State Management of the Development of National Cybersecurity Systems

Myroslav Kryshtanovych †, Roman Storozhev ††, Kostiantyn Malyshev †††, Anna Munko ††††, Olena Khokhba †††††

drvel@ukr.net bvpjp0909@gmail.com zavadyakromann@gmail.com edu31iu@outlook.com anatol.nos@ukr.net

† *Lviv Polytechnic National University, Lviv, Ukraine*

†† Taras Shevchenko National University of Kyiv, Kyiv, Ukraine

††† Zhytomyr Polytechnic State University, Zhytomyr, Ukraine

†††† Dnipropetrovsk State University of Internal Affairs, Dnipro, Ukraine

††††† Dnipropetrovsk State University of Internal Affairs, Dnipro, Ukraine

Abstract

The main purpose of the study is to determine the main elements of the state management of the development of national cybersecurity. Cybersecurity ensures the protection of the properties of information resources and the operability of technical and software users and is directed against relevant cyber incidents. Therefore, today it is impossible to ignore the importance of public administration of the processes taking place in it. The methodological support of our study is determined by its goals and objectives and is based on the use of a combination of general scientific and special methods of scientific knowledge, which ensured the completeness and reliability of the results obtained. The article has limitations and concerns the lack of practical implementation of the research results. The study is purely theoretical to reflect the main aspects of the modern system of state management of the development of national cybersecurity. Further research requires an analysis of the world experience of state management of the development of national cybersecurity.

Keywords:

State management, National Cybersecurity, cybersecurity, security.

1. Introduction

The globalization of social relations and the acceleration of technological progress determine a clear understanding that the modern information society covers all spheres of human and state life, and the cybersphere has become an important economic, political and social resource. The technological development of information relations has created new opportunities for social progress, but at the same time it has also created new opportunities for abuse, and with the development of Internet technologies, a very specific group of threats to the national security system has emerged.

In modern society, the issue of cybersecurity is attracting more and more attention. The relevance of the administrative and legal support of cybersecurity is determined by the modern development of the information society, which is moving from traditional state management to management through electronic forms, the formation of new forms of information activity, which leads to a significant expansion of the volume of information, the penetration of its components into various areas of public activity. At the same time, the development of the information society and the existing legal instruments ensure the implementation of the information rights and obligations of citizens, determine the degree of development of the information sphere, the state of the information law and order, the level of legal protection and protection of social values.

In recent decades, the development of information and communication technologies, cybernetics and the Internet has led to significant changes in society. The Internet has brought great social benefits to the world for many forms of activity. These incomes have become significant for people, businesses, the state and society as a whole. Today, information and communication technology systems are integrated into all aspects of society and are critical to its functioning. And cyberspace and technology have become the basis for interaction between different sectors, both public and private, and can be considered a fundamental social infrastructure. But along with a large number of advantages, a significant number of threats associated with the functioning of modern technologies have appeared. This phenomenon has led to the emergence of a significant number of dangers that affect society both at the national and international levels. So, there is a need for mechanisms to protect cyberspace, which are described in the national strategies of

Manuscript received May 5, 2022
Manuscript revised May 20, 2022
https://doi.org/10.22937/IJCSNS.2022.22.5.3

world states dedicated to ensuring its protection. Therefore, a rather important topic is the study of the main aspects of state management for the development of national cybersecurity.

2. Methodology

The methodological support of our study is determined by its goals and objectives and is based on the use of a combination of general scientific and special methods of scientific knowledge, which ensured the completeness and reliability of the results obtained. In the course of the study, we used general and specific scientific methods: systemic and structural-functional approaches, which made it possible to determine the essence, structure, functions and special features of state management in the development of cybersecurity and information security.

3. Research Results and Discussions

The Internet was a concentrated reflection of the general trends of the information revolution of the late XX - early XXI century. It becomes obvious that the Internet integrates not only communication and technological resources, but also material, financial, intellectual, humanitarian, political and other resources, forms and diversifies the processes of social regulation. The logic of regulation of the Internet itself and the relations associated with its use, in particular, the solution of the issues of Internet governance, its safe use, is objectively in the plane of both national and international law.

The World Wide Web has long become a daily routine, providing access to a wide range of information, but at the same time an easy and affordable way to manage and control people by the state. Conversely, the population of many countries now has the ability to monitor the activities of the authorities through reports on online platforms. In addition, a modern citizen has the opportunity to receive information almost uncontrollably from the state, which is fundamentally different from those times when everything went through censorship.

The comprehensive penetration of information technologies into the daily activities of the individual, society and the state, the ever-growing dependence of observance of fundamental human rights and freedoms on the constancy of the functioning of networks and information systems, the growing sensitivity of the consequences of security incidents for these cybersecurity subjects requires the implementation of operational measures to restore the capabilities of such systems and networks, and systemic measures to improve network and information security in general. A special place in solving this problem is occupied by the introduction of an effective, reliable and productive national system of cybersecurity and cyber defense.

