ppi 201502ZU4645
Esta publicación científica en formato digital es continuidad de la revista impresa
ISSN-Versión Impresa 0798-1406 / ISSN-Versión on line 2542-3185Depósito legal pp
197402ZU34

CUESTIONES POLÍTICAS

Instituto de Estudios Políticos y Derecho Público "Dr. Humberto J. La Roche"
de la Facultad de Ciencias Jurídicas y Políticas de la Universidad del Zulia
Maracaibo, Venezuela

Vol.40

Nº 73
Julio
Diciembre
2022

Cuestiones Políticas Vol. 40, Nº 73 (2022), 583-599
IEPDP-Facultad de Ciencias Jurídicas y Políticas - LUZ

Cyber security as the basis for the national security of Ukraine

DOI: https://doi.org/10.46398/cuestpol.4073.33

Oleh Tarasenko *
Dmytro Mirkovets **
Artem Shevchyshen ***
Oleksandr Nahorniuk-Danyliuk ****
Yurii Yermakov *****

Abstract

The goal of the article is to identify cybersecurity issues as a component of national security and suggest ways to solve them. The topic of the research is the cyber security of Ukraine. In the course of the research, the following methods were used: dialectical method, formal and legal method, comparative-legal method and scientific abstraction method. As a result, the legal acts governing cybersecurity in Ukraine are analyzed, the cyber security actors are determined and their functions are defined. Practical implementation. There is a need to establish and implement an annual plan for the implementation of the Cyber Security Strategy, which should detail the actions to ensure cyber security, identify specific measures, deadlines and responsible actors. It is concluded that, ways to improve the cybersecurity system (as part of national security), which will update the legal mechanisms of cybersecurity, create cybersecurity infrastructure at the global level, establish effective interaction between cybersecurity actors regardless of their departmental affiliation and / or form of ownership, including with the owners of critical infrastructure and non-state owned information), are in their primary phase.

* Doctor of Juridical Sciences, Associate Professor, Professor of the Department of operative-search activity of the National Academy of Internal Affairs (Kyiv, Ukraine). ORCID ID: https://orcid.org/0000-0002-3179-0143

** Candidate of Juridical Sciences, Associate Professor, Associate Professor Department public law disciplines Private Higher Education Institution «University of Modern Knowledge» (Kyiv, Ukraine). ORCID ID: https://orcid.org/0000-0003-2539-2824

*** Doctor of Juridical Sciences, Associate Professor, Professor of the Department of Criminal Procedure of the National Academy of Internal Affairs (Kyiv, Ukraine). ORCID ID: https://orcid.org/0000-0002-1342-6639

**** Candidate of Juridical Sciences, Lecturer of the Department of Civil and Legal Disciplines of the National Academy of Internal Affairs (Kyiv, Ukraine). ORCID ID: https://orcid.org/0000-0003-1511-7140

***** Doctor of Juridical Sciences, Associate Professor, Research Officer of the Department of Scientific and Legal Expertise and Law Drafting of the Educational and Research Institute of Public Law. ORCID ID: https://orcid.org/0000-0002-9400-0604

Recibido el 03/03/2022 Aceptado el 25/05/2022

Keywords: cybersecurity; information and communication technologies; national security; security strategy; cyberterrorism.

La ciberseguridad como base para la seguridad nacional de Ucrania

Resumen

El objetivo del artículo es identificar los problemas de la seguridad cibernética como un componente de la seguridad nacional y sugerir formas de resolverlos. El tema de la investigación es la seguridad cibernética de Ucrania. En el transcurso de la investigación se utilizaron los siguientes métodos: método dialéctico, método formal y legal, método comparativo-legal y método de abstracción científica. A modo de resultado, se analizan los actos jurídicos que rigen la seguridad cibernética en Ucrania, se determinan los actores de la seguridad cibernética y se definen sus funciones. Implementación práctica. Existe la necesidad de establecer e implementar un plan anual para la implementación de la Estrategia de Seguridad Cibernética, que debe detallar las acciones para garantizar la seguridad cibernética, identificar medidas específicas, plazos y actores responsables. Se concluye que, las formas de mejorar el sistema de seguridad cibernética (como parte de la seguridad nacional), que actualizará los mecanismos legales de seguridad cibernética, crear infraestructura de seguridad cibernética a nivel global, establecer una interacción efectiva entre los actores de seguridad cibernética independientemente de su afiliación departamental y/o forma de propiedad, incluso con los propietarios de infraestructura crítica y de información de propiedad no estatal), están en su fase primaria.

Palabras clave: ciberseguridad; tecnologías de la información y la comunicación; seguridad nacional; estrategia de seguridad; ciberterrorismo.

