УДК 355.033.8

A. V. Marushchak
S. S. Nykyporets

CYBER SECURITY AS A COMPONENT OF STATE PROTECTION

Vinnytsia National Technical University

Анотація

У статті розглядається підхід України до національної безпеки та кібербезпеки в умовах розвитку кіберзагроз. Наголошується на важливості державно-приватної співпраці, обміну інформацією та залучення експертів до ініціатив з кібербезпеки.

Ключові слова: *кібербезпека, національна система кібербезпеки, забезпечення національної безпеки, кіберзагрози, принципи, державно-приватна співпраця.*

Abstract

The article examines Ukraine's approach to national security and cyber security in the context of the development of cyber threats. The importance of public-private cooperation, information exchange and involvement of experts in cyber security initiatives is emphasized.

Keywords: *cyber security, national cyber security system, ensuring national security, cyber threats, principles, public-private cooperation.*

Introduction

In today's digital world, where information technology permeates all spheres of life, cyber security is becoming an integral part of national security. Like other countries, Ukraine depends on information systems and computer networks for the functioning of the economy, social and political processes, and national security. That is why the importance of cyber security as a component of the state acquires special importance.

Basics

The national security system of any country is based on conceptual legal documents that outline the official views on the role and place of the state in the world, its national values, interests and goals, and ways and means of preventing external and internal dangers and threats [1]. One of the main aspects of the national security system is the identification of external and internal dangers that may threaten the state. External threats can include military threats, acts of terrorism, cyber-attacks, illegal migration and other forms of hostile activity. Internal threats can manifest themselves in the form of socio-economic problems, political instability, crime and other internal challenges. Ukraine, like many other countries, recognizes the importance of the national security system. In view of modern threats such as Russian aggression, cyber-attacks and terrorism, Ukraine is actively working on improving its national security system.

Ensuring cyber security in Ukraine is based on the following principles:

1) rule of law, legality, respect for human rights and fundamental freedoms and their protection in the manner determined by law;

2) ensuring the national interests of Ukraine;

3) openness, accessibility, stability and security of cyberspace, development of the Internet and responsible actions in cyberspace;

4) public-private interaction, broad cooperation with civil society in the field of cyber security and cyber protection, through the exchange of information about cyber security incidents, implementation of joint scientific and research projects, training and professional development of personnel in this field;

5) proportionality and adequacy of cyber protection measures to real and potential risks, implementation of the state's inalienable right to self-defense in accordance with the norms of international law in case of aggressive actions in cyberspace;

6) priority of preventive measures;

7) the inevitability of punishment for committing cybercrimes;

8) priority development and support of domestic scientific, scientific and technical and production potential;

9) international cooperation with the aim of strengthening mutual trust in the field of cyber security and developing joint approaches to countering cyber threats, consolidating efforts in the investigation and prevention of cyber-crimes, preventing the use of cyber space for terrorist, military, and other illegal purposes;

10) provision of democratic civilian control over military formations and law enforcement agencies formed in accordance with the laws of Ukraine, conducting activities in the field of cyber security [2].

Ensuring the national interests of Ukraine is a fundamental principle guiding cyber security efforts. This entails promoting openness, accessibility, stability, and security in cyberspace, as well as responsible behavior in the digital realm. Collaboration between the public and private sectors and civil society plays a crucial role in cyber security and protection. This includes sharing information about cyber security incidents, engaging in joint scientific and research projects, and enhancing the training and professional development of personnel.

Public-private interactions in the field of cyber security consider the details of the legal order established by law for specific entities and specific types of activities.

Public-private cooperation in the field of cyber security is carried out by:

1) creation of a system for timely detection, prevention and neutralization of cyber threats, including with the involvement of volunteer organizations;

2) increasing the digital literacy of citizens and the culture of safe behavior in cyberspace, complex knowledge, skills and abilities necessary to support the goals of cyber security, the implementation of state and public projects to increase the level of public awareness of cyber threats and cyber protection;

3) exchange of information between state bodies, the private sector and citizens regarding cyber threats to critical infrastructure objects, other cyber threats, cyber-attacks and cyber incidents;

4) partnerships and coordination of computer emergency response teams;

5) involvement of expert potential, scientific institutions, professional associations and public organizations in the preparation of key industry projects and normative documents in the field of cyber security;

6) provision of advisory and practical assistance on responding to cyber-attacks;

7) formation of initiatives and creation of authoritative consultation points for citizens, representatives of industry and business in order to ensure security on the Internet;

8) introduction of a mechanism for public control of the effectiveness of measures to ensure cyber security;

9) periodically holding a national summit with professional business service providers, including insurers, auditors, lawyers, determining their role in promoting better risk management in the field of cyber security;

10) creation of a personnel training system and improvement of competence of specialists in various spheres of activity on cyber security issues;

11) close cooperation with individuals, public and volunteer organizations, IT companies for the purpose of implementing cyber defense measures in cyberspace [2].