Global informatization in the modern world actively controls the existence and life of the states of the world community. Information technologies are used in solving problems of ensuring state, military, economic security, etc. At the same time, one of the fundamental consequences of global informatization was the emergence of a fundamentally new environment for confrontation between competing states - cyberspace. This concept is understood as a set of interconnected information resources, software, databases and data banks processed in computer networks and related infrastructure, together with objects that fall under their control and management. During the formation of global cyberspace, military and civilian computer technologies converge, new means and methods of actively influencing the information infrastructure of potential adversaries are intensively developed in leading foreign countries, various specialized cybernetic centers and command units are created, the main task of which is to protect state information infrastructures.

Today, the problem of protecting information processed in information and telecommunication systems from challenges and threats in cyberspace is one of the most important for any state, and ensuring an appropriate level of cybersecurity of the state is a necessary condition for ensuring the national security of the state, the development of the information society. In the context of globalization of information processes, their integration into various spheres of public life, the leadership of the leading states of the world pays special attention to the creation and improvement of effective public administration systems and the protection of critical infrastructure from external and internal threats of a cybernetic nature. In many leading countries of the world, national systems of state management of cybersecurity have already been formed as the most optimal organizational structures capable of

accumulating the forces and means of various government agencies and the private sector in a short period of time to counter cyber threats [1-5].
The key stages in ensuring the effectiveness of the state management system for the development of cybersecurity are presented in Figure 1.

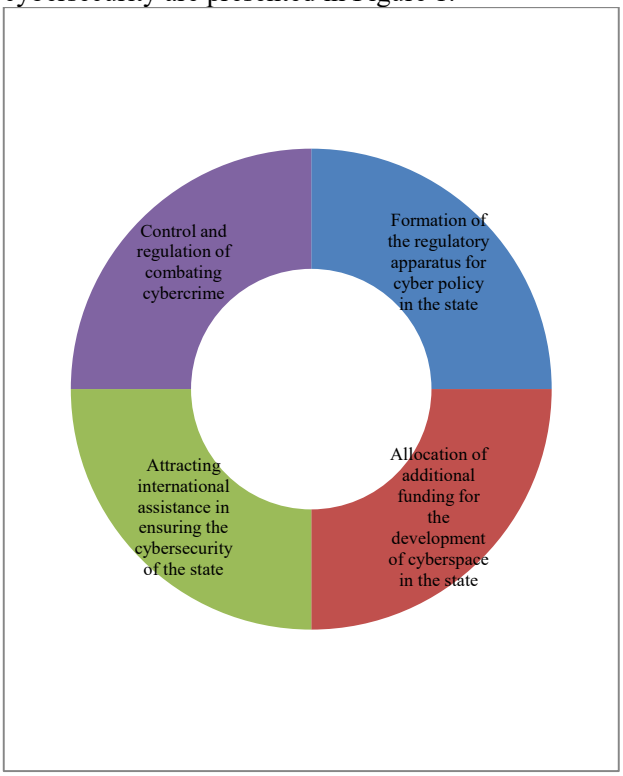

Fig. 1 The key stages in ensuring the effectiveness of the state management system for the development of cybersecurity.

At the present stage of the latest information technologies, cybersecurity, which includes an interdepartmental character in a globalized world, is becoming relevant. After all, cybersecurity is a human rights manifestation of the modern virtual world against the background of the innovative development of information technologies in the system of legal capital.

In the modern conditions of the information world, a special place in scientific research, which is activated every year, is occupied by cybersecurity. Recently, cybersecurity and its particular aspects have become the subject of numerous research papers. However, the problem of understanding this phenomenon remains open, which is logical and necessary, given the ultra-high pace of development of social relations in the electronic sphere. This is due, first of all, to the expansion of the possibilities of informational influence on public relations, which leads to the emergence of new threats to public security and necessitates updating and improving the system for ensuring it. In addition, the very concept of cybersecurity requires a qualitative rethinking, caused by the rapid essential changes in the phenomenon of information and the dominant trends in the development of the world community, which largely receives an “information” dimension [6-8].

In the context of the modern development of cybercapital as a systemic electronic control, monitoring and representation of the activities of all spheres of public life, the question of the legal logic of public administration is relevant. After all, today a significant number of citizens are suffering from a socio-economic crisis, to which a military-political conflict is added. At the same time, one of the factors of these negative social phenomena is corruption, which has already acquired a systemic character. Such corruption is considered a real threat to national and global security, as it hinders the conduct of effective activities that determine the military and law enforcement structures of the domestic and international process in this direction.

