INTERNATIONAL PRACTICE OF LEGAL SUPPORT OF CYBER SECURITY OF THE COUNTRY

Taras Sozanskyy, Lviv State University of Internal Affairs
Ivan Krasnytskyi, Lviv State University of Internal Affairs
Vasyl Lutsyk, Lviv State University of Internal Affairs
Galyna Yaremko, Lviv State University of Internal Affairs
Nazarii Tuz, Lviv State University of Internal Affairs

ABSTRACT

There are systematized and generalized the countries experience on questions of formation and implementation of the state policy of ensuring cyber security on the basis of research of the state policy experience of ensuring cyber security, there are proved necessity of application of administrative influence on processes of ensuring cyber security and revealed possibilities of the adaptation to national circumstances. According to the results of a study conducted among the heads of enterprises and organizations in different countries, it is found that the valuation indicator a cyber attack as an imminent threat, among the leaders: the United States, Australia and Germany. It is determined that over the past ten years, action plans and strategies designed to solve the problem of cyber security have been distributed throughout Europe. It is established that in an environment where cyber threats constantly appear and develop, the state policy of countries is based on flexible, operational strategies of cyber security. The cross-border nature of threats makes the countries to engage in close international cooperation that is due not only need of effective operation to cyber attacks, but the feasibility of timely response, coordinated prevention mechanisms. Attention is focused on the fact that the formation of the national state strategy of cyber security is the basis for the development of effective state policy.

Keywords: Cyber Security, Legal Regulation, Strategy, Policy, Cyber Attack.

INTRODUCTION

The rapid development of information and communication technologies has contributed to the formation of cybernetic space, which has a significant impact on the socio-economic situation of each country in the world and the national security.

However, information technologies not only open up certain opportunities for the development of the country, but also create a number of challenges and threats that are intensified with the spread of such technologies in the political, social and economic spheres, actualizing the processes associated with ensuring cyber security.

In modern conditions, which are characterized by an increase in the number of cyber attacks and cyber incidents, leading to financial losses, disruption of the functioning of information and telecommunication systems, affecting the state of national security and defense of the country, the world has an urgent task to form a state policy to ensure cyber security as a

means of strengthening the security and reliability of information systems, adequate to modern challenges and realities, aimed at timely identification, prevention and neutralization of real and potential cyber interventions and threats of private, corporate, national interests on the basis of an integrated approach and the participation of all entities.

The formation of the state policy of ensuring cyber security is a complex methodological problem that requires detailed consideration in order to develop approaches, methods, instruments, that allow realizing the process of management activity in this area to preserve the openness and security of cyber space.

The aim of the work is to deepen the theoretical foundations and development of scientific, methodological and practical recommendations for the formation of state policy of cyber security ensuring.

REVIEW OF PREVIOUS STUDIES

According to experts valuations, in the field of cyber security of the vast majority of the leading countries of the world, there is a steady trend to a significant increase in the number and expansion of the spectrum of cyber-attacks in order to violate the confidentiality, integrity and availability of public information resources, including those that circulate on the objects of critical information infrastructure (Tetiana et al., 2019).

This is confirmed by the results of a study conducted among business leaders and organizations in various countries Sun et al. (2018), which found that about half of company executives (49%) note the possibility of a cyber-attack as a question of "*when*" rather than "*if*" (Kulish et al., 2018).

The issue of the formation of modern cyberspace and scientific and practical approaches to solving problems in the field of cyber security are devoted to the works of such researchers as Dean & McDermott (2017), Anwar et al. (2017) and other.

The problems of state policy formation, the theoretical foundation of public administration as whole are paid attention to in the works Carrapico & Barrinha (2017), Hilorme et al. (2019) and many others.

Theoretical and methodological foundations of solving problems in the field of state regulation of cyber security processes are reflected in the works of such scientists as Drobyazko et al. (2019).

However, despite a wide range of results of researches of scientists, it is necessary to specify that the range of the questions connected with development, improvement and introduction of methodological approaches concerning formation of the state policy of ensuring cyber security still remains unresolved. Therefore, there is a need to develop a holistic theoretical and methodological framework for ensuring cyber security, which should be based on the use of effective instruments, taking into account the modern risks of cyber attacks and cyber incidents, aimed at the formation of a safe cyber space.

The importance and relevance of these issues and the incomplete solution in certain problems, the absence of unambiguous theoretical justification and relevant methodological and practical developments caused the theme of the works, the purpose, objectives and structures, theoretical and practical significance.