Introduction

Information and communication technologies are one of the most important factors influencing the formation of priority areas of development of the 21st century, which accounted for the achievements of mankind in the practical implementation of new electronic information technologies. There is a development of informatization processes related to expanding the access to information resources and means of their production for all categories of the population (Dovhan and Doronin, 2017).

Although current global development trends are based on the widespread introduction and application of information and communication technologies, they simultaneously raise the issue of information security and cyber security (especially for critical information infrastructure), due to the increasing number and complexity of cyber incidents that enhance the risks of natural and man-made nature (Order of the Cabinet of Ministers of Ukraine No. 1009-r, 2017).

According to the materials of the International Forums in Davos (2018 –2019), the problem of cyber security is particularly acute, affecting virtually all spheres of human life and activity (humanity suffers losses of more than $ 400 billion per year because of cyber-attacks) (Bykov *et al.*, 2019).

The large-scale WannaCry virus attack, which took place on 12 – 13 May 2017, affected tens of thousands of computers around the world: for example, in the UK, a number of medical facilities across the country were forced to deny patients services even in emergencies due to failure of most computer systems; in Spain, the Ministry of Energy and a telecommunications company were attacked; in Germany, the computers of the railway company's control centers were infected, as a result of which the control system failed; in France, car manufacturer Renault was hit by a massive cyber-attack; Portugal Telecom, the largest telecommunications service provider, was attacked in Portugal; in China, about 15% of educational networks were affected; computer systems of shopping and office centers, networks of hospitals and gas stations, postal service, railway stations, as well as government agencies were attacked (the probable damage caused by the WannaCry virus in the first four days exceeded $ 1 billion) (Dovhan and Doronin, 2017).

This phenomenon clearly demonstrates how modern society depends on the stable operation of information systems. Cyber security is considered as a strategic problem at the State level, which affects all segments of society (Dovhan and Doronin 2017).

That is, the formation of the information society gives new impetus to the traditional threats to State security and creates fundamentally new challenges for the national security system. In such conditions, the search for new opportunities to ensure the security of the State becomes especially important in view of the formation of a new field of confrontation – cyberspace.

Although Ukraine began entering the information space only in the early 1990s of the 20th centuries, but it led to a spike in computer crime resulted in the development of appropriate legal instruments, adapting them to new technologies. The activity of the world's leading countries in cyberspace, profound changes in attitudes to domestic information policy necessitates the development of recommendations on short- and long-term priorities for the transformation of the domestic cyber security sector.

The urgency of this problem is also determined by the rapid development of a new type of illegal activity – transnational computer crimes, a sharp increase in criminal computer professionalism, active migration of criminals and organization of their actions, interethnic nature, which significantly complicated the criminogenic situation (Borysova, 2007).

The state and degree of threats in cyberspace have led to the State's response to strategic documents in the area of national security of Ukraine. Challenges and threats to Ukraine's national security in cyberspace resulted in the creation of the Cyber Security Strategy of Ukraine, which was implemented by the Order of the President of Ukraine of March 15, 2016 (Order of the President of Ukraine No. 96/2016, 2016). The incorporation of its provisions led to the adoption of the Law of Ukraine "On the Basic Principles of Cybersecurity in Ukraine" (Law of Ukraine № 2163-VIII, 2017), which is a comprehensive special piece of legislation in the area of cyber security.

Despite some ambiguities in the text of the statute and possible issues with its practical application, it should be noted that the period of formation of the national legislation in the area of cyber security has begun, and the main act of special legislation initiating the relevant legislation has been adopted (Dovhan and Doronin, 2017), as well as the corresponding body of legislation, which constitutes direct legislation in the field of cybers-security, has been established.

However, the problem of their real implementation and coherence, accelerating the incorporation of a set of international documents, especially the EU and NATO ones (the number of which is growing rapidly), coordination and interaction of major objects and actors of cyber security remains relevant.

The analysis of the practical introduction of regulations in the area of cybersecurity shows a number of problematic issues that prevent the creation of an effective system of countering threats in cyberspace (such as terminological uncertainty, lack of proper coordination of relevant agencies, Ukraine's dependence on foreign software and hardware, difficulties with staffing the relevant structural units, etc.) (Dubov, 2010).

1. Methodology

The methodological basis for the research was laid by the system and structural method and the method of ascension from the abstract to the concrete. In combination with the method of analysis, they have become an effective tool in the study of theoretical and methodological principles of ensuring cyber security in Ukraine.

