УДК 323
DOI: 10.31733/15-03-2024/2/305-307

Alona BURIAK
Associate Professor of the Department
of International Economic Relations
and Tourism of the National University
«Yuri Kondratyuk Poltava Polytechnic»,
Candidate of Sciences (Economics),
Associate Professor

MAIN AREAS OF ACTIVITY IN THE SPHERE OF PROVIDING INFORMATION SECURITY OF THE STATE

The strategic dimension of Ukraine's information security includes countering information influences on critically important areas of state functioning. Information interventions in this context are described as a set of measures aimed at spreading specifically selected messages or their interpretations through various communication channels. These measures are aimed at influencing public opinion, forming a certain context or view of a certain situation, and making important decisions by the state leadership. Information technology, foreign-made equipment used in the country can also be involved in such interventions.

It is important to note that these actions can be part of hybrid information wars, where different tools are combined, including cyber-attacks, disinformation, information manipulation and other methods to achieve strategic goals.

One of the key problems is the provision of energy, technological and medical security in the conditions of information interventions. This includes the protection of critical infrastructures, data and systems in the fields of energy, technology and healthcare from cyber-attacks and negative information impact [1].

The general approach to Ukraine's information security strategy includes the development of an effective system of protection against such threats, strengthening cyber security, detecting and countering disinformation, as well as ensuring the stability and resilience of critical sectors in the event of possible impacts.

The Russian Federation's approach to influencing different countries may indicate the variety of methods and approaches it uses to achieve its strategic goals in different regions, as well as the different levels of activity and aggressiveness of these actions.

The economic sphere is one of the important components of the strategic dimension of Ukraine's information security. Russia's war against Ukraine, which includes informational and psychological influence aimed at destabilizing and discrediting the Ukrainian state, includes informational attacks aimed at the economic sector [2].

The full-scale invasion of the Russian Federation into Ukraine created a tense economic situation. This became one of the components of the war, which involves information and psychological methods to influence the country's economy.

In particular, Russian influencers use information channels to create a negative image of the Ukrainian economy, spread disinformation about its stability and development. This can affect the investment climate, the country's internal and external economic potential, as well as general trust in Ukrainian financial and economic institutions.

Ukraine is forced to respond to these threats and increase the level of information security in the economic sector. This includes measures to strengthen the cyber security of financial institutions, protection against cyber-attacks on economic objects, development of information campaigns to preserve trust in financial systems, and creation of mechanisms to respond to disinformation about the economic state of the country.

The development and support of information security in the economic sector is important for ensuring the stability and development of the Ukrainian economy in conditions of war and information threats [3].

Quantum cyber security will become one of the most important aspects in future cyber security, as the development of quantum technologies opens up new opportunities and creates significant challenges for the protection of information and information systems. These technologies can provide a high level of privacy, reliability and security in the field of

communications and computing. However, they can also become the target of new threats in cyberspace.

Currently, many countries and corporations are investing significant resources in the development of quantum technologies and software. The expansion of the use of quantum technologies can change the paradigm of cyber security, providing new methods of encryption and data protection that can become important in the field of sharing confidential information between government structures, financial institutions, defense sectors and other critical systems.

However, with the development of quantum cyber security, new challenges arise. In particular, the development of quantum computers could help decipher some of the encryption systems currently in use. This means that existing protection methods may become less effective, which requires the development of new cryptographic methods to ensure security in the context of quantum computing.

Thus, quantum cyber security represents both new opportunities and new threats. The development of this field requires constant improvement of protection methods and cryptographic means, as well as cooperation between states and the private sector to ensure security in cyberspace.

Ukraine, like many other countries, in its Cyber Security Strategy considers the importance of quantum security for the protection of important state information resources and critical information infrastructure. Quantum technologies can become an important element in protecting against current and future cyber threats.

In the context of the Cyber Security Strategy of Ukraine, the priorities concern [4]:

1. Development and adaptation of the state cyber security policy. Creation and continuous updating of strategies for protection against cyber threats, including aspects of quantum security.

2. Compliance with EU and NATO standards. Compliance with international cyber security standards is important to ensure cooperation with other countries and organizations in this area.

3. Technical and cryptographic protection of information. Development and improvement of technical protection systems that use quantum technologies to ensure the security of data exchange.

4. Involvement of innovative startups for the introduction of quantum technologies. It is important to consider promising technologies and promote their implementation in the field of cyber security through cooperation with innovative companies and startups.

Therefore, quantum security becomes not only an important part of the Cyber Security Strategy of Ukraine, but also a key direction for ensuring the security of state information systems and infrastructure in the conditions of modern and future cyber threats.

In addition to its direct threat to health and life, COVID-19 has also become an object of information manipulation and a place for disinformation to spread. Information security specialists attribute this aspect to the strategic dimension of information security, since the destabilization of the situation in the state and society due to the spread of fake messages about the coronavirus becomes part of hybrid threats.

