Legal basis for cybersecurity in Ukraine under martial law

Mykola Legenkyi[1,*,†], Liudmyla Piankivska[1,†] and Andrii Tolbatov[2,†]

[1] National Aviation University, Liubomyra Huzara Ave. 1, Kyiv, 03058, Ukraine
[2] Sumy National Agrarian University, Herasyma Kondratieva Str., 160, Sumy, 40000, Ukraine

Abstract

The article is devoted to the issues of security in cyberspace of Ukraine. It highlights the vision of understanding and essence of the concept of cybersecurity. It is emphasized that martial law in the country has actualized the issues in this area and increased its risks in cyberspace. The author characterizes international legal acts in the field of cybersecurity, in particular, those of the EU, which are aimed at countering hybrid cyber threats. A number of current regulatory documents that form the legal basis in the field of cybersecurity in Ukraine are analyzed. The essence of the existing legal acts in this area is systematized and defined. It is noted that the changes made to the regulatory legal acts are aimed at strengthening the cyber defense capabilities under martial law.

Keywords

cybersecurity, cyberspace, cybercrime

1. Introduction

The intensive development of information technology and digitalization has contributed to the formation of global cyberspace, which has not only unlimited potential, but also acts as a driving force on a global scale. Today, this process affects every citizen, society, and state, as a complex network of information and communication flows eliminates distances and has a deeper impact on their lives. A new space for conducting legal relations and solving urgent life issues is being formed at the global level. We are witnessing a transformation in the speed and efficiency of information transmission, simplification of access to information resources, and a significant increase in the number of social media users who are able to simultaneously receive and transmit information of various volumes. In general, in today's environment, cyberspace is an effective means of international cooperation, a powerful engine of social governance in the country, and has an unprecedented impact on the national security of the state. In fact, the capabilities of cyberspace have increased the risks of cyber threats, caused a massive and diverse impact on people, and have the ability to undermine fundamental democratic values and freedoms. They can cause and exacerbate the escalation of hostilities in cyberspace, provoke and spread innovative forms of aggression.

Thus, in the course of the hybrid war in Ukraine, cyber threats have had the highest level of negative impact on government agencies and critical infrastructure. The results of statistical studies by experts show that all cyberattacks on Ukraine by the aggressor country had a generally destructive impact, and the number of such cyber incidents increased 2.8 times compared to 2021 [1]. In 2022, 2194 cyberattacks were officially registered in the country [2]. In general, they are aimed at the energy and financial sectors, security and defense, logistics, telecommunications, etc. In particular, in December 2023, experts recorded 170,000 attempts at various vulnerabilities [3].

CH&CMiGIN'24: Third International Conference on Cyber Hygiene & Conflict Management in Global Information Networks, January 24–27, 2024, Kyiv, Ukraine
* Corresponding author.
† These authors contributed equally.
legenkyj@ukr.net (M. Legenkyi); fontan.vv@gmail.com (L. Piankivska); tolbatov@ukr.net (A. Tolbatov)
0000-0003-4179-1964 (M. Legenkyi); 0000-0001-9086-271X (L. Piankivska); 0000-0002-9785-9975 (A. Tolbatov)

It can be argued that cyber threats have not only become widespread, but as a dynamic construct, they have immediate and remote effects. They are a means by which the security of the state is undermined and the stability of society is leveled.

Thus, we can state that in the current realities of the war in Ukraine, cyber warfare and cyber defense are key aspects of hybrid warfare. That is why the issue of ensuring national security, preserving the territorial integrity of the state, protecting democratic processes, information networks of the state and its citizens is becoming acute. Therefore, in view of the new challenges, the issue of rapid response to cyber threats and the definition of a legal basis for cybersecurity in Ukraine requires attention.

2. Analysis of recent research and publications

The theoretical analysis of scientific works shows that the problem of determining the legal basis in the field of cybersecurity in wartime is becoming increasingly relevant and attracts the attention of not only information policy and security experts, but also scientists, lawyers and other researchers.

