UDC 351.746:007 (477)
DOI https://doi.org/10.32836/2308-6971/2020.1.6

STATE REGULATION IN THE FIELD OF CYBERSPACE PROTECTION AS A COMPONENT OF ENSURING INFORMATION SECURITY OF UKRAINE

The purpose of the article is to highlight state regulation in the field of cyberspace protection as a component of information security of Ukraine at the present stage of state building.
Methods. The methodological basis of the development was the dialectical approach, which involves consideration of the prerequisites for the formation of state regulation of ensuring cybersecurity as an objective reality, which is constantly evolving affected by technical, political, legal, security and other factors. In addition, in the course of the study historical and legal, system-structural, structural-functional methods, the method of ascending from abstract to specific were applied.
The results of the scientific development of the topic selected allows to state that the main legal basis for ensuring cybersecurity in Ukraine is the implementation of measures aimed at secure protection of cyberspace, provided that it is open, accessible to the participants of information exchange and stable. Accordingly, state administration of cyberspace security must meet the requirements of a democratic state system and the rule of law when the potential restriction of the right of a person to information is reduced to a minimum. At the level of administrative and legal regulation of cybersecurity processes, state measures in the field of cyberspace protection are not defined systematically, there is no clear list of them and administrative cooperation of cybersecurity entities is not regulated properly.
It has been established that Ukraine commits itself to the European Union to carry out a number of measures aimed at the development and protection of cybersphere within the framework of combating cybercrime, ensuring military-technical cooperation and crisis management, creating and protecting a system of information exchange on terrorism with the European Union, protecting computerized information systems and electronic data exchange system for economic cooperation, development of innovations and innovative technologies.
The conclusions of the study of topic selected allow to point out that the current legal bases of implementation of state policy in ensuring the protection of cyberspace and cybersecurity have major faults. In particular, it is the slowness in reforming the cybersecurity regulatory framework, the lack of regulation of aspects of the administrative interaction of subjects of the national cybersecurity system, the lack of clear legal regulation of main risks and threats to the national cyberspace. Proposals for optimizing the regulatory support of these aspects should form the basis for further scientific research on these issues. It is also substantiated that Ukraine needs to develop and implement measures aimed at fulfilment of provisions of the Association Agreement between Ukraine and the European Union regarding the development and protection of cyberspace.

Key words: Ukraine, cyberspace, cybersecurity, national cybersecurity system, information security, state administration, European Union.

JEL Classification: H56, K23, K24, L86, O38.

Pavlo YAKOVLEV,
Doctoral Candidate
of V. N. Karazin Kharkiv National University,
Candidate of Juridical Sciences
rexi2400@ukr.net
orcid.org/0000-0003-0172-5946

1. Introduction

One of the most significant achievements of scientific and technological progress for the humanity was the creation and expansion of the functional potential of information and communication technologies. Today, with the development of the Internet, entire spheres of manufacturing and non-manufacturing public relations in most countries of the world develop in cyberspace. The advantages of using this method of social communication are obvious, as it provides speed, economy, and maximum saturation of information of socio-economic, political and legal, cultural ties. At the same time, the accelerated growth of the cybernetic component of state-building processes creates the risks of its unlawful damage or unfair use.

According to experts, tens of thousands of crimes with the use information technologies, software, hardware and special technological equipment are committed in Ukraine annually (Nikulesko, 2019). Currently, these issues are compounded by the fact that no comprehensive nationwide cyber security management system has been developed in Ukraine. Thus, in the Cybersecurity strategy of Ukraine (hereinafter – the Cybersecurity strategy), which was put into effect by the Decree of the President of Ukraine "On the decision of the National Security and Defense Council of Ukraine of January 27, 2016 "On the Cybersecurity Strategy of Ukraine " of March 15, 2016 № 96/2016, it is stated that the insufficient effectiveness of the subjects of the security and defense sector of Ukraine in counteracting cyber threats of military, criminal, terrorist and other nature, as well as the inadequate level of coordination, interaction and information exchange between the subjects of cyber security actualize cybersecurity threats (President of Ukraine, 2016). Considering the above, the urgent task of modern legal science is a comprehensive development of organizational and legal aspects of the state regulation in the field of information security of Ukraine. In view of this, ***the purpose of the article*** is to highlight state regulation in the sphere of cyberspace protection as a component of information security of Ukraine at the present stage of state building.