METHODOLOGY

The studies of methodological and theoretical provisions of the work are based on the general scientific principles of complex researches, the works of leading scientists on the state policy issues of ensuring cyber security.

The methodological basis of the research is the conceptual provisions of modern economic theory, the theory of public administration, methods of system analysis, and general scientific principles of the scientific researches. There were used general scientific and specific approaches methods and techniques in the course of the research, in particular: monographic, system analysis, method of generalization, complex approach-for studying theoretical bases of formation the state policy of ensuring cyber security; the method of comparative analysis- in the study of the experience of the state policy of cyber security and identifying the possibility of the adaptation; the method of concretization, graphic- in the analysis of the development level of information and communication technologies, cyber threats and the formation of analytical support for state management of cyber security; conceptualization, abstract-logical method, prescriptive analysis.

RESULTS AND DISCUSSIONS

Cyber security is increasingly seen as a strategic issue at the state level a means of enhancing the security and reliability of information systems and concerns all categories of society. Therefore, a strategic approach is used to solve it: a number of state goals and priorities are put forward that need to be achieved over a certain period of time. In fact, the strategy is a model for solving the problem of cyber security within the state.

The analysis of strategic documents of some countries of the world allowed coming to certain conclusions.

Thus, the International Strategy for cyberspace of the United States is based on the model of cooperation between the government, international partners and private sector and contains a set of measures in the following areas: economy (promotion of international standards and innovative, open markets); protection of national networks (improvement of security and reliability); law and order (expansion of cooperation and legal norms); military industry (preparation for modern security challenges); internet governance; development of international cooperation; freedom on the internet (support of fundamental freedoms and privacy).

Cyber security strategy of Canada is formed in the following areas: protecting government systems (establishing clear roles and responsibilities, strengthening cyber systems security and raising government awareness in the field of cyber security); collaborating to protect key cyber systems outside Government (public-level partnerships involving the private sector and critical infrastructure sectors); ensuring the safety of Canadian citizens in the online environment (combating cybercrime and protecting Canadian citizens in the online environment, the issue of personal data protection).

The key aspects of cyber security Strategy of Japan are as follows: strengthening the fight against potential mass cyber attacks and formation of a body responsible for preventing such attacks; introduction of a policy adapted to changes in the field of information security; preference of active information security policies over passive. At the same time among the main activities highlighted: IT risk management to ensure the safe life of society; the implementation of policy that will strengthen national security, improve crisis management in cyberspace and

will not contradict the policy of using information and communication systems, which serves as the basis for socio-economic activity; implementation of policy aimed at a comprehensive solution to the problem of national security, crisis management and protection of society and person; introduction of information security policy, which does not contradict the strategy of economic growth; development of international alliances.

It should be noted that the EU has an active policy in the field of cyber security.

The European Commission has repeatedly stressed the importance of network and information security and the feasibility of creating a single European information space. There are proposed changes in the existing regulatory framework, practical measures and regulatory norms to enhance the safety and reliability of public networks as a result of the meetings.

Awareness of the importance of cyber security led EU countries to establish the European network and information security agency (ENISA) in 2004. The agency serves as more of an advisory body than a force. The main activity of the agency is to assist the community in providing network and information security to EU member States and business communities.

The tasks of agency are to inform the public about of new viruses, hacker attacks, security problems in the information space of Europe, investigation of epidemics of viruses and electronic attacks.

According to the results of the study, over the past decade, the state policy of ensuring cyber security of the EU countries has undergone significant reforms and transformations, which resulted in the formation, approval and implementation of appropriate state strategies. Throughout Europe took out a proliferation of action plans and strategies to meet the challenge of ensuring cyber security.

Despite the unanimous determination at the state level of the appropriateness of international cooperation in the field of cyber defense, such disagreements significantly complicate such interaction.

Let us consider national strategies specifics aimed at ensuring the cyber security of the EU countries.

Taking into account the consequences of a large-scale cyber attack that took place in 2007, Estonia became one of the first EU member States to publish a state cyber security strategy in 2008.

It should be noted that Estonia attaches particular importance to the need to protect cyberspace in general and places the security of information systems at the centre of attention; the recommended activities are civil in nature and based on legal regulation, training and cooperation.

It should be noted that the strategy of Finland is based on the consideration of cyber security as economic problem, which has an impact on the development of the information society.

The relevant strategy of Slovakia focuses on the implementation of information security measures as one of the conditions for the development of the society. It is aimed at preventing threats through the introduction of modern instruments and set of measures.

