THE CURRENT SITUATION WITH THE INFORMATION SECURITY IN UKRAINE

Liudmyla RYBALCHENKO,

PhD, Associate professor,
Dnipropetrovsk State University of Internal Affairs, Dnipropetrovsk region, Ukraine,
ORCID 0000-0003-0413-8296
E-mail: luda_r@ukr.net

Abstract: The condition in which Ukraine is since 2022 after russia's full scale military invasion, forces us to consider the issue of security in all spheres of life as one of the main components of the state's national security. Conducting informational influence on human consciousness has changed significantly, which is carried out with the use of mass media. The creation of mass information attacks, bots, fakes and other means of influence are effective tools for disorienting the entire society and manipulating people to increase panic. Specially created information resources try to influence in such a way that a person perceives information in the way it is presented and believes it.

Keywords: information security, national security, protection of personal data, information technology.

UDC: 004.056(477)

JEL Classification: H56; D81.

INTRODUCTION

Rapid changes that are taking place in the modern information space require effective protection of national information security, which should guarantee the safe functioning of all spheres of life for Ukrainians. Ensuring information security at all levels of socio-economic development, improving legislative and regulatory provisions on information protection, identifying possible threats and preventing them, and cooperation with other countries and international organizations is an important strategy for the international and national security of the country, especially during the martial law period in Ukraine.

To the main regulatory documents and laws regarding information security of Ukraine belongs: the Constitution of Ukraine, the Criminal Code of Ukraine, the Law of Ukraine "On the Basic Principles of Cybersecurity in Ukraine", the Law of Ukraine "On Information", the Law of Ukraine "On Protection of Information in Information and Telecommunication Systems", the Law of Ukraine "On Personal Data Protection" and documents in the field of personal data protection, the Law of Ukraine "On Access to Public Information", the Law of Ukraine "On National Security of Ukraine" and other laws, also, the Information Security Doctrine of Ukraine, the Council of Europe Convention on Cybercrime and other.

PAPER BODY

The issue of information security is related to information technologies that are used to ensure information security. Protection of information security consists not only of the protection from an unauthorized access to information, but also of the use of appropriate methods for its security and protection [1].

Today, preserving information sovereignty and forming an effective security system in the information sphere is a top priority for our country. Ensuring the integrity of

society, protecting the national information space and countering all negative information influences is an important issue for Ukraine.

Ensuring reliable information security in the country will protect the interests of the citizens in obtaining true and quality information. Information security is one of the important components of the country's national security. It is information security that reflects the state of protection of the interests of citizens and the country from negative informational influences and dangers that may be associated with unauthorized access and interference with personal or state information, as well as its dissemination [2]-[3].

The issue of guaranteeing information security in Ukraine became the most urgent during the war due to the influence and spread of russian propaganda through mass media on the consciousness of Ukrainian citizens and the public around the world.

Now there are significant threats in the national information space of Ukraine, which pose a danger to our state, its sovereignty, integrity, political and economic development.

The creation of threats to the national security of Ukraine in the information sphere is a danger to the life of every citizen, it has a negative informational impact on the consciousness of citizens, the information, technical and critical infrastructure of the country.

The rapid development of information technologies has become a significant impetus for the creation of new manifestations of security caused by the situation of a new technological level.

The division of spheres of influence in cyberspace is constantly increasing. The country's ability to protect its national interests is a priority component of every country's cyber security. The creation of cyber troops in the state will contribute to the powerful protection of the information infrastructure against possible cyber attacks, reliable protection against interference in the national information space, as well as the management of the enemy's information systems and their destruction.

The main cyber threats include violations of data integrity, unauthorized access, information confidentiality, interference with corporate or state secrets, etc. Such threats affect the functioning of any information system, the sphere of activity of a company or institution, as well as ensuring national security.

Therefore, in order to manage any dangers, it is necessary to create powerful protection against possible and potential threats with the involvement of highly qualified personnel and the use of modern software tools.

National-level issues include the identification of cyber threats, cybersecurity measures and capabilities, the development of the main indicators of cyber security, their research according to certain characteristics, and the creation of appropriate groups of cyber security indicators for the analysis and development of measures to avoid them. All government agencies and private entities interact with each other to prevent and overcome negative consequences.

Since there is a war going on now in Ukraine, there is a growing need to ensure security against threats in cyberspace of the country. The priority prospects are the adoption of such strategic decisions, which would be aimed at managing the risks of the companies and strengthening their stability in terms of security. Most business leaders see cyber resilience as a business priority in their organization. Moving from cyber security to cyber resilience is an important step towards a more secure and sustainable future.

The Ministry of Digital Transformation of Ukraine and the State Service of Special Communications and Information Protection of Ukraine are conducting work on strengthening protection against cybercrime through updating and reforming the legislative

framework, improving the mechanism of cyber protection of state authorities, their information and telecommunication systems, conducting an analysis of the condition of cyber protection of state information resources and critical information infrastructure [4].

It is worth mentioning that the modern development of digital technologies is much faster and contributes to the spread of cybercrime. Therefore, the existing regulatory legislation, which is aimed at regulating this type of crime, needs constant improvement.

CONCLUSIONS

Thus, in the conditions of military aggression of russia in Ukraine, the current national information space of our country is not sufficiently protected from negative informational influences and threats. Therefore, the protection of information sovereignty, the creation of a powerful and effective information security system of Ukraine, countering cyber attacks and threats are strategic tasks of the state.

Therefore, at the state level, the current legislation should be improved in the direction of strengthening the legal support for the protection of national information security, in the field of cyber security and cyber protection, through fruitful cooperation with the divisions of the leading countries of the world.

BIBLIOGRAPHY

1. RYBALCHENKO L., KOSYCHENKO O., KLINYTSKYI I. Ensuring economic security of enterprises taking into account the peculiarities of information security. *Scientific journal «Philosophy, Economics and Law Review». Volume* 2 (1), 2022. – p. 71-81. ISSN 2786-491X

2. RYBALCHENKO L., KOSYCHENKO O. Peculiarities of using visual means of information and analytical activity in legal and law enforcement sphere. *Scientific journal «Philosophy, Economics and Law Review».* Volume 2 (2), 2022. – p. 162-169. ISSN 2786-491X

3. RYBALCHENKO L., RYZHKOV E., OHRIMENCO S. Economic crime and its impact on the security of the state. *Scientific journal "Philosophy, Economics and Law Review",* 1(2), (2021). – p. 67-80. ISSN 2786-491X

4. STATE SERVICE OF SPECIAL COMMUNICATIONS AND INFORMATION PROTECTION OF UKRAINE [online]. [viewed 15 october 2023]. Available from: < https://cip.gov.ua/ua >