2. Research methodology

Scientific analysis of state regulation of cyberspace protection has become possible due to the application of a specific system of methods of scientific knowledge. In particular, the methodological basis of the article was the dialectical-materialistic approach, which provides consideration of the prerequisites for the formation of state regulation of cybersecurity as an objective reality, which is constantly evolving affected by technical, political, legal, security and other factors. In addition, a number of methods of scientific knowledge were applied. In particular, the historical method was used to highlight the genesis of regulatory support for cybersecurity. The system-structural method has made it possible to determine the system of aspects of interdependence of increasing danger level of threats to the information environment of Ukraine and the legislative regulation of its protection. The application of the structural-functional method has given the possibility to reveal the role and importance of state-administrative measures for the protection of cyberspace in the aspect of ensuring the information security of the state. The classification method allowed to group primary management measures aimed at ensuring cybersecurity. The method of theoretical and legal forecasting was applied to substantiate the perspective tasks of legal science in the part of further development of the basics of ensuring cybersecurity of Ukraine.

3. An overview of the main sources of scientific information that were used in the course of writing the article

The general theoretical bases of the article were the ideas, conclusions and proposals of national scientists and experts, who considered the issue of securing the cyberspace of Ukraine from unlawful encroachments in their researches and analytical materials. In particular, these are D.V. Dubov, D.S. Nikulesko, V.F. Furashev, O.I. Yaremenko, and others). Also in the process of preparing the article the regulatory acts of the national legislation of Ukraine on cyber security, as well as the Association Agreement between Ukraine and the European Union were used.

4. Main body

4.1. The concept of cyberspace

The term "cyberspace" has been widely used in many fields of engineering and humanities for a long time. Its formation and introduction into the scientific discourse of jurisprudence is determined, as D.V. Dubov notes, rethinking of the priorities of national interests and self-understanding, considering that the protection of interests of state and nation in the information society is qualitatively different from the traditional understanding of security as a "state of safety" (Dubov, 2014). Such rethinking originates from the second half of 20th century, when information became not only a product that has market value at both global and national levels, but also received the status of a resource for state development. In fact, cyberspace is one of the main components of the information infrastructure of a state. As a complex phenomenon, cyberspace includes both a material component (means of computer technology, communication equipment, material components of telecommunication networks, writing algorithms and codes, etc.) and intangible – information, code reading processes, information transmission processes (Furashev, 2012).

In the legal field of Ukraine, the universal definition of the category "cyberspace" appeared only in 2017, when the Law of Ukraine "On the Fundamental Principles of Cybersecurity of Ukraine" of October 5, 2017 № 2163-VIII (Verkhovna Rada of Ukraine, 2017) was adopted. In art. 1 of the act, cyberspace is defined as an environment (virtual space) that enables communications and/or public relations, formed as a result of the functioning of compatible (connected) communication systems and the provision of electronic communications using the Internet and/or other global data networks. Experts point out that the main reason that pushed the legislator to define the term "cyberspace" at the legislative level was the complete unwillingness of Ukraine to repel cyberattacks and the lack of legal regulation of state administration of cybersecurity. For example, in 2016, Petya/Nyetya virus caused unprecedented damage to Ukraine: more than half of Ukrainian companies were affected by the virus, they lost large amounts of data and financial reporting over several reporting periods and had to recover the information for a long time (Krasnyi et al., 2018). Legal regulation of the cyberspace category has become an important step towards structuring a systematic state policy aimed at ensuring cybernetic and information security of Ukraine. In terms of protecting cyberspace from unlawful encroachment, the criminalization of cyberspace crimes is also important. The law provides the concept of "cybercrime", which is referred to as a socially dangerous act for which criminal liability is provided.

4.2. Legal regulation of the components of state regulation policy in the sphere of cyberspace protection

Regarding the issue of state regulation in the field of cyberspace protection, two important features should be emphasized. The first feature is that, according to the content of Article 7 of the above mentioned Law of Ukraine "On Basic Principles of Cybersecurity of Ukraine", the key principle of ensuring cybersecurity in Ukraine is the realization of measures aimed at secure protection of cyberspace subject to ensuring its openness, accessibility and stability. Accordingly, the state administration of cyberspace security must meet the requirements of a democratic state system and the rule of law when the potential restriction of the right of a person to information is reduced to a minimum.