The key objectives of the Czech cyber security strategy include protecting information and communication systems from vulnerabilities to which these systems succumb and reducing the potential damage from attacks on systems. The main focus of the strategy is focused on the problems of free access to information services, data integrity and confidentiality in the

cyberspace of the Czech Republic. It should be noted that the strategy is sufficiently integrated and consistent with other legal documents of the Czech Republic.

The analysis of the features of the implementation of the strategic approach in the field of cyber defense in France has identified benchmarks for the ability of information systems to withstand events in cyberspace that can negatively affect the availability, integrity and confidentiality of information. France focuses on technical means of information protection, combating cybercrime and providing cyber protection. It is received the course on strengthening of the current legislation and development of international cooperation.

The strategy of Germany lays the foundation for the security of the critical information systems. The country is focused on preventing and prosecuting cyber attacks as well as preventing and preventing the failure of IT equipment that is caused by accidental factors. We emphasize that the latter concerns critical information systems. The strategy analyzes whether and where additional actions are needed to protect IT systems by providing basic security functions certified by the state, as well as by supporting small and medium-sized businesses through the creation of a new working group.

Lithuania is focused on defining goals and measures aimed at developing the circulation of electronic information, as well as ensuring the confidentiality, accessibility and integrity in cyberspace. In addition, the strategy of this country is aimed at protecting personal data, telecommunication networks, information systems and critical infrastructure from cyber threats through the formation and implementation of appropriate measures that can ensure a secure cyberspace.

Aware of the vulnerability of information and communication technologies, the strategy of Luxembourg defines the importance of public and economic security and information and communication technologies for the economic development of society. Implementation of the strategy is envisaged in the following areas: protection of key information infrastructure and timely response to security incidents; modernization of the regulatory framework; state and international cooperation; training and information; promotion of standards.

Holland, on the one hand, is committed to secure and reliable information and communication systems, fearing serious violations in these systems, and on the other hand, recognizes the need for freedom and openness of the Internet-space. The strategy defines cyber security which is understood as protection against failures and improper operation of information and telecommunication systems. The country aims to investigate and prosecute crimes in cyberspace.

UK government policy is focused on the development of cyber security has an innovative focus. The goal is to bring the country to the first place out of innovations, investments and quality of services in the field of information and telecommunication technologies, and thus, to take full advantage of all the advantages and advantages of cyberspace.

The results of the study of foreign experience in the formation of state policy for ensuring cyber security of the EU countries allowed to state that in an environment where cyber threats constantly appear and develop, state policy is based on flexible, operational strategies of cyber security.

The cross border nature of threats forces countries to engage in close international cooperation. Such cooperation is necessary not only for effective preparation for cyber attacks, but also for timely response to them, development of coordinated mechanisms of prevention.

We state that the definition of strategic approaches, the formation of the national state strategy of cyber security, development of mechanisms, instruments, measures to counter the challenges and threats in this area has become the basis for the development of effective state policy of the EU countries.

It should be noted that the formation of an appropriate package of documents of a regulatory nature on this issue allowed the countries to determine the legal and organizational bases of state policy in this area the basic principles and directions of ensuring the cyber security of the EU member States.

RECOMMENDATIONS

According to the results of researches on the situation with ensuring cyber security in the EU member States, which was made by BSA-Software Alliance (organization that represents the interests of the largest "software" companies in the world), Sun et al. (2018), the leaders in public-private partnership (hereinafter- PPP), in this area were five countries: Austria, Germany, the Netherlands, Spain and the United Kingdom. It should be noted that the analysis was carried out according to 25 criteria, grouped as follows: legal bases for the functioning of cyberspace; organizational institutions and mechanisms; sectorial cyber security; cyber security education.

It should be noted that the formation of a common policy, which, along with national, provides for joint activities and a single common policy at the supranational level speaking about the European experience of regulatory activity in this area. Among the main components, it should be noted the following:

The use of various forms of public-private partnership (PPP) in the fight against cybercrime, which is reflected in the relevant agreement in the field of cyber security industry;

initiation by the European Commission and formation of an action plan, which defined the main aspects of regulation of legal and economic relations in the field of cyber security in order to create platform aimed at the development of research and innovation potential for cyber security in various sectors (energy, health care, transport and finance) as well as the inclusion in this process of authorities, representatives of science and other stakeholders;

Acceptance by the European Commission of the digital single market Strategy, EU Cyber strategy and the EU network and information security Directive, which should be incorporated into the national legislation of the member States and the internal statutory documents of the main enterprises.