The philosophical and ideological basis for the study is the dialectical method of scientific knowledge of cyber security as a legal category in contradictions and changes, which created an opportunity to assess the historical development of this phenomenon, the establishment of the legal institution and the formation of modern paradigm of cyber security.

With the help of the formal and legal method the concept of research categories was substantiated, the conceptual categorical apparatus was formed. The comparative and legal method was used in the study of domestic legislation on legal support for cyber security in view of cyber threats. The method of scientific abstraction allowed to propose substantiated measures to combat threats in the area of cyber securit**y.**

2. Literature Review

The issues of counteraction to illegal acts in the area of high technology are revealed in the works of a number of domestic and foreign scientists.

Sushko (2021) provided the definition of cyber security, which, according to her opinion, is the practice of protecting networks, devices, and applications from damage or theft. Besides, she emphasized that quit often the concepts of "cybersecurity" and "information security" are applied in parallel, but they are totally different: information security deals with the means that protect personal data and cyber security is the activity aimed at the protection of systems, programmes and electronic data from attacks.

For example, Delesline (2021) considered the difference between IT security and cyber security and comes to the conclusion the first concept is broader one: information technology focuses on the systems that store and transmit digital information, while cyber security deals with protecting electronic information stored within those systems.

Lopez (2022) provided an overview of the state of cyber security in the UK for the period 2016 – 2021. She underlined the increasing role of Internet technologies on the British economy, but at the same time stressed on the growing number of cyber-attacks. That is why she proposed the measures the UK government should undertake to prevent them and minimize their adverse effect.

Part of the research has been undertaken precisely in the context of the scientific rationale for the provision of cyber security; in particular, Bakalinska and Bakalynskyi (2019) analyzed the prerequisites and features of Ukrainian legislation in the area of cyber security, identified problems and prospects for its further development in terms of assessing existing dangers and threats, identified the areas for adapting domestic cyber security legislation to the EU standards within the implementation of the provisions of the Association Agreement between Ukraine and the EU.

Bykov *et al.* (2019) covered such types of protection of cyber security as legal, informational, organizational and psychological one, in humans' centric networks, concluding that the most significant among cyber threats are the methods of social engineering.

Kosinova *et al.* (2021) addressed the regulation of cyber security policy implementation relationships in the EU and Ukraine. The authors analyzed the system of legal instruments of the EU institutions in the area of cyber security, specified mechanisms for adopting cyber policy in the EU Member States, explored their main capabilities, means of implementation and EU institutions responsible for the functioning of secure European cyberspace (including the EU Cyber security Agency).

Stanislavskyi (2020) studied national cyber security strategies, summarized the trends in cyber security systems of leading countries and their associations, the State of international cooperation, defined the list and content of scientifically based capacity-building proposals to enhance Ukraine's ability to adequately address cyber security threats and to develop national cyber security.

Bratel *et al.* (2021) investigated the threats to the information security of Ukraine, and, in particular – to its cyber security. They also examined the legal status, powers and tasks of rule-of-law institutions to ensure this kind of security of our country.

Diorditsa *et al.* (2021) analyzed cyberterrorism as a threat to Ukraine's cyber security. The authors believe that nowadays with the development of information technologies the great harm to the interests of the State could be caused precisely through cyberspace.

Thus, the scientists analyzed the system of legal acts of Ukraine in the area of national cyber security, noted positive changes in the implementation of cyber policy in Ukraine, including the development of the Cybersecurity Strategy of Ukraine for 2021 – 2025 (Order of the President of Ukraine No. 447/2021, 2021; Press-Center of the National Security and Defense Council of Ukraine, 2021), identified the shortcomings in the regulation of cyber security and compliance with national legislation, but ignored the issues related to the implementation of practical tasks of cyber security as a component of national security.

That is why, the purpose of the article is to identify the problems of cyber security as a component of national security of Ukraine and suggest the ways to solve them.

3. Results and Discussion

On March 15, 2016, the Cyber Security Strategy of Ukraine – a strategic planning document – was adopted (Order of the President of Ukraine No. 447/2021, 2021). Later, the Laws of Ukraine "On the Basic Principles of Cybersecurity in Ukraine" (Law of Ukraine № 2163-VIII, 2017), "On the National Security of Ukraine" (Law of Ukraine No. 2469-VIII, 2018), which legitimized the status of the Cyber Security Strategy, were adopted. During the development and adoption of this Strategy, the government took into account the current trends in security policy in world politics, as over the past five years, strategies such as strategic planning documents have been adopted in almost all countries of the world (Dovhan and Doronin, 2017).