O.I. Yaremenko explains this by the fact that cyberspace is a kind of "conductor" of information processes and is a dominant part of the information sphere of the modern society (Yaremenko, 2017). The second feature is that at the level of administrative and legal regulation of cybersecurity processes, state regulation measures in the field of cyberspace protection are not defined systematically and there is no clear list of them. For example, analyzing the provisions of the Cybersecurity strategy and the Law of Ukraine "On the Fundamental Principles of Cybersecurity of Ukraine" systematically, the main measures of the state regulation policy in the field of cyberspace protection are:

– ensuring the formation and realization of the state policy in the field of cybersecurity, protection of national interests of Ukraine in cyberspace and combating cybercrime by the Cabinet of Ministers of Ukraine;

– organization and maintenance of the national cybersecurity system;

– formation of the system of information security audit on the objects of critical infrastructure;

– taking measures by duty-holders to prevent the use of cyberspace for military, intelligence, subversive, terrorist and other illegal and criminal purposes;

– development of measures for protection of cyberspace from real and potentially aggressive actions, preventing the use of cyberspace for terrorist, military and other unlawful purposes;

– ensuring interaction of the main subjects of the national cybersecurity system (State Service of Special Communications and Information Protection of Ukraine, National Police of Ukraine, Security Service of Ukraine, Ministry of Defense of Ukraine and General Staff of the Armed Forces of Ukraine, intelligence agencies, National Bank of Ukraine);

– guaranteeing the safety and sustainable functioning of electronic communications and state electronic information resources, etc.

It should be noted that the primary prerequisite for state regulatory policy in the field of cyberspace protection is the creation of a regulatory and term base in the field of cybersecurity, as well as the development of appropriate regulatory support for the specified issue. The national practice of rulemaking on this issue is just shaping and undergoing a stage of its formation. The imperative for the formation of an effective legal field for the realization of state regulation in the field of cyberspace protection should be a combination of political, legal, technical, energy, intellectual, financial aspects of the development and implementation of legal structures for ensuring cyberspace security.

4.3. Issues of effective functioning of the system of state regulation in the sphere of cyberspace protection at the present stage of state formation

The Cybersecurity strategy includes a list of factors that are major problems for the national cybersecurity policy. In particular, it is an inadequacy of the electronic communications infrastructure of the state and the level of its development and security with modern requirements; insufficient level of protection of critical infrastructure, state electronic information resources and information, the requirement for protection of which is established by law, against cyber threats; unsystematic cyber defense measures for critical infrastructure; insufficient development of the organizational and technical infrastructure providing cybersecurity and cyberprotection for the state electronic information resources; insufficient effectiveness of subjects of the security and defense sector of Ukraine in counteracting cyber threats of military, criminal, terrorist and other nature; insufficient level of coordination, interaction and information exchange between cybersecurity entities. We consider it necessary to amend the Cybersecurity strategy with provisions on the regulation of the main forms of administrative and managerial interaction of subjects of the national cybersecurity system.

In addition, we also consider it appropriate to focus on the slowness of changes to the core documents that make up the legal field of cybersecurity. For instance, since 2016 the Cybersecurity strategy has not been amended, despite the increasing number and level of danger of cyberspace threats in Ukraine. It was only at the end of 2019 when the need to amend the Cybersecurity strategy was oficially announced due to the need to counteract modern cyber weapons and the development of the National Cyber Security Coordination Center within the National Security and Defense Council ("The Day", 2019). The situation is similar with the Law of Ukraine "On the Fundamental Principles of Cybersecurity of Ukraine", which has been amended only once within a few years. This situation needs revision and mobilization of lawmaker's efforts with the participation of international partners and subject to the positive experience of the countries of the world in the implementation of cyberspace protection policy.

4.4. Priority areas for reforming state regulation in the field of cyberspace protection in accordance with the Association Agreement

In 2014, a historic document was signed between Ukraine and the European Union – the Association Agreement between Ukraine, of the one part, and the European Union, the European Atomic Energy Community and their Member States of the other part (hereinafter – the Association Agreement). The document identified the strategic foundations for reforming all spheres of public life in Ukraine in accordance with the standards and rules of the European Union (Verkhovna Rada of Ukraine, 2014).

