Yashchuk V. E., Ph.D., Associate Professor, Associate Professor of the Department of Information Security Management, Lviv State University of Life Safety, Lviv, valentina.lender@gmail.com, ORCID ID: 0000-0003-2651-4918, Researcher ID: F-9466-2019,

THE ROLE AND PLACE OF CYBER WEAPONS IN ENSURING THE INFORMATION SECURITY OF THE STATE

A cyber weapon is a specific type of weapon used in the digital or cyber space to cause harm, influence systems, or gain an advantage in the information, military, or political spheres. It includes a variety of techniques and tools used to carry out cyber attacks, break into information systems, spread viruses and Trojan programs, cyber espionage, and other types of cyber operations.

Cyber weapons can be used for a variety of purposes. Cyber weapons can be used to penetrate computer networks and systems to gather intelligence. Cyber weapons are also used to carry out cyber attacks on information systems, networks and computers with the aim of stealing data, causing damage or blocking operations.

Cyber weapons can be used by terrorist groups to carry out terrorist acts in the digital space, such as attacks on critical infrastructure or networks. Also, this type of weapon is used to manipulate information, influence public opinion and disinformation in order to achieve certain political, economic or military goals. The use of cyber weapons is gaining more and more importance in the modern world, as information technologies are becoming more and more integrated into all spheres of life and are becoming very important for the functioning of society and states.

In today's world, cybernetic weapons are one of the newest and most effective examples of modern weapons. Cyber weapons are the means of conducting cyber warfare and the systems associated with them. Means of conducting cyber warfare are cyber weapons and cyber weapons systems (techniques, tools, mechanisms, equipment, software, etc. - all that is developed and used to carry out cyber attacks [1].

The use of cyber weapons in ensuring the information security of the state remains a very urgent problem in the modern world due to the growing level of cyber

threats, the active digital transformation of the world, active political conflicts, economic consequences, and the existing military strategy. With the development of technologies, the number of cyber threats that can affect state security is also increasing. Cyber attacks can be carried out both by individual hacker groups and by the state with the aim of causing political, economic resonance or military damage. The growing amount of information and processes that take place in the digital space creates new opportunities for cyber attacks and the need to ensure their security.

Cyber attacks can be used as a means of political pressure and influence on government decisions. They can be aimed at influencing elections, manipulating public opinion, as well as other aspects of the country's political life. Cyberattacks can lead to serious economic losses for the state due to disruption of financial systems, critical infrastructure facilities, as well as loss of confidential information. The use of cyber weapons is an important component of the military strategy of states. The ability to conduct and defend against cyber attacks can affect the outcome of military conflicts.

Cyber weapons in the modern world play a key role in ensuring the information security of states. Its place in this process lies in various aspects, including defense against cyber attacks, cyber intelligence, cyber terrorism, and the use of cyber weapons in military operations. Cyber attacks can be directed at government infrastructures, military facilities, critical information infrastructure, political systems, etc. Cyber weapons are used to detect, target and respond to such threats. Cyber weapons can be used to conduct intelligence, which may include hacking information systems and leaking confidential information. This type of intelligence can help identify potential threats to national security.

The use of cyber weapons by terrorist organizations can pose a serious threat to the security of states. Cyber attacks can target critical infrastructure, financial systems, communication networks, and more. In modern military conflicts, cyber weapons are used as one of the key tools. It can be used to paralyze military communications, damage important objects, increase the effectiveness of military operations, etc.

By the classification of cybernetic weapons, we will understand the distribution of all possible types of them into interrelated classes, determined on the basis of the most significant and practically important features. Considering the number and variety

of cybernetic weapons, the main principle that can be used as a basis for classification is characteristic [1,3]. Today, it is proposed to classify cybernetic weapons according to the following basic characteristics: purpose, scope of application; the nature of the impressive action; method of delivery; controllability; destructive influence; efficiency; place of base; masking level; manufacturing method; range of action; objects of damage; the level of influence on the affected objects; aiming properties; integral effect; type of connections and level of interaction; consequences; principle of generation; self-organization; duration of effect; latency.

The advantage of such a classification is the possibility of expanding the set of features by which classification can be carried out. In addition, such a classification ensures the formalization of requirements for newly created samples of cybernetic weapons and makes it possible to more clearly visualize the features of the mechanism of action of cybernetic weapons on all possible objects of damage, to forecast the trends of its development, as well as to foresee measures to protect against the factors of its damage.

In general, the growing number of cyber threats and their potentially wide range of consequences emphasize the relevance of using cyber weapons to ensure the information security of the state. Accordingly, states continue to invest in the development and improvement of cyber defense strategies and technologies. In ensuring the information security of the state, it is important to develop and implement strategies to protect against cyber threats, improve technological solutions, and improve the qualifications of personnel. It is also necessary to actively cooperate at the international level to exchange information and jointly counter cyber threats.

Список використаних джерел

1. Hryshchuk R. V. Cybernetic weapons: classification, basic principles of construction, methods and means of application and protection against it / R. V. Hryshchuk // Modern special technology. - 2016. - No. 3. - P. 94-101. - Access mode: http://nbuv.gov.ua/UJRN/sstt_2016_3_14.

2. David E. Sanger and Eric Schmitt, “U.S. Cyberweapons, Used Against Iran and North Korea, Are a Disappointment Against ISIS,” The New York Times, June

12, 2022. www.nytimes.com/2017/06/12/world/ middleeast/isis-cyber.html

3. Hryschuk R.V. Fundamentals of cyber security: a monograph / R.V. Hryshchuk, Yu.G. Danyk; in general ed. Prof. Yu.G. Danica - Zhytomyr: ZhNAEU, 2016. - 636 p.