The Law of Ukraine "On the Basic Principles of Cybersecurity in Ukraine" (Law of Ukraine № 2163-VIII, 2017) is the concept of development of cyber security, which defines the category-conceptual apparatus, objects, subjects and principles of cyber security, the structure of National cyber security system and the tasks of its main components, mechanisms of public-private and public-State partnership, etc.

It should be noted that logically, this Law as the concept should precede the Cyber Security Strategy of Ukraine (that was adopted a year earlier), which affected the quality of its implementation. The adoption of this Law (Law of Ukraine № 2163-VIII, 2017), as well as the Law "On the National Security of Ukraine" was an important factor influencing the essence of the measures proposed in the draft annual action plans for the implementation of the Strategy.

If the first one solved the problem of regulating public relations in the area of cyber security and outlined the national cyber security system, the second one clearly defined their place in the national security system.

The Law (Law of Ukraine № 2163-VIII, 2017) determines: legal and organizational basis for ensuring protection in cyberspace; main goals, directions and principles of State policy; the capacities of actors and the main principles of their coordination.

The Strategy separates the area of "cyber security and security of information resources" and "information security", as well as identifies its priorities: development of information infrastructure of the State; establishment of cyber security system, development of a computer emergency response network (CERT); cyberspace monitoring in order to timely detect, prevent and neutralize cyber threats; enhancing the capacity of law enforcement agencies to investigate cybercrime; ensuring the protection of critical infrastructure, State information resources from cyber-attacks; reforming the system of protection of State secrets and other information with limited access, protection of State information

resources, e-government systems, technical and cryptographic protection of information.

That is, both the Strategy and the Law (Law of Ukraine № 2163-VIII, 2017) distinguish the elements of the cyber security system, their general functions and tasks, but the organization of their interaction is practically undefined; it means that it should be regulated at the level of regulations (including by-laws) of the executive branch.

The Order of the President of Ukraine of June 07, 2016 No. 242/2016 (Order of the President of Ukraine No. 242/2016, 2016) approved the Regulation on the National Coordination Center for Cyber Security (i.e., before the adoption of the Law of Ukraine "On the Basic Principles of Cybersecurity in Ukraine").

The competence of the National Cyber Security Coordination Center is enshrined in Part 2, 5 of the Law of Ukraine "On the Basic Principles of Cybersecurity in Ukraine" (Law of Ukraine № 2163-VIII, 2017); in particular, the Center coordinates and monitors the activities of security and defense actors, ensuring cyber security, makes proposals to the President of Ukraine on the formation and refinement of the Cyber Security Strategy of Ukraine, ensures cyber security, etc.

The task of performing all procedures, including regulatory ones, is entrusted to the State Service for Special Communications and Information Protection of Ukraine (Law of Ukraine No. 3475-IV, 2006). The Law of Ukraine "On the Basic Principles of Cybersecurity in Ukraine" (Law of Ukraine № 2163-VIII, 2017) amended the Law of Ukraine "On the State Service for Special Communications and Information Protection of Ukraine", which includes: accumulation and analysis of data on acts and / or attempts to commit unauthorized acts on State information resources in information and telecommunication systems, as well as their consequences, informing law enforcement agencies to take measures to prevent and cease criminal offenses in this area;

ensuring the functioning of the Government's computer emergency response teams CERT-UA (CERT is the English abbreviation "computer emergency response team"), which were established as teams of cyber incident information-gathering experts, the classification and neutralization of these incidents);

co-ordination of the activities of cyber security entities in relation to cyber security;

introduction of organizational and technical model of cyber defense, implementation of organizational and technical measures to prevent, detect and respond to cyber incidents and cyber-attacks and eliminate their consequences;

informing about cyber threats and appropriate methods of protection against them;

ensuring the implementation of the information security audit system at critical infrastructure facilities, establishing requirements for information security auditors, their certification (re-certification);

co-ordination, organization and audit of vulnerability of communication and technological systems of critical infrastructure facilities for vulnerability;

ensuring the functioning of the State Center for Cyber Defense (Law of Ukraine No. 3475-IV, 2006; Liha and Tech, 2021). In case of detection of cyber incidents and cyber-attacks that may pose a threat to national security or defense capabilities, the State Center for Cyber Defense and Counteraction to Cyber Threats of the State Service for Special Communications and Information Protection of Ukraine shall inform the National Cyber Security Coordination Center and provide the necessary information from the State Register on critical infrastructure facilities for the formation (adjustment) of the Cyber Security Strategy of Ukraine and other strategic decisions in this area (Stanislavskyi, 2020).