The concept of "cybersecurity" is a complex component of the information society. It is a set of various processes, practical tips and technological solutions that help protect important systems and networks from cyberattacks [4].

The current Law of Ukraine "On the Basic Principles of Ensuring Cybersecurity of Ukraine" defines cybersecurity as "...protection of vital interests of a person and citizen, society and the state during the use of cyberspace, which ensures the sustainable development of the information society and digital communication environment, timely detection, prevention and neutralization of real and potential threats to the national security of Ukraine in cyberspace" [5].

It should be noted that E. Kotukh believes that cybersecurity includes a number of different practices, including: risk assessment, penetration testing; cryptography; disaster recovery; access control and monitoring; network architecture, software and security; various security operations; physical security, etc. [6]. The researcher emphasizes that cybersecurity itself consists of information and communication systems to counter attacks, methods and systems for detecting threats in order to maintain the stability of information and communication systems and ensure a systematic response to cyberattacks [6].

The scientific works of Ukrainian scholars comprehensively outline the issue of cybersecurity. In particular, they consider the peculiarities of interpreting the concept of "cybersecurity" in modern legal science (G. Foros, V. Zhogov) [7], analyze the content and characteristics of cybersecurity in accordance with current regulations (I. Sopilko) [8].

The authors also describe cybersecurity as a direction of Ukraine's Euro-Atlantic integration (A. Voitsikhovsky) [9]. The range of issues of its implementation in the system of public authorities is determined (O. Skybun) [10]. In addition, cyberterrorism is highlighted as a threat to the information sovereignty of the state (O. Dovhan, V. Khlan) [11], the essence of the state policy in the field of combating cybercrime is considered (A. Didenko) [12], scientific and practical measures to combat cybercrime at the national and corporate levels are characterized (I. Revak and R. Gren) [13], etc.

In our opinion, in Ukraine, the process of forming a legal basis for regulating processes and relations in the field of cybersecurity is rapidly undergoing dynamic transformational changes in the context of war. That is why lawyers are faced with the question of implementing a well-thought-out and effective legal and regulatory basis in cyberspace to ensure national security.

The purpose of the article is to determine the legal basis in the field of cybersecurity in wartime as a priority component of the national security system of the state.

3. Research methods

The article uses a set of interrelated scientific theoretical methods to study the issue: the method of analysis, interconnection, systematization, generalization and interdependence, as well as comparative legal and comparative methods. The author has studied various legal acts and scientific

sources, analyzed statistical data, and considered different views of scholars on the views and interpretation of the same data. The applied theoretical research methods are aimed at integrating the knowledge gained into a single system of vision of the problem.

4. Summary of the primary material

After the outbreak of full-scale military aggression against Ukraine, the State has faced the need to rapidly transform effective approaches to martial law measures, in particular, to determine the legal basis for cybersecurity in Ukraine. In this direction, it is important to study and adopt the experience of NATO and the European Union (hereinafter - the EU) in countering hybrid cyber threats to preserve national security in times of war. First, we will focus our research on the analysis of international legal acts in the field of cybersecurity, in particular the EU. It is worth emphasizing that cybersecurity has long been on the agenda of NATO and the European Union. They had a clear understanding that any hybrid threats must be prevented and both soft and hard measures must be applied in the event of hybrid attacks.

In 2002, the Prague Summit expanded cybersecurity mechanisms and laid the groundwork for cybersecurity initiatives within NATO, known as the Communications and Information Systems Agency (NATO's "first line of defense" against cyberterrorism) and the Information Security Technical Center, which is responsible for communications and computer security.

It is worth emphasizing that on December 20, 2002, the UN General Assembly adopted Resolution 57/239 "Elements of a Global Culture of Cybersecurity", which introduced the concept of "cybersecurity" into the legal terminology [14]. This document defines that the global culture of cybersecurity includes such interrelated elements as awareness, responsibility, response, ethics, democracy, risk assessment, design and implementation of security measures, and reassessment [15].