The exchange of information about cyber threats, the establishment of computer emergency response teams, and the involvement of expert potential and scientific institutions contribute to the development of key industry projects and normative documents. By engaging various stakeholders, including citizens, industry representatives, and business entities, Ukraine aims to enhance cyber security measures and ensure a safer online environment.

Additionally, the focus on improving digital literacy, providing counseling assistance, and establishing counseling centers demonstrate Ukraine's commitment to enabling individuals and organizations to protect themselves from cyber threats. Public control mechanisms, national summits with professional service providers, and the development of a comprehensive training system further strengthen Ukraine's cybersecurity capabilities.

Since cyber threats cannot be limited to any one area, it requires all stakeholders to have comprehensive awareness of the risk factors, skills and abilities to address them and appropriate measures to prevent cyber-attacks before they begin. Ukraine actively engages leading organizations in raising the level of awareness of commercial enterprises and non-profit organizations regarding cyber security at all levels [3].

In Ukraine, various higher education institutions are actively introducing educational programs on cyber security, aimed at the bachelor's, master's, or professional level [3].

The rapid advancement of technology has brought numerous benefits to society, but it has also exposed us to new risks and vulnerabilities, particularly in the realm of cyber security. Recognizing the importance of a comprehensive approach to tackling cyber threats, Ukraine has taken proactive steps to raise awareness and enhance education in this critical field.

In order to effectively address cyber threats, it is essential that all stakeholders possess a thorough understanding of risk factors, possess the necessary skills and abilities to mitigate those risks and implement preventive measures before cyber-attacks occur.

Conclusion

In conclusion, cyber security has emerged as a critical component of state protection in the modern world. Ukraine, recognizing the significance of a robust national security system, has prioritized the principles of the rule of law, national interests, openness, and responsible actions in cyberspace. By fostering public-private cooperation, exchanging information, involving experts, and enhancing education, Ukraine aims to strengthen its cyber defense capabilities and ensure a secure online environment. With the rapid advancement of technology, it is crucial for all stakeholders to possess the necessary awareness, skills, and preventive measures to effectively address cyber threats. By actively engaging organizations and introducing educational programs, Ukraine is taking proactive steps to mitigate risks and protect its interests in the digital realm.

REFERENCES

1. ЛІПКАН, В.; ДІОРДІЦА, І. Національна система кібербезпеки як складова частина системи забезпечення національної безпеки України. Підприємництво, господарство і право, 2017, 5: 174-180. http://pgp-journal.kiev.ua/archive/2017/5/40.pdf.

2. ОСНОВНІ ЗАСАДИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ УКРАЇНИ, Про. Закон України. Урядовий кур'єр, 2017, 215. https://usts.kiev.ua/wp-content/uploads/2020/07/zakon-ukrainy-pro-osnovni-zasady-zabezpechennia-kiberbezpeky-ukrainy.pdf.

3. ТРОФІМЕНКО, Олена Григорівна, et al. Кібербезпека України: аналіз сучасного стану. 2019. http://dspace.onua.edu.ua/bitstream/handle/11300/12213/statya_Trofymenko_Prokop_Loginova_Zadereyko_CYBERSECURITY%20OF%20UKRAINE.pdf?sequence=1.

Марущак Анастасія Віталіївна **–** студентка групи УБ-21б, Факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, м. Вінниця, e-mail: anamar349@gmail.com

Никипорець Світлана Степанівна – Викладач англійської та німецької мов, кафедра іноземних мов, Вінницький національний технічний університет, e-mail: fotinia606@gmail.com

Marushchak Anastasiia Vitalyivna – student of group УБ-21б, Faculty of Management and Information Security, Vinnytsia National Technical University, Vinnytsia, e-mail: anamar349@gmail.com

Nykyporets Svitlana Stepanivna – Teacher of English and German, Department of Foreign Languages, Vinnytsia National Technical University, e-mail: fotinia606@gmail.com