The State Service for Special Communications and Information Protection of Ukraine has proposed a Protocol of joint actions of key actors in cyber security, cyber defense actors and owners (managers) of critical information infrastructure facilities and in preventing, detecting, ceasing cyber-attacks and cyber incidents, as well as eliminating their consequences (Letter of the State Service for Special Communications and Information Protection of Ukraine No. 05/02-526, 2019), which provides for the exchange of information in response to cyber incidents and cyber-attacks (although it is mandatory only for public information resources with the application of the Procedure for Coordination of Public Authorities, Local Governments, Military Units, Enterprises, institutions and organizations, regardless of ownership, to prevent, detect and eliminate the effects of unauthorized actions on State information resources in information, telecommunications and information and telecommunications systems (Order No. 94, 2008).

In accordance with this procedure, these entities in the case of an attempt to commit and / or committing unauthorized actions in relation to information and telecommunications systems carry out the following actions:

- Take measures to immediately inform the State Special Communications Service by sending an appropriate electronic message in the form enshrined by this Procedure.
- CERT, which acts as a coordinator within the State Service for Special Communications and Information Protection of Ukraine,

within 24 hours should be informed by the security administrator of the information and telecommunication system, against which attempts or unauthorized acts are detected.

- Owners / managers of information and telecommunication systems should take measures to preserve (fix) signs of unauthorized actions and implement, among other things, the recommendations of the coordinator, as well as the physical access of his (her) representatives to implement measures to block and localize negative consequences of unauthorized actions and restore system.

Formally, the system seems to be working, but based on examples from the more advanced countries of the world, it does not take into account a number of domestic realities. The Law (Law of Ukraine № 2163-VIII, 2017) defines the main actors of the national cyber security system (and their specific tasks), cyberdefence actors, as well as a system of bodies to coordinate them. Indeed, the cyber security system has already been established for key players in the national cybersecurity system, as well as the coordination of their activities has been determined. But remains more significant in the number and range of entities not covered by these security protocols.

The objects of protection in information and telecommunication systems are the relationship of ownership of the information and software processed therein and the software that is designed to process this information. The actors of protection of information in information and telecommunications systems in addition to information owners are: information managers (on the basis of a contract or on behalf of the owner of information); system owners; system managers (on the basis of a contract or on behalf of the system owner); users (consumers of information and telecommunication services).

Although the Protocol should logically apply to the main actors of cyber security, cyber security entities and owners (managers) of critical information infrastructure, but the justification prior to its elaboration indicates not to extend its rules to cyber incidents, which are not related to unauthorized actions on State information resources. Similarly, the Law (Law of Ukraine № 2163-VIII, 2017) does not apply to internal (local) computer networks not interacting (not connected) to global computer networks.

Relationships developed using social networks, as well as "private" electronic information resources (apparently non-State ones) are not regulated by the Law "On the Basic Principles of Cyber security in Ukraine" under certain conditions – lack of information that needs to be protected by law (Dovhan and Doronin, 2017).

However, in the course of privatization, some of the critical infrastructure has already been privatized and, accordingly, the information contained in their information and telecommunications systems does not belong to the State, and therefore they are not formally protected. Moreover, the General Requirements for Cyber security of Critical Infrastructure do not address the exchange of information on cyber-attacks and cyber incidents at all.

This problem, in a slightly different context, has already been considered by the scientists, who noted that in the general problem of cyber security of critical infrastructure is particularly relevant in the development and implementation of organizational and legal mechanisms for strategic management of cyber security (Stanislavskyi, 2020). However, the issue of ensuring co-operation between the National Cyber Security Coordination Center, the State Cyber Defense Center, the Governmental Computer Emergency Response Team of Ukraine CERT-UA and other computer emergency response teams remains unclear, as well their interaction with international cyber security centers.

The division of responsibilities of special institutions to secure the State's cyberspace is unclear. This problem is a continuation of the regulatory uncertainty and, in particular, the lack of strategic documents with such segregation of duties (with a determination of the responsible agency) would be made.

The National Coordination Center for Cyber Security (under the National Security and Defense Council) does not have the appropriate capabilities, but practically coordinates only the main actors of cyber security in Ukraine, the list of which essentially includes the entire power unit and the main form of work of the Centre is the acceptance at its meeting s of instructions to other State bodies on the basis of information provided by both the main actors of cyber security and the special agency – the State Service for Special Communications and Information Protection of Ukraine.

But latter is the specially authorized agency in the area of special communications and information protection, and cyber security is not just about communication and information security. The system and related procedures of the State Service for Special Communications and Information Protection have been built up for decades to ensure the protection of information that is a state secret (of various status and level).