The Association Agreement provides a system of conceptual provisions related to cyberspace protection activities. In particular, Ukraine takes an obligation of establishing a system of interaction with the European Union in the direction of combating cybercrime (art. 26), ensuring military-technical cooperation and crisis management (art. 10), creating and protecting a system of information exchange on terrorism with the European Union (art. 23), ensuring protection of computerized information systems and electronic data exchange system on various forms of economic cooperation (art. 135). In addition, the Association Agreement contains a significant number of provisions on the development of innovations and innovative economic relations. It is impossible without the cyberspace. Accordingly, at the national level, Ukraine needs to develop and implement measures aimed at realization of the Association Agreement provisions regarding the development and protection of cyberspace. Such multi-stage and systematic work provides the involvement of a wide range of specialists for the implementation of the formulated tasks with a focus on ensuring information security of Ukraine.

5. Conclusions

State regulation of cyberspace protection processes in Ukraine is an integral part of ensuring information security of the state. At the beginning of 2020, the basic legal framework for the implementation of state policy towards ensuring the protection of cyberspace and cybersecurity were formed at the level of the legal system of Ukraine. However, the administrative and legal regulation of the state regulation of protection of cybersecurity is characterized by certain gaps. In particular, it is the slowness of reforming the regulatory framework for cybersecurity, the lack of regulation of aspects of administrative interaction between the subjects of the national cybersecurity system, the lack of clear regulation of the main risks and threats to the national cyberspace of Ukraine. These concepts should form the basis of prospective scientific research on identified issues in order to make sound proposals for improving the national cybersecurity legislation.

References:

1. Nikulesko, D.S. (2019). Kiberbezpeka: vrazlyvi momenty [Cybersecurity: vulnerable moments]. *Yurydychna hazeta online*. Retrieved from: https://yur-gazeta.com/publications/practice/inshe/kiberbezpeka-vrazlivi-momenti.html (access date: 14.04.2020) [in Ukrainian].

2. President of Ukraine (2016). Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 27 sichnia 2016 roku "Pro Stratehiiu kiberbezpeky Ukrainy": Ukaz Prezydenta Ukrainy vid 15 bereznia 2016 r. № 96/2016 [On the decision of the National Security and Defense Council of Ukraine of January 27, 2016 "On the Cyber Security Strategy of Ukraine": Decree of the President of Ukraine of March 15, 2016 № 96/2016]. *Ofitsiinyi visnyk Ukrainy*, no. 23, pp. 69, art. 899 [in Ukrainian].

3. Dubov, D.V. (2014). Kiberprostir yak novyi vymir heopolitychnoho supernytstva: monohrafiia [Cyberspace as a new dimension of geopolitical rivalry: monograph]. Kyiv: NISD, 328 p. [in Ukrainian].

4. Furashev, V.M. (2012). Kiberprostir ta informatsiinyi prostir, kiberbezpeka ta informatsiina bezpeka: sutnist, vyznachennia, vidminnosti [Cyberspace and information space, cybersecurity and information security: essence, definitions, differences]. *Informatsiia i pravo*, no. 295), pp. 162–169 [in Ukrainian].

5. Verkhovna Rada of Ukraine (2017). Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy: Zakon Ukrainy vid 5 zhovtnia 2017 r. № 2163-VIII [On the basic principles of cybersecurity of Ukraine: Law of Ukraine of October 5, 2017 № 2163-VIII]. *Vidomosti Verkhovnoi Rady Ukrainy*, no. 45, pp. 42, art. 403 [in Ukrainian].

6. Krasnyi, A., Zymaryn, A., Miahka, I., Polietaieva, M. (2018). Bezpeka v merezhi: yak Ukraina rehuliuvatyme kiberprostir. Ta yak novyi zakon "Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy" vplyne na biznes [Network security: how Ukraine will regulate cyberspace. And how the new law "On the basic principles of cybersecurity in Ukraine" will affect business]. *mind.ua*. Retrieved from: https://mind.ua/openmind/20184620-bezpeka-v-merezhi-yak-ukrayina-regulyuvatime-kiberprostir (access date: 10.04.2020) [in Ukrainian].

7. Yaremenko, O.I. (2017). Kiberprostir yak skladova informatsiinoi sfery: problema pravovoi instytualizatsii [Cyberspace as a component of the information sphere: the problem of legal institutionalization]. *Kiberbezpeka v Ukraini: pravovi ta orhanizatsiini pytannia: materialy Vseukrainskoi naukovo-praktychnoi konferentsii* (Odesa, November 17, 2017). Odesa: Odessa State University of Internal Affairs, pp. 194–195 [in Ukrainian].

