UDC 342.95 (477)
DOI https://doi.org/10.32849/2663-5313/2022.5.08

Oksana Zubko,
External Postgraduate Student, Scientific Institute of Public Law, 2a, H. Kirpy street, Kyiv, Ukraine, postal code 03035, Zubko_Oksana@ukr.net
***ORCID:** 0000-0003-1381-621X*

Zubko, Oksana (2022). Modern concept of administrative and legal protection of cyberspace in Ukraine. *Entrepreneurship, Economy and Law*, 5, 51–55, doi: https://doi.org/10.32849/2663-5313/2022.5.08

MODERN CONCEPT OF ADMINISTRATIVE AND LEGAL PROTECTION OF CYBERSPACE IN UKRAINE

Abstract. ***Purpose.*** The purpose of the article is to cover the modern concept of administrative and legal protection of cyberspace in Ukraine, relying on the systematic analysis of the positions of scientists, reference materials and provisions of current legislation. ***Results.*** It is found that information legislation should regulate the contradiction between the needs of the individual, society and the State in expanding the free exchange of information and certain restrictions on its dissemination. Today, Ukraine has hundreds of laws and other legal regulations focused on the development of information processes, the protection of the national information space, the acceleration of integrated processes in the world information space. It is underlined that the main purpose of law enforcement bodies' performance is to combat dealers of harmful digital services and related tools; thus, it is advisable to establish a register of such suppliers with a questionable reputation, including IT companies, other business entities, thereby ensuring control over the situation in the digital economy. ***Conclusions.*** The article covers the concept of administrative and legal protection of cyberspace in Ukraine as a defining, strategically established, modern model of the national idea, the system of legal measures and processes of effective protection of cyberspace, which further develops general policy on information security and accelerates the integration processes of using the opportunities of cyberspace by Ukrainian society. The fundamentals underlying the modern concept of administrative and legal protection of cyberspace in Ukraine are defined as follows: 1) The elaboration of effective information legislation and national strategic instruments on the use of cyberspace should be a priority; 2) The cybersecurity actors' practical activities should be improved; 3) New programs, measures and tools to protect information and counteract cyberattacks should be created; 4) High-quality digital services should be ensured; 5) The focus should be on an intensive and secure entry of Ukrainian society into the world cyberspace.

Key words: administrative protection, administrative means, administrative and legal framework, State information policy, information security, information, cyberspace, sovereignty.

1. Introduction

The rapid development of information technology is gradually transforming the world. Every day we are faced with the need to use information technologies - from social networks, posting information about our personal data on the Internet to using ATMs, bank accounts, etc. This raises the question of whether the problem is addressed by national legislation and how to protect one's own information from cybercriminals. Of particular concern is the possibility of the development, use and proliferation of information weapons, the resulting threats of information wars and cyberterrorism, whose negative effects are comparable to those of weapons of mass destruction. The illegal creation, collection, receipt, storage, use, dissemination, security, protection of information, illegal financial transactions, theft and fraud on the Internet continue to spread. Cybercrime has become a transnational problem and has the potential to significantly harm the interests of the individual, society and the State in general [6, p. 180–186].

In order to prevent cybercrime and generally protect the information sovereignty of the State, a new concept of administrative and legal protection of cyberspace in Ukraine should be developed.

Current issues of cyberspace in the context of administrative law in Ukraine were studied in their scientific works by V. Bukhariev, V. Hapotii, O. Herasymova, S. Horova, V. Horovyi, S. Demchenko, O. Dovhan, D. Dubov, H. Duhinets, Yu. Lisovska, V. Markov, V. Nabrusko, O. Oliynyk, A. Pysmenytskyi, V. Polevyi, O. Radutnyi,

P. Rohov, O. Skrypniuk, O. Solodka, V. Suprun, V. Torianyk, A. Cherep, and others.

However, given the duration of hybrid warfare, the intensification of cyber-attacks of State portals and other information infringements in the public sector, the relevance of scientific research in the field of cyberspace acquires new features and characteristics.

The purpose of the article is to reveal the modern concept of administrative and legal protection of cyberspace in Ukraine, relying on the systematic analysis of the positions of scientists, reference materials and provisions of current legislation.