Therefore, the primitive inclusion of cyber threats in the list of tasks (and competencies) of the Special Communications and Information Protection of Ukraine is not effective; this is also understood by the authorities, since they have created (albeit on the basis of an already existing structure of the State Special Communications) a specialized unit – the State Center for Cyber Defense. Again, CERT-UA is a practically «fire brigade» for responding to computer emergency events (like other similar teams in the

world), one of the main functions of which is to interact with CERT of other countries.

Formally, the State Service for Special Communications and Information Protection should collect proposals from other entities, formulate a draft Action Plan on the implementation of the Cyber Security Strategy and submit it for approval to the National Security and Defense Council and the government (followed by a corresponding draft order of the Cabinet of Ministers of Ukraine at all stages of the development and adoption).

But such a plan has not been approved since 2019, which is not least due to the tendency to apply mechanisms of related law (information protection) addressing the challenges of cyber security and the imbalance between the interests of non-State actors (trying to ensure the integrity of their own information electronic resources, including those that provide critical infrastructure) and the strategic capabilities of the State Service for Special Communications and Information Protection in the area of cyber security (considering that these functions should be performed by the State Center for Cyber Security and the Government Computer Emergency Response Team (CERT-UA).

As a result, this work is not carried out systematically, the feedback between the State agency and private entities is not provided, which leads to either neglect of relevant proposals or implementation of strategic planning in the form of actual summarization of submitted proposals without appropriate adjustment. As a result, a significant part of cyber security entities, which are not the main actors of cyber security in Ukraine, remain outside the development of annual plans (Stanislavskyi, 2020).

It is also important to stress on the lack of effective interaction between cyber security actors in the context of minimizing the threat of cybercrime, taking preventive measures and investigating cybercrime.

Currently, the existing mechanisms of co-operation are limited to informing the law enforcement agencies of Ukraine about the detected unauthorized actions. However, in the absence of officers of operational units, pre-trial investigation agencies, prosecutors, judges with sufficient knowledge, skills and abilities in the area of information technology and cyber security, it is important to develop appropriate mechanisms for cooperation and involvement of other cyber security actors in the implementation of measures to prevent, detect and cease cybercrime. This issue is especially acute due to the need for an effective response of the State to the manifestations of transnational cybercrime, cyber terrorism and other illegal manifestations that threaten the cyber security of the State.

The analysis of the unified reports of the Prosecutor General's Office of Ukraine on registered criminal offenses and the results of their pre-trial investigation for the period 2019 – 2021 indicated low efficiency of pre-

trial investigation of cybercrime, which includes the suspension of criminal proceedings for lack of suspicion.

These problems cause the inefficiency of cyber security policy as the component of national security of Ukraine and require the changes in certain elements of this system:

- Updating the current Cyber security Strategy and the mechanism for its implementation by clearly defining its tasks (including the time frame for the implementation).
- Development and adoption of the annual State Plan for the implementation of the Cyber Security Strategy.
- Determination of specific measurable results of the Plan's implementation.
- Providing feedback during in formulating the Plan with stakeholders (including non-State critical infrastructure), the disruption of the normal functioning of which (due to the implementation of cyber security threats) may affect national and regional security; i.e., they should be equal partners in both the formation of the Plan and its implementation.
- Financing the implementation of measures to protect information and telecommunications systems of critical infrastructure of non-State ownership should be carried out at the expense of funds provided in the state budget for the implementation of the Cyber Security Strategy Implementation Plan.
- The State Center for Cyber Security should be presented not as a separate specialized unit within another agency, but as a separate entity with appropriate subordination and funding, which will focus solely on cyber security (rather than protection of information constituting official or State secrets), develop a planning mechanism for the implementation of The Strategy, ensure cooperation between cyber security actors (both state and non-State ones), the national coordinator and the Government.
- In order to coordinate the activities of critical infrastructure facilities, a person who has the functions of countering cyber threats and interacting with the State Center for Cyber Security should be included by the State.
- Central authorities that control the areas with critical infrastructure facilities should receive regulatory documents with the list of such objects, possible threats and actions taken to implement such threats in each of the possible situations and the capacity to provide cyber protection in-house.

- Developing and consolidating the mechanisms of interaction of the cyber security actors during the pre-trial investigation of cybercrimes in the criminal procedural legislation of Ukraine.
- Enshrining the possibility of conducting special criminal proceedings subject to all legally defined conditions in criminal proceedings on cybercrime in the Criminal Procedure Code of Ukraine.