In the context of the mobile development of the global information society, the widespread use of information and communication technologies in all spheres of life, the problem of cybersecurity is of particular importance. Cybersecurity cannot be guaranteed without close cooperation with influential security structures at the regional, trans-regional and global levels. Taking care of its security, each state or group of states must support the development of effective stability mechanisms, regarding this as an important component of their own national security.
Cybersecurity is achieved through a balance between the information rights and freedoms of various subjects of law and the protection of national information sovereignty. After all, the issue of cybersecurity, and national security in general, is primarily a matter of balance between human rights and interests and the competence and interests of state power, a balance that can only be established with the help of legal norms. A very important aspect of determining the principles for the formation and operation of a cybersecurity system is the consideration of international legal norms. The main goal of ensuring cybersecurity should be determined on the basis of a broad understanding of this concept

as an important component of national security and a system-forming factor in all spheres of human life, society, state, political, economic, socio-cultural, scientific and technological, defense, environmental, proper informational component of national security.
To date, the issue of implementing state strategic planning in the field of ensuring cybersecurity is still insufficiently disclosed, which primarily provides for the development of annual plans for the implementation of the provisions of the Cybersecurity Strategy, their implementation in practice, the identification of priority measures, the adoption of which will guarantee the cyber protection of state information resources. critical information infrastructure [9-11].

Implementation of the state management in the field of cybersecurity within their competence is carried out by: ministries and other central authorities; local state administrations; local governments; law enforcement, intelligence and counterintelligence agencies, subjects of operational-search activities; Armed Forces, other military formations formed in accordance with the law; National Bank; enterprises, institutions and organizations classified as critical infrastructure facilities; business entities, citizens, other persons carrying out activities and / or providing services related to national information resources, electronic information services, electronic transactions, electronic communications, information security and cyber defense. It should be noted that the regulatory framework in the field of regulating the development of the information society and measures for the formation of state information policy should be consistent with the tasks in the field of information security, the practice of ensuring the preservation of state secrets, protecting information and telecommunications infrastructure and information resources from cyber attacks and other threats in information space It is important to create favorable conditions for the improvement of domestic information security systems, which is of particular relevance in connection with the expansion of information exchange via the Internet. There is an urgent need to develop agreed rules and procedures for protecting the national interests in the process of integration into international information networks [12-15].

The main measures to counter cyber threats in the context of ensuring the cybersecurity of the state are presented in Table 1.

Table 1: The main measures to counter cyber threats in the context of ensuring the cybersecurity of the state

№	The main measures to counter cyber threats in the context of ensuring the cybersecurity of the state
1	Formation and effective implementation of cybersecurity policy
2	The development of new lines of defense, one of which should be international cooperation between all interested parties, so that in the event of a cyber attack, the competent authorities of the attacked party and from whose territory the cyber attack occurs operate mechanisms for prompt notification of such an incident, and also joint fight against it
3	Formation of a unified strategy for the protection of cyberspace in the state
4	Creation and holding of a number of international conferences to gain relevant experience in responding to cyber threats

The state management should lay the foundation for solving the main tasks of developing a democratic and free society, the main of which is the formation of a single secure information space and its entry into the global virtual space, cybersecurity of the individual, society and the state. In addition, much attention should be paid to the formation of a democratically oriented mass consciousness, the development of the information services industry, the legislative regulation of public relations, including those related to the receipt, dissemination and use of information.

4. Conclusions

Summing up the results of the study, it should be noted that cyberspace has become the cause of social and economic growth due to its openness and accessibility to all actors. Over-administration and regulation of cyberspace reduces its benefits and can hinder strong growth in all areas of activity. Therefore, it is very important to ensure openness and interoperability in the cybernetic network, as well as to maintain and develop a safe and reliable cyberspace to create a free flow of information. This will ensure freedom of expression and vibrant economic activity in cyberspace, promote innovation, economic growth and social challenges, and provide

positive benefits that will be available to the global community. Every state in the world, as well as business structures, are taking advantage of the expansion of cyberspace. As a result, cyber threats have become a reality, they are transcontinental in nature and the consequences of their interventions in critical infrastructures have become more severe. Cybersecurity expands the scope of classical IT security to cover the entire cyberspace. The latter includes all information technology connected to the Internet or similar networks, including cyberspace communications, programs, processes and processed information. Thus, for all intents and purposes, modern information and communication technologies become part of cyberspace.

Government leaders are increasingly realizing that promoting prosperity and protecting national security includes ensuring cybersecurity. This means that the nation, state, region or city is a safe environment for living, receiving services and doing business on the Internet. And that includes preventing cyberattacks, preventing cybercrime-related crimes, and protecting critical national infrastructure, as well as maintaining an environment that facilitates technological progress.
Consequently, as a result, modern technologies are progressing at a rapid pace today. The global world of information and information networks and systems is no exception. is actively developing. Such a growth rate of information technology has led to the need for the immediate creation of secure means of working in the cybernetic network and the Internet. Users are faced with a type of crime that was almost unknown to them before - cybercrime. This is how the term “cybersecurity” was born. This area of security is an important component of the entire state defense system.