After the 2007 cyberattack on Estonia, NATO began to work actively to address the problem and a number of cybersecurity bodies were established.In 2008, as a result of the Bucharest Summit and to bring together the main NATO bodies involved in cybersecurity, the Cyber Security Governance Body was established, which takes a flexible approach to understanding cybersecurity rather than adopting a stable and fixed set of rules and guidelines [16]. NATO's Strategic Framework clearly outlines step-by-step measures of the organization to increase resilience to external factors and to strengthen national cybersecurity standards for member states [16].

It should be noted that since the 2010s, attention has been focused on national security policy issues and the vector of attention has been directed towards the protection of physical assets such as satellites, deep-sea cables and other communications. In 2012, the International Center of Criminology also identified eight key innovations that outline future risks and threats in the field of cybersecurity. They include: cloud environment; big data, mobile Internet, neural interface, contactless payments, mobile robots, quantum computing, and militarization of cyberspace [17].

The EU has prioritized countering hybrid threats and further development of the cybersecurity system in the coming years. These aspects are clearly defined in a number of documents, including joint communiqués of the European Parliament and the European Council on the implementation of measures to counter hybrid threats in the EU. Among them are the following: Joint Communication to the European Parliament and the Council on the Joint Framework for Countering Hybrid Threats - European Union Response (06.04.2016) [18], Joint Report to the European Parliament and the Council on the Implementation of the Joint Framework for Countering Hybrid Threats - European Union Response (19. 07.2017) [19], Report on the Joint Staff Working Document on the Implementation of the 2016 Joint Framework for Countering Hybrid Threats and the 2018 Joint Communication on Building Resilience and Strengthening Capabilities to Counter Hybrid Threats (28.05.2019) [20], etc.

The analysis of these documents suggests that they outline a realistic vision of hybrid cyber threats and define the basic directions of legal support for cybersecurity in the EU. They also present to the European Community the achievements and the phasing of further actions to implement them in the areas proposed in the Joint Action, namely: raising awareness of the situation; resilience of

society; strengthening crisis prevention and response capabilities; coordinating the restoration and expansion of cooperation with NATO to ensure complementarity in activities.

The proposed activities focus on raising awareness of hybrid cyber threats, identifying societal vulnerabilities to them, and coordinating joint activities to assess these threats. In order to identify societal vulnerabilities and take into account real hybrid features, an analysis of possible risks that cyber threats may pose to institutions and networks is carried out.

Attention should be drawn to the Directive of the European Parliament and of the Council on measures for a high common level of security of network and information systems in the Union (NIS Directive) [21]. It clearly defines common rules and requirements in the field of cybersecurity, while empowering each member state to take its own measures to implement its provisions in national legislation. It stipulates that these rules must be implemented by May 9, 2018.The implementation of these rules into national legislation expands the possibilities for ensuring national security in this area. This Directive obliges each EU member state to develop its own national strategy for network and information security, which should outline strategic goals, priorities, namely; preventive measures; response and recovery measures after cyberattacks; principles of public-private partnership; educational and awareness-raising activities; plans for research, assessment and risk management; a list of key parties directly responsible for the implementation of the Directive; government agencies responsible for the implementation of the document, etc.

In order to achieve the goal of the Directive, the following basic areas are specified: strengthening the capacity of the cybersecurity system at the national level; improving the level of pan-European cooperation; implementing risk management and the obligation to report cyber incidents to providers of basic services and digital services.

It can be argued that international law is aimed at countering hybrid cyber threats. It outlines risk management as a priority component and promotes awareness of the system's cybersecurity vulnerabilities. We believe that in order to further improve Ukraine's cybersecurity system, it is necessary to gradually implement European legislation, including the provisions of the Directive of the European Parliament and of the Council. This issue has become particularly relevant after President Zelenskiy signed Ukraine's application for EU membership and the decision to start negotiations on Ukraine's accession to the EU.