Conclusion

Thus, Ukraine began to create a system of cyber security, for which a number of regulations were developed, the actors were identified and their functions in the area of cyber security were determined. However, the situation in the domestic cyber security sector is characterized by several significant problems:

1) the Cyber Security Strategy is formulated without taking into account the current state of cyber threats, systematic regulations identifying threats to Ukraine in cyberspace, rapid development of computer and communication technologies;
2) the annual plan for the implementation of the Cyber Security Strategy (which should detail the actions to ensure cyber security, determine specific measures, deadlines and responsible actors) is not drawn up;
3) the National Security Strategy of Ukraine does not partially meet the risks in cyberspace, as it only states the need to fulfill the task of developing a cyber security system (guaranteeing cyber resilience and cyber security of the national information infrastructure, including in the digital transformation), but only identifies the need to complete capabilities of cyber security and cyber defense actors and strengthening their coordination system.

In the absence of developed and implemented national standards and technical regulations at the level of critical infrastructure facilities (including information critical infrastructure) of non-State ownership, lack of information and communication technologies harmonized with relevant European standards, the actors that should provide cyber security (as a component of national security), solve the problems of securing cyberspace, are more focused on combating criminal acts with the use of information and telecommunications systems.

The proposed ways to improve the cyber security system (as part of national security) will update the legal mechanisms for cyber security, create cyber security infrastructure at the global level, establish effective

interaction between its actors regardless of their departmental affiliation and / or ownership (including with the owners of critical and information infrastructure of non-State ownership), increase the efficiency of pre-trial investigation of cybercrime.

Bibliographic References

BAKALINSKA, Olha; BAKALYNSKYI, Oleksandr. 2019. "Legal support for cyber security in Ukraine" In: Entrepreneurship, Economy and Law. No. 19, pp. 100-109.

BORYSOVA, Larysa. 2007. Transnational computer crimes as an object of forensic research. PhD Dissertation. Kyiv National University of Internal Affairs. Kyiv, Ukraine.

BRATEL, Serhii; MAKARENKO, Nataliia; BORTNYK, Valentyn; LEVCHENKO, Yurii, MYKYTCHYK, Andrii. 2021. "The Role of Rule-of-Law Institutions in Ensuring Information Security of Ukraine" In: Amazonia Investiga. Vol. 10, No. 39, pp. 238-244.

BYKOV, Valeriy; BUROV, Oleksandr; DEMENTIIEVSKA, Nina. 2019. "Cyber security in the digital learning environment" In: Information technologies and teaching aids. Vol. 70, No. 2, pp. 313-331.

DELESLINE, Nate. 2021. IT security and cybersecurity: What's the difference? Available online. In: https://www.zdnet.com/education/computers-tech/difference-between-it-security-cybersecurity/. Consultation date: 11/12/2021.

DIORDITSA, Ihor; KATERYNCHUK, Kateryna; TELESTAKOVA, Armenui; NASTIUK, Andrii. 2021. "Cyberterrorism as a threat to the cyber security of Ukraine: a discussion of Theoretical Aspects" In: Amazonia Investiga. Vol. 10, No. 40, pp. 73-83.

DOVHAN, Oleksandr; DORONIN, Ivan. 2017. Escalation of cyber threats to the national interests of Ukraine and legal aspects of cyber defense: a monograph. Armtek Publishing House. Kyiv, Ukraine.

DUBOV, Dmytro. 2010. Current trends in cyber security policy: conclusions for Ukraine. Analytical note. Available online. In: http://www.niss.gov.ua/articles/294/. Consultation date: 11/12/2021.

KOSINOVA, Daryna; IVCHUK, Kateryna; CHERNIAVSKYI, Oleksandr. 2021. "Legal analysis of the current state and trends in the development of the EU and Ukrainian legislation in the area of cyber security"

In: International Scientific Journal "Internauka", Series: Juridical Sciences. Available online. In: https://www.inter-nauka.com/issues/law2021/4/7119. Consultation date: 11/12/2021.

LAW OF UKRAINE NO. 2163-VIII. 2017. On the Basic Principles of Cyber security in Ukraine. Bulletin of the Verkhovna Rada of Ukraine, Kyiv, Ukraine. Available online. In: https://zakon.rada.gov.ua/laws/show/2163-19#Text. Consultation date: 11/12/2021.

LAW OF UKRAINE NO. 2469-VIII. 2018. On National Security of Ukraine, Bulletin of the Verkhovna Rada of Ukraine, Kyiv, Ukraine, 21 June 2018. Available online. In: https://zakon.rada.gov.ua/laws/show/2469-19#Text. Consultation date: 11/12/2021.

LAW OF UKRAINE NO. 3475-IV. 2006. On the State Service for Special Communications and Information Protection of Ukraine. Bulletin of the Verkhovna Rada of Ukraine. Kyiv, Ukraine. Available online. In: https://zakon.rada.gov.ua/laws/show/3475-15#Text. Consultation date: 11/12/2021.