2. Cyberspace as a subject matter of administrative and legal protection

First, the concept of cyberspace as a subject matter of legal protection should be defined. The analysis of the related concept of "cybersecurity" allows defining the object of administrative and legal protection (according to V. Bukhariev) cybersecurity is a certain legal institution, protected within the scope of the rules of administrative law and is carried out by individual State bodies on the basis of imperative and hierarchy. Moreover, the scientist elucidates features of cybersecurity as an object of administrative and legal protection, such as: a) A clear definition of the content of administrative and legal protection of cybersecurity is absent; b) Administrative and legal protection of cybersecurity, although it is a single legal institution, is enshrined in provisions of different legal regulations on the activities of the relevant State authorities; c) It is enforced not only in legal relations arising in the sphere of administrative offenses. The concept has a broader scope of application, including not only deterrence of violations but also prevention; d) The basic principles of cybersecurity have only recently been incorporated into the relevant legal regulation, the Law of Ukraine "On the Basic Principles of Cyber Security of Ukraine"); e) A special conceptual apparatus (Bukhariev, 2018, p. 182).

In our view, cyberspace is a valuable subject matter of administrative and legal protection and is an information space derived from the use of computer technologies and systems, the functioning of which ensures interactive communication in society.

Next, from the current perspective of scientists on the concept of protection of cyberspace, the dominant problem is the formation of effective administrative and legal protection of cyberspace in Ukraine is the need for its safe operation at the administrative, programmatic and procedural levels (Azarova, Tkachuk, Nikiforova, Shyian, Khoshaba, 2019).

Accordingly, the development of the concept of administrative and legal protection of cyberspace in Ukraine should focus on the effective implementation of plans and measures of the concept of protection at the administrative, programmatic and procedural levels of the implementation of legal relations.

The State, with its arsenal of a wide range of means of influencing public relations in the information sphere, should naturally be the main actor of information security policy. If information security is considered as certain conditions, parameters and characteristics of information processes taking place in the information sphere of the State, then the State has the possibility, through legal regulation, to define uniform, universally binding standards of information processes that meet the security requirements of the forces exercising political power in that State. This is the basis of public policy on information security, embodied in the relevant legal regulations. The level of information security depends not only on the goals of the relevant public policy, but also its content (Foros, 2018, pp. 180–186).

Modern challenges and threats to cyber-driven critical infrastructure as a strategic object of the State require guarantees and effective improvement of legislative, institutional and other instruments for the implementation of public policy on information. In addition, the critical infrastructure of Ukraine is based on the security and defence sector, consisting of four mutually agreed components: security forces; defence forces; defence and industrial complex; citizens and public associations. To this end, it should be emphasised that the Ukrainian Security Service has special tasks in the institutional mechanism for ensuring the critical information infrastructure of Ukraine. This relates primarily to counter-intelligence protection of State sovereignty, constitutional order and territorial integrity, defence, scientific and technological capabilities. In addition, a national system of confidential communication, making of public policy on cyber protection, namely, cryptographic and technical protection of information, telecommunications, use of Ukraine's radio frequency resource, special purpose mail, government field communication, etc., should be established at an appropriate level (Lisovska, 2019, pp. 162–171).

3. Administrative and legal protection of cyberspace in Ukraine

Since Ukraine faces hybrid warfare, it has been possible at the state level to synchronise measures for the development of armament and military equipment, with measures for the reform and development of the defence and industrial complex. These measures are aimed at restructuring, reorganisation and corporatisation of enterprises of the defence

and industrial complex and improvement of the management system of such complex; introduction of the mechanism of strategic management of the defence and industrial complex; provision of financial control of enterprises; integration of science and production; improvement of the system of standardisation, quality unification and management (Lisovska, 2019, pp. 162–171).

Information legislation should regulate the contradiction between the needs of the individual, society and the State in expanding the free exchange of information and certain restrictions on its dissemination. Today, Ukraine has hundreds of laws and other legal regulations focused on the development of information processes, the protection of the national information space, the acceleration of integrated processes in the world information space. The most significant laws are: "On the protection of personal data", "On the protection of information in information and telecommunication systems", "On information", "On the printed media (press) in Ukraine", "On the Protection of Industrial Design Rights", "On Copyright and Related Rights", "On State Support for Mass Media and Social Protection of Journalists", "On the Procedure for Covering the Activities of State and Local Authorities in the Ukrainian Mass Media", "On the National Informatisation Programme", and others (Foros, 2018, pp. 180–186).