Let us consider the legal framework in the field of cybersecurity in Ukraine. It is worth emphasizing that martial law in Ukraine has actualized issues in this area. Cybersecurity risks are potentially increasing both in terms of spread in cyberspace and destructive impact. In March 2022, Ukraine's largest telecom provider, Ukrtelecom, suffered a powerful cyberattack [22]. One of the most devastating cyberattacks on the Ukrainian mobile operator Kyivstar occurred in December 2023, destroying about 40% of its infrastructure [23, 24]. As we can see, the state and society face such cyberattacks as: disruptions in the provision of electronic services, blocking the work of government agencies, blocking the work or destruction of strategically important critical infrastructure and life support systems [25].

Ukrainian legislation in the field of information security outlines the fundamental principles and mechanisms for ensuring information security, in particular, the Constitution of Ukraine, the Criminal Code of Ukraine, the Laws of Ukraine "On the Fundamentals of National Security", "On the Basic Principles of Ensuring Cybersecurity of Ukraine", "On Information", "On State Secrets", "On Access to Public Information", "On Protection of Information in Information and Telecommunication Systems", "On Scientific and Scientific-Technical Expertise", "On Technical Regulations and Conformity Assessment".

In general, the formation of Ukrainian cybersecurity legislation began in 2011 and is still ongoing. Its development was based on the principles of international regulations of other countries. The first legislative act in the field of cybersecurity was the NSDC Decision "On Challenges and Threats to the National Security of Ukraine in 2011", enacted by Presidential Decree No. 1119/2010 of December 10, 2010 (no longer in force). This Decision provided for the development of proposals for the creation of a unified national system for combating cybercrime and the approval of a list of facilities that are

important for ensuring national security and defense of Ukraine and require priority protection from cyberattacks.

The fundamental legal document that regulates the issues of the basis for ensuring the protection of the vital interests of a person and a citizen, society and the state, the national interests of Ukraine in cyberspace, the main goals, directions and principles of state policy in the field of cybersecurity is the Law of Ukraine "On the Basic Principles of Ensuring Cybersecurity of Ukraine" [26]. It clearly defines the legal and organizational framework for ensuring the protection of interests, principles, main goals, directions of state policy in the field of cybersecurity, objects of cybersecurity and cyber defense, critical infrastructure, cybersecurity actors and their powers, etc. This document establishes that the basic types of activities that are likely to be intensively used in the context of military operations in cyberspace are: cyberintelligence, cyberterrorism, and cyberespionage [26]. We emphasize that Part 1 of Art. 1 of this Law of Ukraine is supplemented by clauses 22, 23, which relate to the system of active counteraction to aggression in cyberspace and active counteraction to aggression in cyberspace [27].

Given that Ukraine has the status of a NATO partner with enhanced capabilities, clause 3, Article 8 of this Law also outlines the functioning of the national cybersecurity system. It is ensured by developing and promptly adapting the state policy in the field of cybersecurity aimed at developing cyberspace, achieving compatibility with the relevant standards of the European Union and NATO, and creating a regulatory and terminological basis in the field of cybersecurity in accordance with international standards. It also focuses on the development of international cooperation in the field of cybersecurity, support for international cybersecurity initiatives that meet Ukraine's national interests, and deepening Ukraine's cooperation with the European Union and NATO.

The subjects of the national cybersecurity system that directly carry out cybersecurity measures within their competence are defined: The Ministry of Defense of Ukraine, the State Service for Special Communications and Information Protection of Ukraine, the Security Service of Ukraine, the National Police of Ukraine and other public authorities that must implement the state's information security policy, which provides for the detection of illegal activities in relation to digital infrastructure, prevention of unauthorized access to certain information resources, protection against cybercrime and other actions [26].

