increased responsibility for violating these rules. Regulatory acts in the field of information security should establish special cybersecurity standards for certain industries, rules for working with confidential information, and so on.

The specificity of legal mechanisms in the conditions of hybrid warfare lies in the fact that these processes must be aimed at preventing and countering the use of information technologies to carry out aggression, as well as protecting against new forms of information security threats. Such mechanisms must be dynamic, i.e. quickly adapt to changing conditions and threats.

Special legal mechanisms for ensuring information security of the state in the conditions of hybrid warfare have to be related to response to information security threats from foreign subjects and the actions of their agents in the Ukrainian information space. One example of such mechanisms is the development and implementation of legislation that regulates activity of various subjects on the Internet, including the national segment of the network. This legislation must include special requirements for network service providers and other entities that ensure network operation under conditions of martial law to protect national security.

In addition, development and implementation of mechanisms for international cooperation in the field of information security can be considered as special legal instrument that allow solving problems of preventing information security threats and combating cybercrime on a global scale.

One of the key features of regulatory and legal support for information security in the conditions of hybrid warfare is the need to develop new approaches and strategies to combat new forms of information threats. This may involve creating new laws and regulations that regulate cybersecurity in wartime, as well as developing new technologies and methods for protection against cyberattacks and negative information influences, implementing special economic and information regimes in a conflict zone, which allow the state to provide additional measures of control and restriction in the field of economic and information activity in this territory.

5. Discussion of the results of the study of the peculiarities of the functioning of legal mechanisms for ensuring information security in the conditions of hybrid warfare

In the conditions of hybrid warfare, it may be appropriate to form temporary information structures that are responsible for ensuring the operational exchange of information between the military, law enforcement and other state agencies in order to quickly and effectively respond to new information threats. Such structures, in order to carry out special monitoring and protection measures against cyberattacks, must be equipped with special cybertools. Their legislative consolidation and development of regulatory and legal documentation will ensure the implementation of preventive measures for information security and will be a sign of the state's readiness to defend itself in cyberspace for any adversary.

It is advisable to legislatively recognize the ensuring information security of Ukraine as a complex of systemic preventive and countermeasures that provide guarantees for the protection of the vital interests of individuals, society, and the state from cyberattacks and negative information influences associated with information warfare.

In addition, the state should actively cooperate in the field of information security with foreign partners and international organizations such as NATO, the EU, OSCE, and others. This cooperation may include information and experience exchange, joint training and education, project and program development, and collective efforts to reduce cyberthreats and the impact of negative information influences.

To ensure effective regulatory and legal support in the conditions of hybrid warfare, the following factors need to be taken into account.

International aspect. Hybrid warfare can take place not only within one country but also between different countries. Therefore, it is necessary to develop international norms and standards for information security.

Comprehensiveness. Regulatory and legal support for information security should be comprehensive and include not only legislative but also organizational, technical, and other measures.

Adaptability. The rapid development of technology requires constant analysis and updating of the regulatory and legal framework to ensure protection against new information threats.

Cooperation between the state and the private sector. Regulatory and legal support for information security should include cooperation between the public and private sectors since most critical infrastructures belong to the private sector.

Identified problems in the field of legal regulation of information security and proposed ways to solve them in the conditions of hybrid warfare require detailed scientific research and development of proposals for changes to domestic legislation.

6. Conclusion

Thus, alongside the achievements in improving legal mechanisms in the field of information security, there are still many problems that require urgent regulation in the legal field, taking into account the modern challenges associated with the hybrid war against Ukraine.

The results of the analysis of research on normative and legal support for information security in the conditions of hybrid warfare indicate the need to apply a systematic approach to the improvement of legislation in this direction. There is a need for legislative consolidation of special information security mechanisms to organize complex measures aimed at preventing cyberattacks and negative information influences on society; strengthening responsibility for cybercrime, abuse and neglect of information security measures; legislative consolidation of mechanisms for legal regulation of information relations in cyberspace; and strengthening cooperation with the international community in accordance with international agreements.

References:

1. Informatsiyna bezpeka derzhavy u konteksti protydiyi informatsiynym viynam: Navchal′nyy posibnyk / Za zah. red. V. B. Tolubka. – K.: NAOU, 2004. – 315 s. (in Ukrainian).

2. Grabusts P., Zorins A., Teilans A. Informational warfare – influence on informational structures. In *Vide. Tehnologija. Resursi - Environment, Technology, Resources.* 2019. Vol. 2, pp. 56–60. Rezekne Higher Education Institution. https://doi.org/10.17770/etr2019vol2.4035 (date of access: 12.03.2023).