LETTER OF THE STATE SERVICE FOR SPECIAL COMMUNICATIONS AND INFORMATION PROTECTION OF UKRAINE NO. 05/02-526. 2019. Protocol of joint actions of the key actors in cybersecurity, cyberdefence actors and owners (managers) of critical information infrastructure facilities and in preventing, detecting, ceasing cyber-attacks and cyber incidents, as well as eliminating their consequences. Available online. In: http://www.drs.gov.ua/wp-content/uploads/2019/06/5606.pdf. Consultation date: 11/12/2021.

LIHA.TECH. 2021. The National Security and Defense Council has adopted the Strategy for the development of cyber security in Ukraine for 5 years. Available online. In: https://tech.liga.net/technology/novosti/snbo-prinyal-strategiyu-razvitiya-kiberbezopasnosti-ukrainy-na-5-let. Consultation date: 11/12/2021.

LOPEZ, Julia. 2022. 2022 cyber security incentives and regulation review. GOV.UK. Available online. In: https://www.gov.uk/government/publications/2022-cyber-security-incentives-and-regulation-review/2022-cyber-security-incentives-and-regulation-review. Consultation date: 11/12/2021.

ORDER NO. 94. Procedure for coordinating the activities of public authorities, local governments, military formations, enterprises, institutions and organizations, regardless of ownership, to prevent, detect and eliminate the effects of unauthorized actions on State information resources in information, telecommunications and information and

telecommunication systems of the administration of the state service for special communications and information protection of Ukraine. Bulletin of the Verkhovna Rada of Ukraine. Kyiv, Ukraine. Available online. In: https://zakon.rada.gov.ua/laws/show/z0603-08. Consultation date: 11/12/2021.

ORDER OF THE CABINET OF MINISTERS OF UKRAINE NO. 1009-R. 2017. The concept of establishing the State system of critical infrastructure protection, Bulletin of the Verkhovna Rada of Ukraine, Kyiv, Ukraine, 06 December 2017. Available online. In: https://zakon.rada.gov.ua/laws/show/1009-2017-%D1%80?lang=en#Text. Consultation date: 11/12/2021.

ORDER OF THE PRESIDENT OF UKRAINE NO. 242/2016. 2016. On the National Coordination Center for Cyber Security. Bulletin of the Verkhovna Rada of Ukraine. Kyiv, Ukraine. Available online. In: https://zakon.rada.gov.ua/laws/show/242/2016#Text. Consultation date: 11/12/2021.

ORDER OF THE PRESIDENT OF UKRAINE NO. 447/2021. 2021. On the decision of the National Security and Defense Council of Ukraine "On the Cyber Security Strategy of Ukraine". Bulletin of the Verkhovna Rada of Ukraine. Kyiv, Ukraine. Available online. In: https://www.president.gov.ua/documents/4472021-40013. Consultation date: 11/12/2021.

ORDER OF THE PRESIDENT OF UKRAINE No. 96/2016. 2016. On the Cyber Security Strategy of Ukraine. Bulletin of the Verkhovna Rada of Ukraine, Kyiv, Ukraine, 15 March 2016. Available online. In: https://zakon.rada.gov.ua/laws/show/96/2016. Consultation date: 11/12/2021.

PRESS-CENTER OF THE NATIONAL SECURITY AND DEFENSE COUNCIL OF UKRAINE. 2021. The Working Group at the National Coordination Center for Cyber Security of the National Security and Defense Council of Ukraine approved the draft Cyber Security Strategy of Ukraine for 2021 – 2025. Available online. In: https://www.ukrinform.ru/rubric-society/3202073-rabocaa-gruppa-pri-snbo-odobril-proekt-strategii-kiberbezopasnosti.html. Consultation date: 11/12/2021.

STANISLAVSKYI, Taras. 2020. The development of cyber security public administration's mechanisms. PhD Dissertation. The Training of Personnel Institute of the State Employment Service of Ukraine. Kyiv, Ukraine.

SUSHKO, Olga. 2021. What Is Cybersecurity and Why Is It Important? Clario. Available online. In: https://clario.co/blog/what-is-cyber-security/. Consultation date: 11/12/2021.

UNIVERSIDAD
DEL ZULIA

CUESTIONES POLÍTICAS

Vol.40 Nº 73

Esta revista fue editada en formato digital y publicada en julio de 2022, por el ***Fondo Editorial Serbiluz, Universidad del Zulia. Maracaibo-Venezuela***

www.luz.edu.ve
www.serbi.luz.edu.ve
www.produccioncientificaluz.org