It should be noted that Art. 6 of the Law regulates the activities of the governmental computer emergency response team of Ukraine CERT-UA (Computer Emergency Response Team of Ukraine), which operates as part of the State Service for Special Communications and Information Protection of Ukraine [26, 28]. The purpose of its activities is to systematically protect the activities of state institutions and citizens of Ukraine from illegal access to the cyberspace of our country, countering cyber weapons, etc. However, its specialists are not authorized to carry out investigative actions and prosecute cybercriminals.

Also, we consider it necessary to point out the importance of the National Coordination Center for Cybersecurity, which is defined as a working body of the National Security and Defense Council of Ukraine [29]. It was established in accordance with the decision of the National Security and Defense Council of Ukraine of January 27, 2016 "On the Cybersecurity Strategy of Ukraine", enacted by the Decree of the President of Ukraine of March 15, 2016 No. 96. The National Coordination Center for Cybersecurity is directly engaged in ensuring coordination of the activities of the national security and defense entities of Ukraine in the process of implementing the Cybersecurity Strategy of Ukraine, improving the efficiency of the public administration system in the formation and implementation of state policy in the field of cybersecurity.

The Decree of the President of Ukraine "On the Decision of the National Security and Defense Council of Ukraine of May 14, 2021 "On the Cybersecurity Strategy of Ukraine" of August 26, 2021 No. 447/2021 approved the Information Security Strategy. The main goal of the Strategy is to strengthen the capabilities to ensure the information security of the state, its information space, support social and political stability, defense of the state, protection of state sovereignty, territorial integrity of Ukraine, democratic constitutional order, and ensuring the rights and freedoms of every citizen by information means and measures [30]. As we can see, this document identifies current

challenges and threats to Ukraine's national security in the information sphere, specifies strategic goals and directions aimed at countering such threats, protecting the rights of individuals to information and personal data protection, and outlines implementation mechanisms and expected results [30].

It is noteworthy that before the full-scale invasion began, the Decree of the National Security and Defense Council of Ukraine "On the Plan for Implementation of the Cybersecurity Strategy of Ukraine" was enacted by Presidential Decree No. 37/2022 of February 1, 2022. This Plan defines a number of strategic goals that need to be implemented in accordance with the Cybersecurity Strategy of Ukraine. These include [31]:

1. Effective cyber defense.
2. Effective counteraction to reconnaissance and subversive activities in cyberspace and cyberterrorism.
3. Effective counteraction to cybercrime.
4. Development of asymmetric deterrence tools.
5. National cyber preparedness and reliable cyber defense.
6. Professional development, cyber-savvy society and scientific and technical support for cybersecurity.
7. Secure digital services.
8. Strengthening the coordination system.
9. Formation of a new model of relations in the field of cybersecurity.
10. Pragmatic international cooperation.

It should also be noted that this regulatory document clearly sets a deadline for the completion of the implementation of the provisions of the Convention on Cybercrime into Ukrainian legislation [31]. In cybersecurity, cyber defense is based on cyber troops, which are obliged to ensure effective protection of state information resources and information, as well as critical information infrastructure [31].

After the start of a full-scale invasion, the legal mechanisms for implementing cybersecurity were strengthened by the Resolution of the Cabinet of Ministers of Ukraine "Some Issues of Response by Cybersecurity Entities to Various Types of Events in Cyberspace" [32]. This regulatory document clearly defines the levels of response by cybersecurity entities to various types of events in cyberspace and regulates the actions of the relevant authorities regarding the procedures for ensuring protection and restoration of capacity.

It is worth noting that the Decree of the President of Ukraine of May 11, 2023, No. 273/2023 "On the Comprehensive Strategic Plan for Reforming Law Enforcement Agencies as Part of the Security and Defense Sector of Ukraine for 2023-2027" identifies the need to strengthen the capacity of prosecutors and law enforcement agencies to combat internal and external cyber threats [33].

It is necessary to point out positive changes in the Criminal Code of Ukraine (hereinafter - the CCU). In general, Art. 361 has undergone significant terminological and constructive changes. It has been expanded with new legal elements, in particular, in parts 3, 4 of this article, the element of committing a crime under martial law is defined as a qualifying element only for qualified elements. Also, the qualified legal elements of the crime under this article have been expanded and differentiated.