3. Maskun, Rum R. A. Cyber warfare: national security in dealing with changing method of war. *Kanun Jurnal Ilmu Hukum.* 2021. Vol. 23, Issue 3, pp. 477-490. https://doi.org/10.24815/kanun.v23i3.22371 (date of access: 22.03.2023).

4. Kovács L. National Cyber Security as the Cornerstone of National Security. *Land Forces Academy Review*. 2018. 23(2) 113-120. https://doi.org/10.2478/raft-2018-0013 (date of access: 22.03.2023).

5. Clarke R., Knake R., Borah, C. Cyber war: the next threat to national security and what to do about it?, *Strategic Analysis*. 2015. 39:4, 458-460, https://doi.org/10.1080/09700161.2015.1047221 (date of access: 25.03.2023).

6. Schneier B. Applied Cryptography, Second Edition: Protocols, Algorthms, and Source Code in C. *Wiley*. 2015. 758 p. https://doi.org/10.1002/9781119183471 (date of access: 24.03.2023).

7. Marlin-Bennett R. Cyber Peace: Is That a Thing?, in Cyber Peace: Charting a Path Toward a Sustainable, Stable, and Secure Cyberspace, S. J. Shackelford, F. Douzet, and C. Ankersen, Eds. Cambridge: *Cambridge University Press*, 2022, pp. 3–21. https://doi.org/10.1017/9781108954341.001 (date of access: 24.03.2023).

8. European Network and Information Security Agency (ENISA). NCSS Good Practice Guide Designing and Implementing National Cyber Security Strategies. 2016. available at: https://www.enisa.europa.eu/publications/ncss-good-practice-guide/at_download/fullReport (date of access: 27.03.2023).

9. Konstytutsiya Ukrayiny. Vidomosti Verkhovnoyi Rady Ukrayiny. – 1996. – № 30. – St. 141 URL: https://zakon.rada.gov.ua/go/254k/96-vr/ (date of access: 13.03.2023) (in Ukrainian).

10. Pro rishennya Rady natsional′noyi bezpeky i oborony Ukrayiny vid 29 hrudnya 2016 roku «Pro Doktrynu informatsiynoyi bezpeky Ukrayiny». Ukaz prezydenta Ukrayiny vid 25 lyutoho 2017 roku № 47/2017. URL: https://www.president.gov.ua/documents/472017-21374#Text (date of access: 13.03.2023) (in Ukrainian).

11. Pro natsional′nu bezpeku Ukrayiny. Zakon Ukrayiny. (Vidomosti Verkhovnoyi Rady (VVR), 2018, № 31, st.241) URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text (date of access: 15.03.2023) (in Ukrainian).

12. Pro informatsiyu. Zakon Ukrayiny. (Vidomosti Verkhovnoyi Rady Ukrayiny (VVR), 1992, № 48, st.650). URL: https://zakon.rada.gov.ua/go/2657-12#Text (date of access: 16.03.2023) (in Ukrainian).

13. Pro derzhavnu tayemnytsyu. Zakon Ukrayiny. (Vidomosti Verkhovnoyi Rady Ukrayiny (VVR), 1994, № 16, st.93). URL: https://zakon.rada.gov.ua/go/3855-12 (date of access: 16.03.2023) (in Ukrainian).

14. Pro zakhyst informatsiyi v informatsiyno-telekomunikatsiynykh systemakh. Zakon Ukrayiny. (Vidomosti Verkhovnoyi Rady Ukrayiny (VVR), 1994, № 31, st.286). URL: https://zakon.rada.gov.ua/go/80/94-vr (date of access: 16.03.2023) (in Ukrainian).

15. Malashko, O. YE. Administratyvno-pravovi zasady zabezpechennya informatsiynoyi bezpeky v Ukrayini u konteksti yevropeys′koyi intehratsiyi: dys. … kand. yur. nauk : 12.00.07. L′viv, 2020. 200 s. https://mydisser.com/ua/catalog/view/6/352/533061.html (date of access: 16.03.2023) (in Ukrainian).

16. Kovaliv M., Skrynkovskyy R., Nazar Y., Yesimov S., Krasnytskyi I., Khrystyna K., Kniaz S., Kemska Y. Legal Support of Cybersecurity of Critical Information Infrastructure of Ukraine. *Traektoriâ Nauki= Path of Science*. 2021. Vol. 7.No 4. Зз. 2011-2018. https://doi.org/10.22178/pos.69-12 (date of access: 20.03.2023).