Cyber security and cyberspace of Ukraine for a long time remained out of sight by domestic researchers, and then civil servants. For more than 20 years, the young Ukrainian State has not spent its efforts on forming not only an effective and reliable military force, but also information security. The leadership of the State made no efforts to strengthen the defence capability of the country, and rather weakened it by lack of progress in the fight against corruption and the domination of the Russian media and secret services. As a result, in the spring of 2014, after a long confrontation between Ukrainian citizens and the Yanukovych regime, Russia resorted to a special operation to annex Crimea and contribute to the war in the Donbas. An important role in this special operation was played by information factors and cyber-attacks of Russian hackers in order to paralyse government structures and influence the formation of public opinion in Ukraine through Russian-controlled media. Long and massive cyberattacks caused significant material and reputational losses for Ukrainian public structures, banking system, industrial facilities and private business. At the same time, Ukraine began to understand the seriousness of cyberspace security as a component of national security and this contributed to the creation of the cyber police, the State strategy for cybersecurity, the adoption of a number of legal regulations on cybersecurity, strengthening of the State protection in the national cyberspace security (Katerynchuk, 2018).

All cybersecurity actors have a range of both specific and general powers. Common features of cybersecurity actors are: first, they use coercion in their activities in order to exercise their statutory functions; second, cybersecurity actors are in a systemic relationship with other actors in an administrative legal relationship based on hierarchy; third, the activities of cybersecurity actors are aimed not only at suppressing cybersecurity offences, but also at ensuring that such violations are not possible, through monitoring activities (Bukhariev, 2018, p. 185).

The main purpose of law enforcement bodies' performance is to combat dealers of harmful digital services and related tools, it is advisable to establish a register of such suppliers with a questionable reputation, including IT companies, other business entities, thereby ensuring control over the situation in the digital economy. According to I. Revak, the main areas of strengthening cyberspace are continuous modernisation of information and telecommunication technologies; strengthening of communication security, namely improvement, development and launch of the latest data protection programs; the legal regulatory mechanism and coordination of actions to create separate elements of the cybersecurity system; introduction and use of blockchain technology. The activities of law enforcement bodies to prevent (minimise, neutralise) real and potential threats should include: long-term and sustainable effective communicative cooperation and close communication between the various units of the internal affairs bodies and other State bodies; activities of different departments and subordinate law enforcement bodies in the field of information technologies for collective functioning and coordination of purposes; more intensive use (application) of electronic evidence, information and telecommunication technologies and registers; development of criteria for regulating secret data on effective circumstances, establishing software access of various internal affairs bodies, which effectively counteract crimes in digital computer technology and cyberspace (Revak, 2021, pp. 164–169).

4. Conclusions

To sum up, the concept of administrative and legal protection of cyberspace in Ukraine as a defining, strategically established, modern model of the national idea, the system of legal measures and processes of effective protection of cyberspace, which further develops general

policy on information security and accelerates the integration processes of using the opportunities of cyberspace by Ukrainian society.

It is possible to formulate the fundamentals underlying the modern concept of administrative and legal protection of cyberspace in Ukraine as follows:

1) The development of effective information legislation and national strategic instruments on the use of cyberspace should be a priority;

2) The cybersecurity actors' practical activities should be improved;

3) New programs, measures and tools to protect information and counteract cyberattacks should be created;

4) High-quality digital services should be ensured;

5) The focus should be on an intensive and secure entry of Ukrainian society into the world cyberspace.

References:

Azarova, A.O., Tkachuk, L.M., Nikiforova, L.O., Shyian, A.A., Khoshaba, O.M. (2019). Publichne upravlinnia ta administruvannia v konteksti zakhystu yoho informatsiinoho prostoru [Public administration and administration in the context of protecting its information space]. *«Visnyk ZhDTU»: Ekonomika, upravlinnia ta administruvannia - "Bulletin of ZhSTU": Economics, Management and Administration, 2(88),* 149–155 (in Ukrainian).