The analysis shows that the assessment of the category of harm under Articles 361...363-1 of the CCU, as well as the approach to the formulation of the legal elements of the crime under Article 361-1 of the CCU, have been changed. It should be noted that the sanctions for the relevant criminal offenses have been increased. In particular, the amendments to the CCU increase liability for unauthorized interference with electronic systems depending on their consequences and provide for punishment for cybercrime committed directly during martial law [27]. However, according to the Law, unauthorized interference with the operation of a number of information and communication systems is not considered unauthorized if it is committed in accordance with the Procedure for Searching and Identifying Potential Vulnerabilities of Such Systems or Networks [27].

Thus, we believe that Ukrainian legislation is aimed at ensuring cybersecurity in the state, and the amendments to the regulatory legal acts are aimed at strengthening cyber defense capabilities under martial law.

5. Conclusions

To summarize, cybersecurity is one of the main components of the national security of the state. It is an element of Ukraine's cyberspace and a component of the information society.

We believe that in order to preserve national security in times of war and further improve Ukraine's cybersecurity system, it is necessary to gradually implement European legislation, in particular that of NATO and the European Union, which will automatically require appropriate amendments to existing regulations.

Currently, the country's regulatory legal acts on cybersecurity are the Constitution of Ukraine, the Criminal Code of Ukraine, the Laws of Ukraine, decrees of the President of Ukraine, and decisions of the National Security and Defense Council of Ukraine. The Law of Ukraine "On the Basic Principles of Ensuring Cybersecurity of Ukraine" is the fundamental legal document regulating the state policy in the field of cybersecurity. A number of regulations also identify current challenges and threats to Ukraine's national security in the information sphere, regulate legal mechanisms for implementing cybersecurity, and amend the Criminal Code to strengthen cyber defense capabilities under martial law.

It is established that cybersecurity measures are carried out by the subjects of the national cybersecurity system. The National Coordination Center for Cybersecurity was established as a working body of the National Security and Defense Council of Ukraine. The systemic protection of the activities of state institutions and citizens of Ukraine from illegal access to the state's cyberspace is directly handled by the governmental team for responding to computer emergencies of Ukraine CERT-UA.

We believe that the regulatory basis in the field of cybersecurity should take into account the requirements and trends of modern scientific and technological progress, as well as the need for a comprehensive interdisciplinary approach to the legal regulation of cybersecurity measures, especially in times of war to maintain the stability and integrity of the state.

Declaration on Generative AI

The author(s) have not employed any Generative AI tools.

References

[1] Report on the work of the vulnerability detection and response system for cyber incidents and cyber attacks. Operational Center for Response to Cyber Incidents, State Center for Cyber Defense, State Service for Special Communications and Information Protection of Ukraine. 2022. URL: https://scpc.gov.ua/api/docs/sseb6a10-b7aa-4396-8b04-e0e4b7fca1l1/sseb6a10-b7aa-4396-8b04-e0e4b7fca1l1.pdf [in Ukrainian].

[2] R. Melnyk, State Special Forces Service: Ukraine repels from 5 to 40 powerful DDoS attacks every day. MediaSapiens, 2023. URL: https://ms.detector.media/kiberbezpeka/post/31017/2023-01-18-derzhspetszyazku-ukraina-shchodoby-vidbyvaie-vid-5-do-40-potuzhnykh-ddos-atak/ [in Ukrainian].

[3] Ukraine repels up to 40 powerful cyberattacks every day – State Service for Special Communications. Ukrinform, 2023. URL: https://www.ukrinform.ua/rubric-technology/3654348-ukraina-sodobi-vidbivae-do-40-potuznih-kiberatak-derzspeczvazku.html [in Ukrainian].

