DOI 10.52363/2414-5866-2024-2-50
УДК 355/359.07; 342.08

Filonov M., *Postgraduate student of the Classic Private University, Zaporizhzhia, ORCID: 0009-0001-3958-5822*

Філонов М.В., *аспірант Класичного приватного університету, м. Запоріжжя*

STATUS OF IMPLEMENTATION OF PUBLIC INFORMATION SECURITY MANAGEMENT IN UKRAINE AT THE REGIONAL LEVEL IN THE CONTEXT OF ENSURING PUBLIC SECURITY

СТАН РЕАЛІЗАЦІЇ ПУБЛІЧНОГО УПРАВЛІННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА РЕГІОНАЛЬНОМУ РІВНІ В КОНТЕКСТІ ЗАБЕЗПЕЧЕННЯ ПУБЛІЧНОЇ БЕЗПЕКИ

Проаналізовано стан реалізації публічного управління інформаційної безпеки України на регіональному рівні у період 2014–2024 рр. Досліджено роль соціально-політичних та інформаційних технологій у забезпеченні розвитку системи публічного управління інформаційною безпекою в регіоні. Обґрунтовано необхідність оновлення Стратегії інформаційної безпеки України в напрямку включення до цієї стратегії положень щодо заходів публічного управління у сфері забезпечення інформаційної безпеки на регіональному рівні.

Ключові слова: *публічне управління, сфера інформаційної безпеки, стратегія інформаційної безпеки, органи державної влади, регіони.*

The state of implementation of public information security management in Ukraine at the regional level in the period 2014–2024 is analyzed. The role of socio-political and information technologies in ensuring the development of the public information security management system in the region is investigated. The need to update the Information Security Strategy of Ukraine in order to include provisions on public management measures in the field of ensuring information security at the regional level is substantiated.

Keywords: *public administration, information security sphere, information security strategy, state authorities, regions.*

Formulation of the problem. State management of information security is one of the important functions of the state. Its essence lies in ensuring a coordinated national strategy at the state, regional and local levels with a mutually agreed distribution of responsibilities for regulatory, informational, moral and psychological, documentation and resource support. The state must constantly compare threats and dangers with the available resources for managing them. A comprehensive detailing of the rights, duties, powers and responsibilities of all

ISSN 2414-5858 (Print)
ISSN 2414-5866 (Online)

components of the national security management system is required.

Unfortunately, it should be noted that as a result of improper legal regulation in the national information space of Ukraine, a number of negative phenomena are observed that create real and potential threats to the information security of a person and a citizen, society at the regional level.

In the 2000s, the information and psychological pressure on the population of Ukraine by the mass media of the Russian Federation was carried out on the territory of the Autonomous Republic of Crimea and the south-eastern regions of Ukraine, information expansion into the national information space of Ukraine was observed, strategic objects of the Ukrainian telecommunications infrastructure were seized. All this created fertile ground for the formation of a significant layer of Ukrainians who are pro-Russian.

According to the public organization "Institute of Mass Information", for the period from March 1 to June 10, 2014 (i.e. after the beginning of the external aggression of the Russian Federation) 368 facts of violations of freedom of speech were recorded in Ukraine, of which almost 80% were related to the actions of terrorists, Russian aggression, and occurred in the East and in Crimea [4]. There were numerous obstacles to the professional activities of journalists. All this is happening against the backdrop of a massive and aggressive information offensive by Russian propaganda, which, contrary to European standards in the field of mass media, tried to incite interethnic hostility and separatist sentiments in Ukraine, encroached on the state sovereignty and territorial integrity of Ukraine. Under these conditions, the issue of improving the domestic information security system in general and the mechanisms of state response to modern challenges and threats to information security in particular becomes relevant.

Analysis of recent research and publications. Publications of such scientists as Ya. Bazylyuk, A. Hrytsenko, M. Denysenko, S. Dombrovska, A. Karsrud, R. Klyut, P. Kolisnichenko, S. Lekar, V. Orlyk, G. Pocheptsov, and others are devoted to consideration of the peculiarities of the formation and implementation of state policy in the sphere of information security [1; 3].

Setting objectives. The purpose of the article is to analyze the state of implementation of public information security management in Ukraine at the regional level.

Presenting main material. When determining the place of information security in the system of state activity in the performance of its functions, it should be borne in mind that at the present stage there is a need to consider in a complex the subject and content of state activity and the means and methods that ensure it, that is, to study state policy. State policy determines the content of state activity, methods of its organization. It is policy that provides for the harmonization of the interests of the state with the interests of other states, social groups and individuals, and most importantly - the definition of the specific content and forms of state activity in a particular area.

