RESPONSE TO EMERGENCIES

DOI: 10.52363/passa-2024.2-22
UDC: 351:004.056

Kurilo A. - PhD in Public Administration, lecturer of the department of organization and technical support of emergency and rescue works, National University of Civil Defence of Ukraine, Cherkasy
ORCID: 0000-0002-5139-0278

PECULIARITIES OF THE APPLICATION OF SOCIAL TECHNOLOGIES IN PUBLIC MANAGEMENT OF INFORMATION SAFETY PROCESSES UNDER MARTIAL LAW

The article is devoted to the analysis of social technologies that public administration subjects use to influence public administration objects. According to the author, these technologies play an important role in optimizing public administration processes of forming information safety of society, especially in conditions of martial law.

Key words: public administration, information, information safety, martial law, hybrid warfare, threats to information security, social technologies.

Formulation of the problem. Social technologies in public management of information security processes, given the strengthening of the humanitarian approach to the study of information security problems, are becoming increasingly important in the processes of ensuring information security of society and managing these processes. They form a scientific and practical social basis, contributing to the acquisition of the necessary knowledge and its practical application to protect the information interests of society, taking into account the social aspects of the functioning of the information environment.

Analysis of recent research and publications. Scientific, theoretical and methodological aspects of the development of public administration in the field of state information safety were studied in the works of domestic scientists, in particular A. Barinov, V. Horbulin, O. Vlasyuk, O. Kokhanovsky, V. Lipkan, O. Kryukov, E. Makarenko, A. Marushchak, Ya. Romanovsky, O. Senchenko, V. Tertichko, S. Lutsenko, V. Golobutsky, O. Radchenko, P. Maslyanko, G. Pocheptsov, O. Danilyan, V. Stepanov, O. Valevsky, B. Kormych, Yu. Dreval and others, devoted their works to various aspects of the problem of the information society.

Analysis of the applied use of social technologies in the field of public management of information security processes, especially in the context of hybrid warfare. The main thesis of the study is to determine how social technologies can contribute to effective public management, in particular in countering disinformation, strengthening national unity, and increasing the resilience of society to destructive information influences.

Presenting main material. The state of war significantly changes priorities and approaches to the use of social technologies in public administration. Threats associated with information attacks, disinformation, cybercrime and the undermining of social stability require prompt and effective solutions. In such conditions, social technologies are aimed not only at the usual optimization of management processes, but also at ensuring information stability, supporting civic unity and mobilizing society's resources. The issue of implementing changes

in the educational sphere aimed at training universal-level information security specialists in the higher education system becomes relevant. Such training involves a comprehensive study of all aspects of information security, including the effective use of existing technical and humanitarian knowledge and opportunities to create an optimal system for protecting the information interests of society. In the context of martial law, this task becomes particularly urgent, as the information space becomes one of the key areas of confrontation, requiring a prompt response to new threats. Special attention is paid to the training of specialists capable of countering information attacks, manipulations, disinformation, and ensuring the protection of critically important information infrastructure facilities.

We are talking about the development and implementation of a specialty that will provide training for specialists with comprehensive competencies. They must have technical knowledge, have an understanding of psychophysical aspects, know the basics of law, sociology, political science, and informatization. In the context of martial law, this is complemented by the need to study crisis management, cyber defense, and tactics for countering hybrid threats. Such an interdisciplinary approach will allow creating professionals capable of solving information security problems at the intersection of technology, the human factor, and social processes even in critical conditions. To train information security specialists of a universal level, it is extremely important to develop and implement new educational standards that will meet the challenges of the modern information society. This requires the creation of a specialty that would integrate the diverse aspects of professional activity related to information security. If we recognize the information society as a key factor in the modern development of civilization, then future educational programs should be aimed at training specialists who are equally competent in both the technical and humanitarian aspects of their activities.