[4] What is cybersecurity? Microsoft, 2023. URL: https://www.microsoft.com/uk-ua/security/business/security-101/what-is-cybersecurity [in Ukrainian].

[5] On the basic principles of ensuring cybersecurity in Ukraine: Law of Ukraine dated October 5, 2017 No. 2163-VIII. Verkhovna Rada of Ukraine, 2023. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text [in Ukrainian].
[6] Ye. Kotukh, Theoretical and methodological principles of ensuring cybersecurity in the public sector: dissertation - doctor of philosophy: 25.00.02 "Mechanisms of public administration". Kharkiv, 2022. 479 p. [in Ukrainian].
[7] H. V. Foros, V. S. Zhohov, Peculiarities of the interpretation of the concept of "cybersecurity" in modern legal science, Lawful State 33 (2019) 128–134. URL: http://nbuv.gov.ua/UJRN/Prav_2019_33_20 [in Ukrainian].
[8] I. Sopilko Information security and cybersecurity: a comparative legal aspect, Scientific works of the National Aviation University. Series: Legal Bulletin "Air and Space Law" 2(59) (2021) 110–115. [in Ukrainian].
[9] A. V. Voitsikhovskyi, Cybersecurity as a direction of Euro-Atlantic integration of Ukraine. Law and security in the context of European and Euro-Atlantic integration: a collection of articles and abstracts of scientific reports based on the materials of the discussion panel of the II Kharkiv International Legal Forum, Kharkiv, September 28, 2018 / editorial board: Yu.H. Barabash, T.M. Anakina, D.V. Abbakumova. Kharkiv: Pravo, 2018. pp. 42–48. [in Ukrainian].
[10] O. Zh. Skybun Cybersecurity of electronic communications systems of state authorities of Ukraine. Bulletin of the State Administration of Ukraine. Series "State Administration" 1(100) (2021) 30–39. [in Ukrainian].
[11] O. D. Dovhan, V. H. Khlan Cyberterrorism as a threat to the information sovereignty of the state, Information Security of Man, Society, and the State 10 (2011) 49–53. [in Ukrainian].
[12] A. S. Didenko The goal, objectives and principles of state policy in the field of combating cybercrime, Law and Security 1 (2020) 53–59. URL: http://nbuv.gov.ua/UJRN/Pib_2020_1_9 [in Ukrainian].
[13] I. O. Revak, R. T. Hren Peculiarities of forming a safe cyberspace in the context of the development of the digital economy, Innovative Economy 3-4 (2021) 164–169. [in Ukrainian].
[14] UN General Assembly Resolution 57/329, adopted at the 78th plenary meeting of the 57th session, 2002. URL: https://documents-ddsny.un.org/doc/UNDOC/GEN/N02/555/24/PDF/N0255524.pdf?OpenElement [in Ukrainian].
[15] O. D. Dovhan, I. M. Doronin, Escalation of Cyber Threats to the National Interests of Ukraine and legal aspects of cyber defense, Kyiv, 2017. [in Ukrainian].
[16] A. J. Lewis, G. Neuneck, The Cyber Index. International security trends and realities, New York and Geneva, United Nations Institute for Disarmament Research, 2013.
[17] B. Dupont, L'environnement de la cybersecurite a l'horizon tendances, moteurs et implications.Note de recherche 14 Centre International de Criminology Compare. Universite de Montreal, Montreal. 2012.
[18] The joint communication to the European Parliament and the Council on a joint framework programme to counter hybrids threatens a response from the European Union, 2016. URL: https://eur-lex.europa.eu/legalcontent/EN/TXT/?uri=CELEX%3A52016JC0018. [in Ukrainian].
[19] Joint Report to the European Parliament and the Council on the Implementation of the Joint Framework Programme on Countering Hybrid Threats – The European Union's Response, 2017. URL: https://eur-lex.europa.eu/legalcontent/EN/TXT/?uri=CELEX%3A52017JC0030 [in Ukrainian].
[20] Report on the Joint Staff Working Document on the Implementation of the 2016 Joint Framework Programme on Countering Hybrid Threats and the 2018 Joint Communication on Enhancing Resilience and Strengthening Capabilities to Counter Hybrid Threats, 2018. URL: https://eeas.europa.eu/ [in Ukrainian].
[21] Directive of the European Parliament and of the Council (IeS) 2016/1148 of 06.07.2016 concerning measures for a high common level of security of network and information systems across the Union, 2016. URL: https://zakon.rada.gov.ua/laws/show/984_013-16/find?text=%F0%E8%E7%E8%EA [in Ukrainian].