External and internal information interventions that spread fake and manipulative information about COVID-19 may contain a variety of claims that have no scientific basis or are based on conspiracy theories. This can lead to ignoring the necessary preventive measures, incorrect treatment, refusal of quarantine and strengthening of negative relations with the authorities due to the formation of protest behavior among the public.

Such manipulations can have serious consequences for society and the state. Strengthening the relevance of information campaigns, public education and raising citizens' awareness of facts, reliable information and viral threats are important steps in combating misinformation and increasing the level of covid security in the country.

Thus, innovative tools of information security policy, such as quantum security and covid security, have the potential to be important factors in countering cyber threats and in controlling their possible use in hybrid conflicts. The development of these areas allows the use of advanced technologies and scientific achievements to improve information security.

Ukraine's cooperation with EU institutions and European organizations, as well as the industrial sector, can become a key element in this process. This collaboration can facilitate the sharing of knowledge, best practices and technologies related to cyber security, including aspects of quantum and biological security. Cooperation in the field of applied scientific research is also important for the implementation of innovative approaches in practical application, ensuring cyber security and information protection [5].

The creation of strategic digital capabilities and the development of integrated information and cyber security measures play an important role in strengthening the country's defense against cyber threats. This can be achieved through the integration of advanced technologies, cooperation and exchange of experience with European partners in order to create more sustainable and innovative information protection and cyber security systems.

Ensuring Ukraine's information sovereignty involves a set of measures and areas of activity aimed at protecting and preserving the national information system, as well as ensuring its own information resources. The main areas of state activity in this area include:

1. Cyber security and cyber protection. Development and implementation of cyber security strategies and policies, protection measures against cyber threats, development of cyber protection systems for critical infrastructures, improvement of cyber security of government and state networks.

2. Information security and protection of personal data. Development and implementation of policies and legislation on personal data protection, ensuring compliance with international information protection standards.

3. Control over the spread of disinformation and fakes. Creating mechanisms for detecting and countering fake news, viral news, as well as supporting media literacy among the population.

4. Creation and support of the national information infrastructure. Development and support of own information infrastructure, including communication networks, data centers, information systems, etc.

5. Creation and improvement of legislation. Development and implementation of laws and regulations aimed at protecting the information security of the state, including cyber security, personal data protection, combating cybercrime and disinformation.

6. International cooperation. Participation in international exchange programs, cooperation with other countries and international organizations on issues of cyber security and information security.

7. Increasing information awareness of citizens. Development of educational programs and initiatives aimed at increasing the level of awareness of citizens regarding cyber security, Internet security, recognition of disinformation and fakes.

These directions allow the state to improve its systems of information protection and combating cyber threats to ensure the stability and security of the information space of Ukraine.

1. Onyshchenko S.V., Masliy O.A., Buriak A.A. Threats and risks of ecological and economic security of Ukraine in the conditions of war. XVII International Scientific Conference *«Monitoring of Geological Processes and Ecological Condition of the Environment»* 7-10 November 2023. Kyiv. Ukraine. Mon23-072. https://reposit.nupp.edu.ua/bitstream/PoltNTU/13700/1/2023_11_Mon23-072.pdf.

2. Buriak A., Levchenko I., Herashchenko V., Shevchenko O. Impact of full-scale war on changes in the format of Ukraine's cooperation with the European Union. *The EU Cohesion policy and healthy national development: Management and promotion in Ukraine*: monograph. In: Letunovska N., Saher L. & Rosokhata A. Szczecin: Centre of Sociological Research, 2023. P. 369–378 (645 p.). DOI: https://doi.org/10.14254/978-83-968258-5-8/2023.

3. Маслій О.А., Буряк А.А. Трансформація загроз економічній безпеці та безпеці інформаційного середовища України в умовах повномасштабної війни. Держава та регіони. Серія: *Економіка та підприємництво*. 2023. № 3 (129). С. 28–32. DOI: https://doi.org/10.32782/1814-1161/2023-3-5.

4. Буряк А.А., Маховка В.М., Сторожук Л.М. Стратегія і механізми запровадження цифрової економіки в країнах ЄС та Україні як умова подолання кризових явищ. *Економіка і регіон*. 2023. № 2(89). С. 53–59. DOI: https://doi.org/10.26906/eip.v0i2(89).2934.

5. Буряк А.А., Кудряшова Д.О., Сторожук Л.М. Стратегія розвитку digital-економіки в Україні: національна візія та виклики глобалізації. *Система управління відходами в циркулярній економіці: фінансові, соціальні, екологічні та енергетичні детермінанти*: монографія. Суми: Сумський державний університет. 2023. С. 239–248.