At the same time, policy itself is a supra-legal category and hence is regulated by legal norms only in its external, formalized expression. But the specific content of state policy is the will of the state, aimed at achieving a specific goal. This will of the state is enshrined in legal norms, implemented with their help in the process of activity of state bodies and institutions. Thus, from a legal point of view, there is a certain mechanism for the formation and implementation of state policy, in the field of information security - this is the organizational and legal mechanism of information security.

The organizational and legal mechanism of information security is an ordered set of state institutions involved in the process of forming and implementing information security policy, the internal and external roles and relations of which are regulated by a system of legal norms and principles. This organizational and legal mechanism, in accordance with the specified directions of implementing information security policy, consists of three interrelated elements.

First, it is a set of state institutions involved in the process of forming and implementing information security policy, that is, the institutional mechanism of information security.

Second, it is a set of roles and relations, which includes legal relations that arise when implementing information security policy and specific roles, forms and methods of activity of subjects implementing information security policy.

Third, it is a hierarchical set of legal norms and principles that regulate the content and process of implementing information security policy, that is, the legal mechanism of information security. The last two elements constitute the legal mechanism of information security.

The set of public authorities and civil society institutions involved in the process of forming and implementing information security policy constitutes the institutional mechanism of information security. The hierarchical set of legal norms and principles that regulates the content and process of implementing information security policy, as well as the set of roles and relationships that includes legal relations that arise when implementing information security policy and specific roles, forms and methods of activity of subjects implementing information security policy constitute the legal mechanism of information security. The effectiveness of protecting the information security of the state as a whole is ensured by the effectiveness of each component of its mechanism.

The subjects of ensuring information security of Ukraine should be considered a system of state and non-state institutions, as well as citizens of Ukraine united by a common goal of protecting national interests in the information sphere. Thus, the circle of subjects of ensuring information security of Ukraine represents a multi-level system that has a common goal - ensuring information security of Ukraine, but different powers, capabilities, means, etc. These entities include: 1) the state, which carries out its functions through the relevant state authorities by creating a system for ensuring information security; 2) citizens, public

or other organizations and associations that have the authority to ensure information security in accordance with the legislation of Ukraine.

The system of entities to ensure information security should operate regardless of the domestic political situation in Ukraine and the state of its individual elements. The systemic, integrating factor should be the common goal for the activities of the entities indicated in the diagram - ensuring national information sovereignty. So, for further awareness of the problem of identifying signs of threats to national security in the information sphere, a list of those entities that are involved in the processes of identifying, assessing information threats and organizing countermeasures can be distinguished. In particular, this list includes the following entities:

1. The President of Ukraine, who heads the National Security and Defense Council (NSDC) of Ukraine. The following entities also report to the President of Ukraine: The National Institute for Strategic Studies. The NSDC of Ukraine's apparatus coordinates the activities of the Interdepartmental Commission on Information Policy and Information Security under the NSDC of Ukraine and the specified research institutions of the strategic level.

2. The Cabinet of Ministers of Ukraine. The Secretariat of the Cabinet of Ministers of Ukraine includes the Department of Strategy for the Development of Information Resources and Technologies.

In addition, the Cabinet of Ministers of Ukraine coordinates the activities of:

• State Department of Intellectual Property of the Ministry of Education and Science of Ukraine;

• State Administration of Communications of the Ministry of Transport and Communications of Ukraine;

• Department of the State Service for Combating Economic Crime of the Ministry of Internal Affairs of Ukraine. This department includes the Department for Combating Offenses in the Field of Intellectual Property and High Technologies;

• diplomatic missions, consular institutions and other structural units of the Ministry of Foreign Affairs of Ukraine;

• special units of the Ministry of Defense and the Armed Forces of Ukraine.

3. Security Service of Ukraine.

4. State Service for Special Communications and Information Protection of Ukraine.

5. Intelligence agencies of Ukraine.

The above-mentioned central government bodies, in the course of implementing their functions to identify threats to the information security of the state, may involve the EFA and the IC, the mass media, political parties and movements, public organizations and trade unions, non-governmental research organizations, as w Ensuring the national security of the state is a matter not only for state authorities, but also for the entire society and every citizen. The presence of

an effective network of public structures is becoming one of the conditions for ensuring national security under modern conditions. According to the Law of Ukraine "On the Fundamentals of National Security of Ukraine", citizens of Ukraine and associations of citizens are subjects of ensuring national security, and the development of civil society and its democratic institutions is recognized as a priority direction for the implementation of the national interests of Ukraine [2].