[22] Cyberattack on Ukrtelecom on March 28: details. State Service for Special Communications and Information Protection of Ukraine, 2022. URL: https://cip.gov.ua/ua/news/kiberataka-na-ukrtelekom-28-bereznya-detali [in Ukrainian].
[23] The cyberattack on Kyivstar may have been one of the most destructive in Ukraine since early February 2022 – British intelligence. Interfax-Ukraine, 2022. URL: https://interfax.com.ua/news/general/954657.html [in Ukrainian].
[24] Yu. Tarasovskyi, Hackers destroyed about 40% of Kyivstar's infrastructure – Komarov, 2023. URL: https://forbes.ua/news/khakeri-zruynuvali-blizko-40-infrastrukturi-kiivstar-komarov-22122023-18082 [in Ukrainian].
[25] O. H. Trofymenko, Yu. V. Prokop, N. I. Lohinova, O. V. Zadereiko, Monitoring the state of cybersecurity in Ukraine. Legal life of modern Ukraine: materials of the International Scientific and Practical Conference of May 17, 2019. Odesa. Helvetica Publishing House. 2019. Vol. 1, pp. 642–646. [in Ukrainian].
[26] On the basic principles of ensuring cybersecurity in Ukraine: Law of Ukraine dated October 5, 2017 No. 2163-VIII. Verkhovna Rada of Ukraine, 2017. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text [in Ukrainian].
[27] On Amendments to the Criminal Code of Ukraine to Increase the Effectiveness of Combating Cybercrime under Martial Law: Law of Ukraine No. 2149-IX of March 24, 2022. Database "Legislation of Ukraine". Verkhovna Rada of Ukraine. URL: https://zakon.rada.gov.ua/laws/show/2149-20#Text [in Ukrainian].
[28] On the CERT-UA Computer Emergency Response Team of Ukraine, 2022. URL: https://cert.gov.ua/about-us [in Ukrainian].
[29] On the National Cybersecurity Coordination Center: Decree of the President of Ukraine No. 242/2016 of June 7, 2016 / Verkhovna Rada of Ukraine. Legislation of Ukraine, 2016. URL: https://zakon.rada.gov.ua/laws/ show/242/2016#Text. [in Ukrainian].
[30] On the decision of the National Security and Defense Council of Ukraine dated October 15, 2021 "On the Information Security Strategy": Decree of the President of Ukraine dated December 28, 2021. № 685/2021. URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text [in Ukrainian].
[31] About the Implementation Plan of the Cybersecurity Strategy of Ukraine: Decision of the National Security and Defense Council of Ukraine of May 14, 2021: Decree of the President of Ukraine of August 26, 2021 № 447/2021. URL: https://www.president.gov.ua/documents/4472021-40013 [in Ukrainian].
[32] Some issues of response by cybersecurity entities to various types of events in cyberspace: Resolution of the Cabinet of Ministers of Ukraine dated April 4, 2023. № 299. URL: https://zakon.rada.gov.ua/laws/show/299-2023-%D0%BF#Text [in Ukrainian].
[33] On the Comprehensive Strategic Plan for Reforming Law Enforcement Agencies as Part of the Security and Defense Sector of Ukraine for 2023-2027: Decree of the President of Ukraine dated May 11, 2023 № 273/2023. URL: https://zakon.rada.gov.ua/laws/show/273/2023#Text [in Ukrainian].