New educational standards should be based on advanced achievements of science and technology, and also take into account an interdisciplinary approach to learning. They should include the study of modern educational technologies that allow for the integration of knowledge from various fields necessary for the formation of specialists capable of solving complex tasks. In military conditions, this includes in-depth study of methods for countering cyber threats, ensuring information security of critical state facilities, as well as strategies for information resistance. In particular, such educational programs should cover achievements in informatization, cryptography, information and communication systems, cybersecurity, mathematics and other exact and applied sciences. However, technical knowledge should be supplemented by the study of social and humanitarian disciplines, such as sociology, psychology, management, corporate communications, ethics and legal aspects of activities in the information sphere. This will ensure the formation of comprehensively developed specialists who are able not only to create and implement technical solutions to ensure information security, but also to effectively analyze social processes, form risk management strategies, resolve conflicts and carry out effective communication at all levels.

In wartime, it is important to introduce special training in crisis management, anti-crisis communications, countering disinformation and information attacks by the enemy. This will allow adapting the educational process to changing realities, ensuring the readiness of specialists to work in extreme conditions.

Thus, the creation of a new educational specialty that would integrate various aspects of technical and humanitarian training is not only a pressing task, but also a strategically important step for the development of human resources in the face of rapidly growing challenges

in the information sphere. Martial law requires not only the training of universal specialists, but also the operational adaptation of educational programs to modern challenges, which will increase national resilience in the context of information confrontation. Given the growing demand for highly qualified specialists in the field of information security, which is observed in the state, social and commercial sectors, there is a need to create a system of training personnel capable of effectively responding to the challenges of the modern information society. In conditions of martial law, this task becomes especially important, because information security becomes an integral part of national security, and the training of specialists must meet the realities of information confrontation.

Such training should be carried out exclusively in leading higher education institutions of Ukraine (at the university level), which have the necessary technological base, methodological support and a team of highly qualified teachers. This decision is key to ensuring the high quality of the educational process and preventing the spread of training in institutions with insufficient resource potential. In military conditions, it is also important to provide training programs that take into account the peculiarities of crisis management, cyber defense, protection of critical information infrastructure and counteraction to information attacks.

Particular attention should be paid to the limitation of training practices in some commercial higher education institutions, which often face a lack of appropriate infrastructure, material and technical support, modern educational equipment and professional teaching staff. The absence of these components can negatively affect the quality of training, which, in turn, threatens with an insufficient level of competencies of future specialists responsible for the security of information systems and processes in key areas of activity. In the context of war, any shortcomings in the training of specialists can have critical consequences for ensuring national resilience and defense capability. The optimal approach to solving this problem would be to create specialized faculties or departments at leading universities in Ukraine that would be able to provide interdisciplinary training in the field of information security. In particular, preference should be given to those universities that already have a developed base in such fields as technical sciences, engineering, law, sociology and psychology. This will allow building a comprehensive educational program that integrates modern achievements in the relevant scientific disciplines and meets the current needs of the labor market. Universities should also adapt their educational programs to wartime conditions, including training modules on information resistance, data protection in wartime and risk management in crisis situations.

Such specialized departments should develop and implement innovative teaching methods that include practical classes, laboratory research, simulations of real cases, solving information security problems and interdisciplinary projects. It is important that students not only acquire technical knowledge, but also develop their skills in analyzing social and psychological factors, studying the legal aspects of information activities, and mastering risk management. In wartime conditions, it is important to add practical exercises in responding to real cyber incidents, training in information intelligence, and analyzing disinformation campaigns. In addition, it is necessary to ensure cooperation between universities, government agencies, leading companies and international organizations working in the field of information security. This approach will allow students to gain access to best practices, internships and experience, and will also contribute to the adaptation of educational programs to new challenges and standards in this area. In conditions of martial law, such cooperation becomes especially

important, as it allows for a direct exchange of experience and best practices that are relevant for wartime conditions.

Thus, the concentration of training of information security specialists in the best higher education institutions of Ukraine with the involvement of their scientific and technical potential is a strategically important step for the formation of competitive personnel capable of ensuring effective protection of the information interests of society at the national and international levels. In the context of martial law, this is not only an educational but also a defense task that contributes to strengthening the information resilience of the state and society.