However, science in Ukraine has not yet comprehensively studied the non-state security system as a public mechanism, and public associations as subjects of ensuring the national security of the state. The activities of certain types of public associations have not been linked to the state strategy for ensuring national security. In Ukraine, the non-state system of ensuring national security is at the stage of formation and does not have a significant impact on the situation. Today, it lacks a single coordinating body as a methodological and organizational center. In this context, proposals for the organization of the Center for Non-State Provision of National Security of Ukraine or the Independent Public Advisory Council of representatives of the Ukrainian and international expert communities under the NSDC of Ukraine can be considered relevant.

The problem of ensuring information security must be considered in a nationwide dimension. The state mechanism for ensuring information security must take into account national interests in the information environment, internal and external threats to these interests, and a system of means for detecting and neutralizing threats must be provided. It must necessarily include a two-way connection between society, the media, and the state, which will help to timely notify about changes in public opinion under targeted influence and assess the effectiveness of countermeasures. To implement the above provisions, a clear system of bodies is needed that can take on the task of protecting the information space. In his research and scientific conclusions, Ukrainian scientist V. Ostroukhov emphasizes the formal existence of such a system and identifies four interconnected levels: legislative support and parliamentary control are carried out by the Verkhovna Rada of Ukraine; law enforcement and national security functions are provided by a number of bodies subordinate to the President of Ukraine; managerial and administrative functions are concentrated in the Cabinet of Ministers of Ukraine; private initiative, commercial interest and public control are implemented through the activities of various non-governmental organizations and independent media.

Thus, the analysis of the state of information security shows the need to improve the system of administrative and legal regulation of information security. There is a need to develop new means, methods and ways to ensure information security of state administration, monitoring the information environment, the presence of threats and dangers.

Conclusions. Ukraine needs such regulatory and legal acts that would regulate relations in the formation and management of information resources at the state, regional and local levels. The regulatory consolidation of the orientation of

state and public information resources to the activities of state administration bodies is relevant. The problem of legal regulation of information technologies that create the infrastructure of the information society, issues of intellectual property in the field of information relations also need to be resolved. Regulatory and legal acts that would regulate public relations in the field of accounting and monitoring in the information sphere are necessary. It is necessary to establish by law the approved provisions: on the mandatory composition and basic technical equipment of production and corporate networks that affect the state of information security; on mandatory requirements for information security of systems, software and hardware; on safe business operations using new information technologies and global information networks. Further resolution of the issue of developing a set of information standards taking into account information security, developing a certification system for information products, systems and services, and creating a licensing system for the activities of organizations in certain areas of forming a unified information space of Ukraine is required.

Список використаних джерел:

1. Домбровська С.М., Помаза-Пономаренко А.Л., Крюков О.І., Порока С.Г. Інформаційні загрози та комунікативна інфраструктура в державному секторі : монографія. 2024. Харків: НУЦЗУ. 244 с. URL: http://repositsc.nuczu.edu.ua/handle/123456789/19990.

2. Офіційний веб-сайт Верховної Ради України. URL: https://zakon.rada.gov.ua/laws.

3. Почепцов Г. Токсичний інфопростір. Як зберегти ясність мислення і свободу дії. Харків : Віват, 2022. 384 с.

4. Підсумки порушень прав журналістів та свободи слова з початку російської агресії — IMI (інфографіка). URL: http://imi.org.ua/analytics/44669-pidsumki-porushen-prav-jurnalistiv-ta-svobodi-slova-z-pochatku-rosiyskoji-agresiji-imi-infografika.html.

References:

1. Dombrovska S.M., Pomaza-Ponomarenko A.L., Kryukov O.I., Poroka S.G. Information threats and communication infrastructure in the government sector: monograph. 2024. Kharkiv: NUTSZU. 244 p. URL: http://repositsc.nuczu.edu.ua/handle/123456789/19990.

2. Official website of the Verkhovna Rada of Ukraine. URL: https://zakon.rada.gov.ua/laws.

3. Pocheptsov G. Toxic infospace. How to maintain clarity of thinking and freedom of action. Kharkiv: Vivat, 2022. 384 p.

4. Summary of violations of journalists' rights and freedom of speech since the beginning of Russian aggression — IMI (infographics). URL: http://imi.org.ua/analytics/44669-pidsumki-porushen-prav-jurnalistiv-ta-svobodi-slova-z-pochatku-rosiyskoji-agresiji-imi-infografika.html.

дата надходження статті: 06.10.2024
дата прийняття статті: 18.11.2024
дата публікації: 25.12.2024