INFORMATION SECURITY AS AN ELEMENT OF CIVIL DEFENSE IN THE CONDITIONS OF HYBRID WAR

Levchenko O. G., doc. of tech. sc., prof., Head of Department of Labour Protection, Industrial and Civil Safety of Igor Sikorsky Kyiv Polytechnic Institute;
Zemlyanska O. V., Senior lecturer, Polukarov Yu. O., Ph.D., Ass. Prof., Polukarov O. I., Ph.D., Ass. Prof. (Dep. LPICS of Igor Sikorsky Kyiv Polytechnic Institute);
Samofal D. V., stud. (gr. BB-11, Faculty of Biotechnology and Biotechnics of Igor Sikorsky Kyiv Polytechnic Institute)

Abstract. The article explores the role of information security as a crucial component of the civil defense system under the conditions of hybrid warfare. The authors focus on modern challenges related to the spread of disinformation, cyberattacks, and psychological influence on the population. The main threats in the field of information security are identified, and the need to enhance citizens' information resilience is substantiated. The paper emphasizes the importance of media literacy, the development of state systems to counter fakes and cyber threats, and the coordination of actions between authorities and the public to ensure civilian protection in the information space.

Keywords: information security, civil defense, hybrid warfare, disinformation, cyber threat, media literacy, information resilience.

Анотація. У статті розглядається роль інформаційної безпеки як важливої складової системи цивільного захисту в умовах гібридної війни. Автори акцентують увагу на сучасних викликах, пов'язаних із поширенням дезінформації, кібератаками та інформаційно-психологічним впливом на населення. Визначено основні загрози, що виникають у сфері інформаційної безпеки, та обґрунтовано необхідність підвищення інформаційної стійкості громадян. Наголошено на важливості медіаграмотності, розвитку державних систем протидії фейкам і кібератакам, а також координації дій органів влади та громадськості для забезпечення захисту населення в інформаційному просторі.

Ключові слова: інформаційна безпека, цивільний захист, гібридна війна, дезінформація, кіберзагроза, медіаграмотність, інформаційна стійкість.

Introduction. In the 21st century, information has become not only a source of knowledge, but also a powerful tool of influence that can be used as a weapon in new-type wars. With the beginning of hybrid aggression against Ukraine, the problem of information security has become particularly urgent. Systematic information and psychological operations, the mass spread of disinformation, fakes, manipulative narratives, as well as cyberattacks on the state's infrastructure are components of the enemy's modern military strategy [1-3].

In such conditions, the issue of information security goes beyond the purely technological or military sphere and becomes a key direction of civil defense, which includes training the population, creating an effective information system, identifying and neutralizing information threats.

Analysis of the state of the issue. In modern conditions of global instability and constant aggravation of the military-political situation in Ukraine, the issue of information security is gaining special importance. The hybrid war waged against our state by the aggressor includes not only traditional forms of armed confrontation, but also the active use of information and psychological operations, disinformation, cyberattacks and manipulation of public opinion.

A feature of hybrid war is that the enemy seeks to destabilize the situation from within, undermining trust in state institutions, sowing panic, spreading fakes and demoralizing the population. That is why information security becomes a critical element of the civil defense system, as it is aimed at protecting the population from the influence of destructive information, as well as ensuring timely, truthful and clear information about real threats and actions in emergency situations [4].

In war conditions, information can be no less dangerous than weapons. Unreliable messages, hostile propaganda or leaks of critically important data can lead to mass panic, disruption of evacuation measures, sabotage or losses among the civilian population. Therefore, the issues of forming the information resilience of the population, increasing the level of media literacy and creating an effective system for countering information threats are extremely relevant.

In addition, in the 21st century, cyberspace is becoming a new theater of hostilities. Already now, there is significant activity by hacker groups that attack energy, transport, banking infrastructure, as well as websites of state authorities. These actions are aimed at paralyzing the work of life support systems, sowing chaos and intimidating the population. Thus, protecting information infrastructure is one of the priority tasks in the field of national security and civil defense. It is in the context of hybrid aggression that the issue of information security should be considered not only as the competence of special services or individual IT specialists, but as an integral component of the civil defense system, which requires the active participation of all citizens, increasing the level of information hygiene and consolidated counteraction to information threats.

The purpose of this work is to highlight the role of information security as a critically important factor in ensuring the protection of the civilian population in conditions of hybrid warfare, as well as to analyze the main threats and ways to overcome them.

Methods, materials and research results. In the 21st century, traditional forms of armed conflict are increasingly being supplemented or even replaced by hybrid methods of warfare, among which information warfare occupies a special place. Ukraine, being in a state of prolonged hybrid aggression, has become one of the main targets for large-scale information attacks by an external aggressor. This puts forward new requirements for the civil defense system, the key element of which should be an effective information security system.