A modern analysis of information threats and dangers, as well as their sources, indicates the relevance of a number of problems identified seven years ago in the Information Security Doctrine of Ukraine [1]. Key challenges include information aggression from other states, cyberattacks, a low level of information literacy among the population, an insufficient level of protection of the national information space, and imperfect legislative regulation in the field of information security. In conditions of martial law, these challenges become even more acute, because information attacks can have critical consequences for the security of the state, and cyberthreats become part of hybrid wars [2]. Effective training of personnel in the field of information security is an important task and requires a comprehensive approach, which includes:

• creation of general methodological foundations of personnel training with the definition of mechanisms for public regulation of this process;

• analysis and integration of an interdisciplinary approach that takes into account knowledge from technical, social, legal and management disciplines;

• introduction of innovative educational technologies aimed at increasing the efficiency of the dissemination of knowledge and skills;

• formation of a scientific and methodological base that will ensure continuous and high-quality training of specialists;

• development of an organizational and regulatory framework that will ensure the effectiveness of the training system and its compliance with modern challenges;

• technological modernization of the educational process, including the use of digital tools, the creation of interactive materials and the introduction of the latest methods.

This approach will contribute not only to the formation of highly qualified specialists capable of solving information security problems in peacetime, but will also prepare personnel for emergency situations and ensuring the stability of the information space in wartime.

Today, more than 100 Ukrainian higher education institutions train specialists in information security, focusing mainly on its technical aspects, such as technical information protection, cybersecurity and cryptography. However, this orientation ignores the humanitarian dimension of the issue, which is critical in the context of modern hybrid threats and information warfare.

Educational programs in Ukraine practically do not cover the socio-humanitarian aspects of information security. The lack of disciplines such as information psychology, sociology of information processes, legal regulation of the information space, strategic communications and information risk management creates a gap in the training of specialists capable of working at the intersection of technical and humanitarian knowledge. This limits the state's capabilities in countering disinformation, manipulation, protecting national identity and building social resilience.

Modern challenges emphasize the need for a comprehensive approach to training specialists in information security. Educational programs should integrate technical, legal, sociological, political, psychological, and information-analytical aspects. This approach will allow training versatile specialists who are able to work with modern technologies, analyze social processes, form effective communication strategies, and manage information risks. To achieve this goal, it is necessary to develop new educational standards that will ensure the training of versatile specialists in the field of information security. The creation of specialties that integrate technical and humanitarian knowledge should become a priority of state educational policy. This will allow Ukraine to effectively respond to national and global challenges in the information sphere and strengthen its resilience to the threats of information aggression.

In the conditions of martial law in Ukraine, the formation of information culture and legal awareness of society takes on special importance [5]. This is not only an important element of national resilience, but also a tool for countering information aggression and disinformation, which are actively used in modern conflicts. Information culture should be based on the principles of transparency, respect for individual rights and freedoms, as well as the inevitability of punishment for their violation.

Unfortunately, in many countries, including Ukraine, the mass media mostly act as passive fixers of events. The media often confine themselves to reporting on the facts of crimes, including human rights violations, rather than focusing on their disclosure and punishment. This reinforces public pessimism and distrust of legal institutions, which is critical in wartime, when trust in the state and its ability to provide justice is an important factor in social mobilization. The media play a special role in this context. Their task is not only to cover the facts of violations, but also to demonstrate the inevitability of punishment for crimes. Shifting the emphasis from sensational reporting of crimes to publicizing the facts of their disclosure and punishment of the guilty creates a sense of justice and faith in the legal system among citizens. This also has a preventive effect, contributing to the improvement of legal culture, especially among young people, who are most vulnerable to information influence.

The formation of a new information culture in wartime requires a special approach. Information culture should become an element of the general culture of society, which includes knowledge of the laws of the functioning of the information space, the ability to adapt to information flows and critically evaluate the information received. These skills are necessary to ensure the information stability of society and counteract manipulations and fakes that are actively spread by the enemy to undermine morale and unity.