Bukhariev, V.V. (2018). Administratyvno-pravovi zasady zabezpechennia kiberbezpeky Ukrainy [Administrative and legal principles of cybersecurity in Ukraine]. *Candidate's thesis.* Sumy: Un-t suchasnykh znan (in Ukrainian).

Foros, H.V. (2018). Pravovi osnovy zakhystu informatsii v kiberprostori [Legal bases of information protection in cyberspace]. *Pravova derzhava - Constitutional state, 30,* 181-186 (in Ukrainian).

Katerynchuk, P. (2018). Zakhyst kiberprostoru yak skladova informatsiinoi bezpeky Ukrainy [Cyberspace protection as a component of Ukraine's information security]. *Mediaforum - Media forum, 6,* 57-70 (in Ukrainian).

Lisovska, Yu.P. (2019). Administratyvno-pravovyi zakhyst krytychnoi informatsiinoi infrastruktury v suchasnomu kiberprostori [Administrative and legal protection of critical information infrastructure in modern cyberspace]. *Informatsiia i pravo - Information and law, 83,* 161-171 (in Ukrainian).

Revak, I.O. (2021). Osoblyvosti formuvannia bezpechnoho kiberprostoru v umovakh rozvytku tsyfrovoi ekonomiky [Features of the formation of secure cyberspace in the digital economy]. *Innovatsiina ekonomika - Innovative economy, 3-4,* 164-169 (in Ukrainian).

Оксана Зубко,
здобувач наукового ступеня доктора юридичних наук, Науково-дослідний інститут публічного права, вулиця Г. Кірпи, 2А, Київ, Україна, індекс 03035, Zubko_Oksana@ukr.net
***ORCID:** 0000-0003-1381-621X*

НОВІТНЯ КОНЦЕПЦІЯ АДМІНІСТРАТИВНО-ПРАВОВОГО ЗАХИСТУ КІБЕРПРОСТОРУ В УКРАЇНІ

Анотація. ***Мета.*** Мета статті полягає в тому, щоб на основі системного аналізу позицій вчених, довідникових матеріалів та норм чинного законодавства розкрити новітню концепцію адміністративно-правового захисту кіберпростору в Україні. ***Результати.*** З'ясовано, шо інформаційне законодавство має регулювати суперечність між потребами особи, суспільства та держави у розширенні вільного обміну інформацією та окремими обмеженнями на її поширення. Сьогодні Україна має сотні законодавчих та інших нормативно-правових актів, що зорієнтовані на розвиток інформаційних процесів, захист національного інформаційного простору, прискорення інтегральних процесів у світовому інформаційному просторі. Наголошено, що основною метою діяльності правоохоронних органів є боротьба з дилерами шкідливих цифрових послуг та відповідних інструментів, доцільним є створення реєстру таких постачальників, які мають сумнівну репутацію, в тому числі ІТ-компаній, інших суб'єктів господарювання, тим самим забезпечивши контроль над ситуацією у сфері цифрової економіки. ***Висновки.*** У статті розкрито концепцію адміністративно-правового захисту кіберпростору в Україні як визначальну, стратегічно-закріплену, сучасну модель національної ідеї, систему правових заходів та процесів ефективного захисту кіберпростору, що забезпечує та в подальшому розвиває загальну політику інформаційної безпеки та прискорює інтеграційні процеси використання можливостей кіберпростору українським суспільством. Визначено засади формування новітньої концепції адміністративно-правового захисту кіберпростору в Україні: 1) першочерговим має стати формування ефективного інформаційного законодавства та національ-

них стратегічних документів щодо використання можливостей кіберпростору; 2) удосконалення практичної діяльності суб'єктів забезпечення кібербезпеки; 3) створення нових програм, заходів та інструментів захисту інформації та протидії кібератакам; 4) забезпечення високої якості надання цифрових послуг; 5) зосередження на інтенсивному та безпечному входженні українського суспільства у світовий кіберпростір.

Ключові слова: адміністративний захист, адміністративні засоби, адміністративно-правові засади, державна інформаційна політика, інформаційна безпека, інформація, кіберпростір, суверенітет.

The article was submitted 18.07.2022
The article was revised 08.08.2022
The article was accepted 29.08.2022