Information security in the context of civil defense includes not only technical measures to counter cyberattacks, but also socio-communicative mechanisms to protect citizens from disinformation, propaganda, panic and information terror. The relevance

of this issue is due not only to military threats, but also to the broader impact of the information environment on the security of society. When the population is systematically exposed to false information, it loses the ability to think critically, make the right decisions in emergency situations and coordinate its actions with state structures.

One of the greatest risks is the use of mass media and social networks to spread fake news, which destabilizes public opinion, undermines trust in state authorities, and demoralizes military personnel and civilians [5]. For example, during air raids or emergencies, the spread of false reports about hit sites or imaginary threats can provoke mass panic, overload emergency services, and chaos in communications. That is why timely, reliable, and official information of the population should become a priority in the structure of emergency response.

In this context, increasing the information resilience of citizens - that is, the ability to recognize fakes, check sources of information, think critically, and not succumb to information provocations – becomes particularly important. This can be achieved by developing media literacy through the education system, social enlightenment, regular trainings and educational campaigns in the media. In addition, the state must ensure the effective functioning of information space monitoring systems, prompt refutation of fake information and interaction with social media platforms.

An equally important aspect is the protection of the country's information infrastructure from cyber threats. Massive attacks on government websites, energy, transport, and financial infrastructure have become commonplace in the conditions of hybrid warfare. Such attacks are aimed not only at destroying critical systems, but also at creating an atmosphere of fear and uncertainty among the population. Therefore, the functioning of cybersecurity in the conditions of a hybrid threat is a strategic component of state policy and should be closely integrated into the civil defense system [6].

Information security is not an isolated area, but an interdisciplinary component that should take into account technological, social, psychological, and organizational aspects. Its integration into the civil defense system is a necessary condition for maintaining stability, security and moral and psychological endurance of Ukrainian society in the conditions of hybrid war. Only a combination of the efforts of the state, the expert community, public organizations and each citizen can ensure the proper level of protection in the information sphere and strengthen national resilience to the challenges of modernity. That is why in the conditions of hybrid war it is necessary to [7]:

1. Develop a system of informing the population about the occurrence of emergency situations by creating unified information platforms, prompt dissemination of verified information and a wide presence of state structures in social networks.

2. Introduce systematic training of the population for information security through educational programs, media literacy trainings, educational campaigns for different age and social groups.

3. Strengthen cyber protection of state bodies and critical infrastructure, in particular by updating legislation, involving cybersecurity specialists, and creating centers for rapid response to incidents.

4. Increase the level of interaction between the state, civil society and the media, ensuring openness, transparency and trust in the information space.

5. Support scientific research in the field of information security, developing new approaches to countering hybrid threats and studying the dynamics of the impact of information attacks on social stability.

Conclusions. Information security in the context of hybrid warfare is not only a part of state security policy, but also an important component of the civil defense system. In modern realities, it performs a critical function in preserving the psychological stability of the population, countering destructive information influence, ensuring effective communication in times of crisis, and protecting critical infrastructure.

Hybrid aggression is accompanied by informational and psychological pressure, the spread of fakes, cyberattacks, and manipulation of public opinion, which requires not only a professional response from state institutions, but also the readiness of society to such challenges. Ensuring informational stability of citizens, the development of media literacy, and the active presence of official structures in the public information space are key factors in successfully countering hybrid threats.

Information security should be considered as part of national stability, which encompasses not only the technical, but also the socio-communicative and educational dimensions.

References

1. Закон України «Про основи національного спротиву» від 16.07.2021 № 1702-IX. – Режим доступу: https://zakon.rada.gov.ua/laws/show/1702-20.
2. Національна стратегія кібербезпеки України від 26.08.2021. – Режим доступу: https://www.president.gov.ua/documents/4472021-40025.
3. Державна служба спеціального зв’язку та захисту інформації України. Рекомендації щодо захисту інформаційного простору. – Режим доступу: https://cip.gov.ua/.
4. Панченко, С. В. Цивільний захист у контексті інформаційної безпеки держави / С. В. Панченко // Інформаційна безпека людини, суспільства, держави. – 2021. – № 2(8). – С. 19–26.
5. Войтович, І. Медіаграмотність як інструмент протидії дезінформації в умовах гібридної війни / І. Войтович // Український журнал безпекових студій. – 2023. – № 1. – С. 33–40.
6. NATO Strategic Communications Centre of Excellence. Hybrid Threats and the Role of Information. – 2021. – Режим доступу: https://stratcomcoe.org/.
7. Zawadzki, M. Information warfare in hybrid conflicts: Case of Ukraine // Security and Defense Quarterly. – 2022. – Vol. 39(2). – P. 67–79.