The war also demonstrates the importance of the social responsibility of the media. In times of information and military threats, the media should become not only a source of news, but also a tool for raising legal awareness and strengthening social stability. Dissemination of information about the punishment of war criminals, the effectiveness of the legal system, as well as about heroic deeds and achievements in restoring justice should become the basis of the media strategy.

Thus, in the modern information society, especially in conditions of martial law, the formation of information culture is not just a challenge, but also a necessity. This is a process that requires the integration of knowledge about the information space, the legal aspects of its functioning, as well as the ability to think critically and navigate complex information flows. Such approaches will not only increase the level of information and legal culture, but will also contribute to the overall stability of society in the face of the threats of the modern world. The

formation of information culture is gaining strategic importance, since not only the resilience of society to destructive information flows depends on it, but also the ability to mobilize, support national identity and preserve moral and ethical values. Technologies aimed at the development of information culture should popularize traditional moral, ethical and spiritual values inherent in Ukrainian society, actively counteracting harmful and artificially imposed influences that spread through modern information and communication technologies. Today, Ukraine is faced with massive information aggression, which uses destructive information flows to demoralize the population, split society and increase chaos. In this context, state and public institutions should play a key role, creating and distributing reasoned and constructive content that can withstand information threats. Such content should expose the harmfulness of propaganda, debunk myths, promote positive ideas based on the values of patriotism, social responsibility, unity and justice.

Social technologies for the formation of information culture should use the historical experience of Ukraine, modern achievements and cultural uniqueness as a basis for strengthening public consciousness. Examples of heroism, selflessness and the struggle for freedom of the Ukrainian people can and should become the foundation for creating a strong and stable information environment. This will contribute to the formation of faith in the national legal system, respect for moral and ethical norms and intolerance for destructive manifestations among citizens. At the same time, the implementation of such technologies is complicated by the democratic principle of freedom of speech, which is inviolable in peacetime, but in wartime requires rethinking. The state must define clear boundaries between freedom of speech and permissiveness, which leads to the spread of anti-spiritual and anti-moral values. This issue becomes especially relevant against the background of information expansion through domestic media and the Internet, which sometimes become a platform for the propaganda of hostile narratives.

Conclusions. In conditions of martial law, the use of social technologies in the processes of public management of the information security of society becomes critically important for countering destructive information influences that threaten national unity, traditional values, and social stability. Such technologies allow to reduce the risks of social decomposition under the influence of manipulation and propaganda, to increase the level of social immunity to such influences, to preserve the cultural and national identity of Ukrainian society, and also to minimize the negative impact of information and communication technologies on public consciousness. Thus, social technologies in managing the processes of formation and provision of information security are an important tool in protecting Ukrainian society. Their comprehensive implementation will allow not only to reduce the threats of destructive influence, but also to strengthen social unity, support traditional values and create a stable information environment capable of withstanding the challenges of modernity.

References:

1. On the Information Security Doctrine of Ukraine. Decree of the President of Ukraine dated 25.02.2017 No. 47/2017 URL: https://zakon.rada.gov.ua/go/47/2017 (accessed: 03.11.2024)
2. Averyanova N.M. Hybrid war: Russian-Ukrainian confrontation. Young Scientist, 2017. No. 3 (43). P. 30-34
3. Politanskyi V. S. Information Society in Ukraine: From Its Origin to the Present. Scien-

tific Bulletin of the Uzhhorod National University. 2017. Issue 42. P. 16–22.
4. Prodanyuk R. I. Information security in a sociological context: to the formulation of the problem. Grani: scientific and theoretical almanac. 2018. Vol. 21. No. 4. P. 84–90.
5. Torichny V.O. Information security of the state in the conditions of the information society: state and administrative aspect: Monograph. Kharkiv: NUCZU, 2020. 274 p.
6. Disinformation and Russia's war of aggression against Ukraine. OECD: website. URL: https://www.oecd.org/ukraine-hub/policy-responses/disinformation-and-russia-s-war-of-aggression-against-ukraine-37186bde/ (accessed: 07.11.2024).