The article has limitations and concerns the lack of practical implementation of the research results. The study is purely theoretical to reflect the main aspects of the modern system of state management of the development of national cybersecurity. Further research requires an analysis of the world experience of state management of the development of national cybersecurity.

References

[1] Gordieiev, O., Kharchenko, V., Illiashenko, O., Morozova, O., Gasanov, M. Concept of using eye tracking technology to assess and ensure cybersecurity, functional safety and usability. *International Journal of Safety and Security Engineering*, Vol. 11, No. 4, 2011, pp. 361-367. https://doi.org/10.18280/ijsse.110409

[2] Kryshtanovych, M., Petrovskyi, P., Khomyshyn, I., Bezena, I., & Serdechna, I. Peculiarities of implementing governance in the system of social security. *Business, Management and Economics Engineering*, 2020, 18(1), 142-156. https://doi.org/10.3846/bme.2020.12177 .

[3] Ismail A., Saad M., Abbas R. Cybersecurity in internet of things, *Review of Computer Engineering Studies,* Vol. 5, No. 1, 2018, pp. 17-22. https://doi.org/10.18280/rces.050104

[4] Kryshtanovych M., Britchenko I., Lošonczi P., Baranovska T., Lukashevska U. State Management Mechanisms for the Exchange of Information Regarding Cyberattacks, Cyber Incidents and Information Security Incidents. International *Journal of Computer Science and Network Security*. Vol. 22 2022, No. 4 pp. 33-38. https://doi.org/10.22937/IJCSNS.2022.22.4.5

[5] Sylkin, O., Kryshtanovych, M., Bekh, Y., & Riabeka, O. Methodology of forming model for assessing the level financial security . *Management Theory and Studies for Rural Business and Infrastructure Development*, 2020, 42(3), 391–398. https://doi.org/10.15544/mts.2020.39

[6] Kryshtanovych, S., Gutsulyak, V., Huzii, I., Helzhynska, T., & Shepitchak, V. Modeling the process of risk management response to the negative impact of risks as the basis for ensuring economic security. *Business, Management and Economics Engineering,* 2021, 19(2), 289-302. https://doi.org/10.3846/bmee.2021.14798

[7] Kryshtanovych, S., Treshchov, M., Durman, M., Lopatchenko, I., & Kernova, M. Gender parity in public administration in the context of the development of european values in the management system. *Financial and Credit Activity: Problems of Theory and Practice*, 2021, 4(39), 475–481. https://doi.org/10.18371/.v4i39.241416

[8] Petroye, O., Lyulyov, O., Lytvynchuk, I., Paida, Y., Pakhomov, V. Effects of information security and innovations on country’s image: Governance aspect. *International Journal of Safety and Security Engineering*, Vol. 10, No. 4, 2020, pp. 459-466. https://doi.org/10.18280/ijsse.100404

[9] Lainjo, B. Network security and its implications on program management. *International Journal of Safety and Security Engineering*, Vol. 10, No. 6, 2020, pp. 739-746. https://doi.org/10.18280/ijsse.100603

[10] Yasmin, M., Sohail, A.; Sarkar, M., & Hafeez, R. Creative methods in transforming education using human resources. *Creativity Studies*, 10(2), 2017, 145-158. https://doi.org/10.3846/23450479.2017.1365778

[11] Gandhi, R., Sharma, A., Mahoney, W., Sousan, W., Zhu, Q., Laplante, P. Dimensions of cyber-attacks: Cultural, social, economic, and political. *IEEE Technology and Society Magazine,* 2011, 30(1): 28-38. https://doi.org/10.1109/MTS.2011.940293

[12] Jarvis, L., Macdonald, S., Nouri, L. The cyberterrorism threat: Findings from a survey of researchers. *Studies in Conflict & Terrorism*, 37(1): 2014, 68-90. https://doi.org/10.1080/1057610X.2014.853603

[13] Thijittang, S. A study of pragmatic strategies of English of Thai University students: Apology speech acts. University of Tasmania. 2010.https://eprints.utas.edu.au/10754/7/Thijittang_whole_thesis.pdf

[14] Hutchings, A. Crime from the keyboard: organised cybercrime, co-offending, initiation and knowledge transmission. *Crime, Law and Social Change,* 62(1): 2014, 1-20. https://doi.org/10.1007/s10611-014-9520-z .

[15] Luo, H.N. An emergency management system for government data security based on artificial intelligence. *Ingénierie des Systèmes d'Information*, Vol. 25, No. 2, 2020, pp. 207-213. https://doi.org/10.18280/isi.250208