UDC 338.24

THREATS TO INFORMATION SECURITY OF UKRAINE IN THE CONDITIONS OF DIGITALIZATION

Onyshchenko Svitlana
Doctor of Economics, Professor
Hlushko Alina
Maslii Oleksandra
PhD in Economics, Assistant Professor
National University Yuri Kondratyuk Poltava Polytechnic
Poltava, Ukraine

Annotation: the issue of information security of the national economy in the conditions of digitalization is actualized in the article. A study of the regulatory framework in Ukraine on information security. There is a lack of a systematic approach to the definition of threats to information security as a basis for its provision. The main threats to information security of Ukraine in the conditions of strengthening of digitalization processes are substantiated and determined.

Keywords: information security, threat, digitalization, national economy, state regulatory policy.

In the conditions of deepening of digitalization processes, the problem of maintenance of such level of information sphere development at which external negative influences do not create real dangers to information security of Ukraine becomes urgent.

The information security subsystem occupies a special place in the national security system. Information relations and processes permeate all others that take place in society. The information sphere exists simultaneously on two levels: independently and in conjunction with other areas of the national economy through their information services and ensuring interaction through information [1]. Thus, the

information sphere and its separate elements make it possible to indirectly influence the social, economic, political, spiritual, and other spheres of the national economy. Therefore, information security is a guarantee for other components of economic security and national security in general.

Ukraine's information security is ensured by protecting the national information space from information threats and by promoting its sustainable development to realize the vital interests and needs of the citizen, society, and the state in the information sphere [2]. At the same time, the national information space is not enough protected from the negative impact of external and internal threats today, which poses a threat to the socio-economic development of the country, its integration into European structures, and functioning in general.

Threats to information security can legitimately identify existing and potentially possible phenomena and factors that pose a danger to the vital interests of man and citizen, society, and the state in the information sphere [3].

The regulatory framework in Ukraine on information security is several regulations, including Laws of Ukraine: "On National Security of Ukraine"; "On the Concept of the National Informatization Program"; "On Basic Principles of Information Society Development in Ukraine for 2007- 2015"; the Concept of development of digital economy and society of Ukraine for 2018-2020. These acts disclose certain aspects of the definition of information security and areas of its provision. At the same time, there is no systematic approach to the definition of information security threats.

Given the provisions of the Draft Concept of Information Security of Ukraine, the system of threats to information security can rightly be presented in the form of two blocks, which include:

1) threats of a communicative nature in the field of realization of the needs of man and citizen, society and the state regarding the production, consumption, distribution, and development of national strategic content and information;

2) threats of technological nature in the field of operation and security of cybernetic, telecommunication, and other automated systems that form the material

(technical, instrumental) basis of domestic information space.

The first group of threats should include external negative informational influences on the consciousness of man and community through the media, as well as the Internet, which are carried out to the detriment of the state. Also dissemination of distorted, unreliable, and biased information to discredit public authorities, destabilize the socio-political situation, which significantly complicates political decision-making, harms the national interests of Ukraine or creates a negative image of Ukraine; threats to freedom of speech; creation, dissemination, transfer, and storage of information to support or intensify criminal and terrorist activities.

The second group of threats to information security involves the use by foreign states of cyber troops, cyber units, new types of information weapons and weapons of a cyber nature to the detriment of Ukraine; manifestations of cybercrime, cyberterrorism or cyber military aggression that threaten the sustainable and secure operation of national information and telecommunications systems through interference, unauthorized access or disruption of telecommunications, cyber, automated computer systems, regardless of ownership; insufficient level of development of the national information infrastructure; violation of the procedure for access, treatment and established regulations for the collection, processing, storage, dissemination or transfer of information protected by the state (state secret, confidential information, personal data, copyright or intellectual property), or work with information resources containing it; lack of public control over the activities of information security entities, protection of the national information infrastructure and information space of Ukraine.

However, we should note that this list of threats cannot be considered exhaustive and constant. The most pressing threats to the information security of the state in the context of digitalization are primarily cross-border and those that have a political color have long been studied in the context of the problem of information warfare, the concept of which they cover [4].

Information warfare, taking into account existing views on its nature, can be defined as a set of purposeful information influences carried out using information

weapons (algorithm of purposeful influence on the information system by transmitting information to it or carrying out other planned actions). As well as actions aimed at the acquisition of information that is not publicly available, its unauthorized distribution, modification, or destruction, carried out to achieve the intended purpose. The danger, reality, and effectiveness of information warfare are provided by the suggestive nature of influences, secret or veiled nature of unauthorized receipt or use of information, other harmful actions in the information sphere, which, in turn, directly create conditions for the oppression of interests, primarily national, or violation processes of functioning of information systems [1].

We should note that the technical aspect is not the main one in the structure of information security. It is necessary to ensure not only the security of information from destruction, distortion, blocking, unauthorized leakage, or violation of the established routine procedure but also the information security of society. Society itself is the bearer of such a global threat to human information security as information discrimination, which is manifested in the separation of people into those who have access to information and those who are deprived of it. Of fundamental importance for modern society is the fact of the existence of an information picture of the world.

One of the most common types of information threats is the dissemination of so-called pathogenic texts, which are aimed, in particular, at undermining national and state interests, threatening public morals, having a harmful psychological impact, leading to neglect of fundamental rights, and freedoms [5]. It is impossible to close the national information space from such information influence, first of all external, using administrative measures therefore it should be protected from security threats as well as ground, air, and sea.

The complex nature of current threats to information security of the state requires the definition of innovative approaches to the formation of a system of protection and development of the information space in the context of globalization and free information circulation.

REFERENCES

1. Tkachuk T. Legal provision of information security in the conditions of Ukraine's European integration: dis. – Uzhhorod. – 2019. – 487 p.

2. Onyshchenko S. The impact of the COVID-19 pandemic on information security as a determinant of protection of national interests / S. Onyshchenko, A. Hlushko // Perspectives of world science and education. Abstracts of the 13th International scientific and practical conference. CPN Publishing Group. – Osaka, Japan. – 2020. – Pp. 207-212.

3. Onyshchenko S. Risks and threats in the context of digitalization: the security aspect / S. Onyshchenko, O. Maslii // II International Scientific Conference Development of Socio-Economic Systems in a Global Competitive Environment: Conference Proceedings, May 24th, 2019. – Le Mans, France. – Pp. 54–56.

4. Onyshchenko S. Conceptual principles of information security of the national economy in the conditions of digitalization / S. Onyshchenko, A. Hlushko // Social economy. – HNU, 2020. –59. – Pp. 14-24.

5. Maslii O. Challenges to economic security of business in the conditions of digitalization / O. Maslii, B. Ivaniuk // NEW ECONOMICS: Proceedings of the International Scientific Forum «NEW ECONOMICS – 2019» (Kiev, 14-15 November 2019): T.1; NAS of Ukraine, Institute of Industrial Economics. – Kiev, 2019. – Pp. 86-89.