Список використаної літератури:

1. Інформаційна безпека держави у контексті протидії інформаційним війнам: Навчальний посібник / За заг. ред. В. Б. Толубка. – К.: НАОУ, 2004. – 315 с.

2. Grabusts P., Zorins A., Teilans A. Informational warfare – influence on informational structures. In Vide. *Tehnologija. Resursi - Environment, Technology, Resources*. 2019. Vol. 2, pp. 56–60. Rezekne Higher Education Institution. https://doi.org/10.17770/etr2019vol2.4035 (дата звернення: 12.03.2023).

3. Maskun, Rum R. A. Cyber warfare: national security in dealing with changing method of war. *Kanun Jurnal Ilmu Hukum*. 2021. Vol. 23, Issue 3, pp. 477-490. https://doi.org/10.24815/kanun.v23i3.22371 (дата звернення: 22.03.2023).

4. Kovács L. National Cyber Security as the Cornerstone of National Security. *Land Forces Academy Review*. 2018. 23(2) 113-120. https://doi.org/10.2478/raft-2018-0013 (дата звернення: 22.03.2023).

5. Clarke R., Knake, R, Borah C. Cyber war: the next threat to national security and what to do about it?, *Strategic Analysis.* 2015. 39:4, 458-460, https://doi.org/10.1080/09700161.2015.1047221 (дата звернення: 25.03.2023).

6. Schneier B. Applied Cryptography, Second Edition: Protocols, Algorthms, and Source Code in C. *Wiley*. 2015. 758 p. https://doi.org/10.1002/9781119183471 (дата звернення: 24.03.2023).

7. Marlin-Bennett R. Cyber Peace: Is That a Thing?, in Cyber Peace: Charting a Path Toward a Sustainable, Stable, and Secure Cyberspace, S. J. Shackelford, F. Douzet, and C. Ankersen, Eds. Cambridge: *Cambridge University Press*, 2022, pp. 3–21. https://doi.org/10.1017/9781108954341.001 (дата звернення: 24.03.2023).

8. European Network and Information Security Agency (ENISA). NCSS Good Practice Guide Designing and Implementing National Cyber Security Strategies. 2016. available at: https://www.enisa.europa.eu/publications/ncss-good-practice-guide/at_download/fullReport (дата звернення: 27.03.2023).

9. Конституція України. Відомості Верховної Ради України. – 1996. – № 30. – Ст. 141.URL: https://zakon.rada.gov.ua/go/254к/96-вр (дата звернення: 13.02.2023).

10. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України». Указ президента України від 25 лютого 2017 року № 47/2017. URL: https://www.president.gov.ua/documents/472017-21374#Text (дата звернення: 13.03.2023).

11. Про національну безпеку України. Закон України. (Відомості Верховної Ради (ВВР), 2018, № 31, ст.241) URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text (дата звернення: 15.03.2023).

12. Про інформацію. Закон України. (Відомості Верховної Ради України (ВВР), 1992, № 48, ст.650). URL: https://zakon.rada.gov.ua/go/2657-12#Text (дата звернення: 16.03.2023).

13. Про державну таємницю. Закон України. (Відомості Верховної Ради України (ВВР), 1994, № 16, ст.93). URL: https://zakon.rada.gov.ua/go/3855-12 (дата звернення: 16.03.2023).

14. Про захист інформації в інформаційно-телекомунікаційних системах. Закон України. (Відомості Верховної Ради України (ВВР), 1994, № 31, ст.286). URL: https://zakon.rada.gov.ua/go/80/94-вр (дата звернення: 16.03.2023).

15. Малашко, О. Є. Адміністративно-правові засади забезпечення інформаційної безпеки в Україні у контексті європейської інтеграції: дис. … канд. юр. наук : 12.00.07. Львів, 2020. 200 с. https://mydisser.com/ua/catalog/view/6/352/533061.html (дата звернення: 16.03.2023).

16. Kovaliv, M. & Skrynkovskyy, R, & Nazar, Y. & Yesimov, S. & Krasnytskyi,I. Khrystyna K. & Kniaz, S. & Kemska, Y. (2021). Legal Support of Cybersecurity of Critical Information Infrastructure of Ukraine. *Traektoriâ Nauki= Path of Science*. 2021. Vol. 7.No 4. 3з. 2011-2018. https://doi.org/10.22178/pos.69-12 (дата звернення: 20.03.2023).