8. "The Day" (2019). RNBO pratsiuie nad onovlenoiu Stratehiieiu kiberbezpeky [The National Security and Defense Council is working on an updated Cyber Security Strategy]. *day.kyiv.ua*. Retrieved from: https://day.kyiv.ua/uk/news/141219-rnbo-pracyuye-nad-onovlenoyu-strategiyeyu-kiberbezpeky (access date: 10.04.2020) [in Ukrainian].

9. Verkhovna Rada of Ukraine (2014). Pro ratyfikatsiiu Uhody pro asotsiatsiiu mizh Ukrainoiu, z odniiei storony, ta Yevropeiskym Soiuzom, Yevropeiskym spivtovarystvom z atomnoi enerhii i yikhnimy derzhavamy-chlenamy, z inshoi storony: Zakon Ukrainy vid 16 veresnia 2014 r. № 1678-VII [On ratification of the Association Agreement between Ukraine, of the one part, and the European Union, the European Atomic Energy Community and their Member States, of the other part: Law of Ukraine of 16 September 2014 № 1678-VII]. *Vidomosti Verkhovnoi Rady Ukrainy*, no. 40, pp. 2843, art. 2021 [in Ukrainian].

ДЕРЖАВНЕ РЕГУЛЮВАННЯ У СФЕРІ ЗАХИСТУ КІБЕРПРОСТОРУ ЯК СКЛАДНИК ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

Павло ЯКОВЛЄВ,
докторант
Харківського національного університету імені В. Н. Каразіна,
кандидат юридичних наук
rexi2400@ukr.net
orcid.org/0000-0003-0172-5946

Мета статті полягає у висвітленні державного регулювання у сфері захисту кіберпростору як складового компоненту інформаційної безпеки України на сучасному етапі державного будівництва.
Методи. Методологічною основою дослідження став діалектичний підхід, що передбачає розгляд передумов формування державного регулювання забезпечення кібербезпеки як об'єктивної реальності, яка постійно еволюціонує під впливом технічних, політико-правових, безпекових та інших чинників. Крім цього, у процесі дослідження було застосовано історико-правовий, системно-структурний, структурно-функціональний методи, а також метод сходження від абстрактного до конкретного.
Результати наукового розроблення представленої теми дають підстави констатувати, що основною юридичною засадою забезпечення кібербезпеки в Україні є реалізація заходів, спрямованих на надійний захист кіберпростору за умови забезпечення його відкритості, доступності для учасників інформаційного обміну та стабільності. Відповідно, державне адміністрування безпеки кіберпростору має відповідати вимогам демократичного державного устрою та принципу верховенства права, коли звуження потенційної можливості реалізації права особу на інформацію зведене до мінімуму. На рівні адміністративно-правового регулювання процесів забезпечення кібербезпеки заходи державного регулювання у сфері захисту кіберпростору визначено несистемно, відсутній чіткий їх перелік, а також не досконало регламентовано адміністративну співпрацю суб'єктів забезпечення безпеки кіберсередовища.
Встановлено, що Україна зобов'язується перед Європейським Союзом виконати низку заходів, спрямованих на розвиток і захист кіберсфери в межах протидії кіберзлочинності, забезпечення військово-технічного співробітництва та антикризового управління, створення й захист системи обміну інформацією про тероризм із Європейським Союзом, захист комп'ютеризованих інформаційних систем та електронної системи обміну даними з питань господарської взаємодії, розвиток інновацій та інноваційних технологій.
Висновки дослідження дають підстави стверджувати, що чинні базові правові засади реалізації державної політики в напрямі забезпечення захисту кіберпростору й кібербезпеки мають істотні недоліки. Зокрема, це мінливість реформування нормативної бази забезпечення кібербезпеки, недостатня урегульованість аспектів адміністративної взаємодії суб'єктів національної системи кібербезпеки, відсутність чіткої нормативної регламентації основних ризиків і загроз національному кіберпростору. Вироблення пропозицій щодо оптимізації нормативного забезпечення зазначених аспектів має лягти в основу подальших наукових досліджень цієї проблеми. Обґрунтовано також, що Україна потребує розроблення й упровадження заходів, які спрямовані на втілення положень Угоди про асоціацію між Україною та Європейським Союзом у частині розвитку й захисту кіберпростору.

Ключові слова: Україна, кіберпростір, кібербезпека, національна система кібербезпеки, інформаційна безпека, державне управління, Європейський Союз.