The increase in the number and constant changes in the nature of cyber threats, in turn, contributed to the dynamism of the cyber security market, increasing the number of entities interested in the further development in various sectors of the counties economy and forming the national legislation of the EU countries, taking into account the features of measures to protect critical infrastructure.

CONCLUSIONS

Among the main common features of state cyber security strategies are the following:

1. Building a government model aimed at ensuring cyber security and identifying an appropriate mechanism (mainly public-public partnership) that allows private and public stakeholders to discuss and approve policies related to the cyber security problem;

2. Planning and definition of regulatory mechanisms, clear identification of roles, rights and responsibility for the private and public sector;
3. International cooperation, introduction of the necessary legislative framework in this area;
4. Improve readiness, reduce incident response time, develop a disaster recovery plan and protection mechanisms for critical infrastructure objects;
5. Development of a systematic and integrated approach to public risks management;
6. Formation of information programs designed to teach users new patterns of behavior and work; formation of education programs that provide training for it professionals and professionals in the field of cyber security;

However, it should be noted that at the international level today there is still no single definition of the cyber security. This term, as well as other key definitions that are given in regulatory documents, differ significantly. Having certain common features, the national strategies of EU countries aimed at the formation of a secure cyber space are characterized by a variety of approaches and specific measures that take into account the peculiarities of state policy in this area.

It should be noted that the study of positive world experience in the implementation of PPP as an instrument for ensuring cyber security and the adaption to modern conditions will form a modern, effective basis for the formation of an effective state policy in this area in order to create mechanisms for cooperation and partnership in the field of cyber security.

Among the main directions, it should be noted the following:

1. Development of PPP in the formation of legislative framework, the creation of relevant industry standards in the field of cyber defense;
2. Government support for scientific researches aimed at protecting against cyber incidents;
3. Introduction and implementation of the program approach to build effective cooperation in the exchange of information in the field of cyber security between the state and business;
4. Creation of a mechanism for state support of innovations in the field of cyber security using PPP mechanisms.

Thus, the systematization and generalization of the developed countries experience on the formation and implementation of the state policy of ensuring cyber security has allowed to prove the need for the use of managerial influence on the processes of ensuring cyber security. The state policy of the leading countries of the world is based on flexible, operational cyber security strategies.

REFERENCES

Anwar, M., He, W., Ash, I., Yuan, X., Li, L., & Xu, L. (2017). Gender difference and employees' cyber security behaviors. *Computers in Human Behavior, 69*(1), 437-443.

Carrapico, H., & Barrinha, A. (2017). The EU as a coherent (cyber) security actor? *JCMS: Journal of Common Market Studies, 55*(6), 1254-1272.

Dean, B., & McDermott, R. (2017). A research agenda to improve decision making in cyber security policy. *Penn State Journal of Law &International Affairs, 5*(1), 29.

Drobyazko, S., Alieksieienko, I., Kobets, M., Kiselyova, E., & Lohvynenko, M. (2019). Transnationalisation and segment security of the international labor market. *Journal of Security and Sustainability Issues, 9*(2), 1-20.

Drobyazko, S., Makedon, V., Zhuravlov, D., Buglak, Y., & Stetsenko, V. (2019). Ethical, technological and patent aspects of technology blockchain distribution. *Journal of Legal, Ethical and Regulatory Issues, 22*(2S), 1-9.

Drobyazko, S., Potyshniak, O., Radionova, N., Paranytsia, S., & Nehoda, Y. (2019). Security of organizational changes via operational integration: Ensuring methodology. *Journal of Security and Sustainability Issues, 9*(1), 1595-1612.

Hilorme, T., Tkach, K., Dorenskyi, O., Katerna, O., & Durmanov, A. (2019). Decision making model of introducing energy-saving technologies based on the analytic hierarchy process. *Journal of Management Information and Decision Sciences, 22*(4), 489-494.

Kulish, A., Petrushenko, M., Reznik, O., & Kiselyova, E. (2018). The relations unshadowing in business activities: The economic and legal factors of security at the macroeconomic level. *Problems and Perspectives in Management, 16*(1), 428-436.

Sun, C.C., Hahn, A., & Liu, C.C. (2018). Cyber security of a power grid: State-of-the-art. *International Journal of Electrical Power & Energy Systems, 99*(1), 45-56.

Tetiana, H., Chernysh, O., Levchenko, A., Semenenko, O., & Mykhailichenko, H. (2019). Strategic solutions for the implementation of innovation projects. *Academy of Strategic Management Journal, 18*(1), 1-11.