ISSN 2786-5533 (Online)

DOI: 10.52363/passa-2024.2-33
UDC:004.9:004.056.5:378.147:355.45(477)

Lasukov O. Head of the Department of Electronic Communications and Cybersecurity at the Cherkasy Institute of Fire Safety named after the Heroes of Chernobyl, National University of Civil Protection of Ukraine
ORCID: 0009-0006-4780-1202

DIGITAL TRANSFORMATION OF THE PERSONNEL TRAINING SYSTEM TO ENSURE CYBERSECURITY OF SECURITY AND DEFENSE SECTOR AGENCIES

The article is devoted to the study of digital transformation processes in the system of personnel training for cybersecurity in the security and defense sector bodies of Ukraine under conditions of hybrid threats and full-scale aggression. The relevance of the study is determined by the critical need for qualified cybersecurity specialists capable of countering modern cyber threats, and the necessity to modernize educational processes in accordance with the challenges of the digital era. The purpose of the work is to comprehensively analyze the features of digitalization of the educational process for training cybersecurity specialists and to substantiate strategic directions for improving the professional education system in the security sector. The article provides a theoretical analysis of the conceptual foundations of digital transformation of education, examines the specifics of implementing blended learning and online platforms in the personnel training system, and considers the challenges of integrating digital technologies into the educational process of specialized educational institutions. Particular attention is paid to analyzing the experience of adapting educational programs to martial law conditions and distance learning formats. The research results indicate the need for a systematic approach to education digitalization, which involves not only technological updates but also transformation of the methodological foundations of the educational process, development of digital competencies of teaching staff, and creation of modern infrastructure for practical training of specialists. The study conclusions contain recommendations regarding strategic priorities for developing the cybersecurity personnel training system in the context of Ukraine's Euro-Atlantic integration.

Keywords:*digital transformation, cybersecurity, personnel training, security and defense sector, blended learning, online platforms, digital competencies, distance education, virtual laboratories, professional education.*

Statement of the problem. The current stage of development of the information society is characterized by an unprecedented growth of cyber threats, which pose a serious challenge to the national security of the state. In the conditions of a full-scale war, cyberspace has turned into a separate sphere

of confrontation, where information operations are conducted, attacks are carried out on critical infrastructure, control systems and communications of security and defense sector bodies. This situation makes the problem of training highly qualified cybersecurity specialists capable of effectively countering modern threats in the digital space more urgent. At the same time, the traditional system of vocational education is not flexible enough to respond promptly to dynamic changes like cyber threats and the rapid development of information technologies.

The system of training personnel to ensure cybersecurity faces a double challenge: on the one hand, the need to adapt to the new realities of wartime, when traditional forms of organizing the educational process may be limited or impossible, and on the other hand, the need to modernize the methodological foundations of training in accordance with the requirements of the digital era. The digital transformation of education is not a simple technological update, but involves complex changes in approaches to the formation of professional competencies, the organization of the educational process and interaction between participants in educational activities. The problem is that digitalization processes are often implemented in a fragmented manner, without a systematic approach and strategic vision, which reduces their effectiveness and does not allow for the full use of the potential of modern technologies to improve the quality of specialist training.

Analysis of recent research and publications. The issue of digitalization of the educational process and training of cybersecurity specialists is in the focus of attention of many domestic researchers. The theoretical foundations of the digital transformation of education are considered in works devoted to the modernization of higher education in the information society [1]. The issues of training personnel for the security and defense sector are studied in the context of reforming the national security system and adapting to NATO standards [2]. The features of the formation of competencies in the field of cybersecurity are highlighted in works that analyze the challenges of hybrid warfare and cyber threats to critical infrastructure [3]. At the same time, a systematic analysis of the digital transformation of the educational process of training cybersecurity specialists for security sector bodies, taking into account the specifics of functioning under martial law, remains insufficiently researched, which justifies the relevance of this scientific research.

Formulation of the article's objectives. The purpose of the article is a comprehensive analysis of the features of the digital transformation of the personnel training system to ensure cybersecurity of the security and defense sector bodies of Ukraine and to substantiate strategic directions for improving the educational process in conditions of hybrid threats and martial law.

Presentation of the main research material. The current stage of society's development is characterized by the rapid spread of digital technologies in all spheres of life, which necessitates a rethinking of traditional approaches to training specialists, especially in the field of national security. The digital transformation of the education system is not a simple technological update,

but a complex process of fundamental changes in the methodology of training, organizational forms of educational activities and approaches to the formation of professional competencies. In conditions of full-scale war and increasing cyber threats, the issue of training qualified personnel to ensure cybersecurity of security and defense sector bodies is becoming critical for the national security of Ukraine.

The theoretical understanding of the digital transformation of education is based on the concept of lifelong learning, which involves constant updating of knowledge and competencies in accordance with the dynamic changes in the technological environment. A feature of the training of cybersecurity specialists is the need to combine fundamental theoretical knowledge with practical skills in working with modern information systems and information protection technologies. The traditional model of education, focused on the transfer of established knowledge, is not effective enough in conditions where technologies are updated faster than the training of one generation of specialists. This requires a review not only of the content of educational programs, but also of the forms of organization of the educational process, creating conditions for the formation of the ability to self-study and adapt to new challenges.

The methodological basis for studying the digital transformation of education is a systemic approach, which allows us to consider the processes of modernization of personnel training as an interconnected set of changes in various components of the educational system. System transformation involves simultaneous changes in the target orientations of education, the content of curricula, methods and forms of training, material and technical support, and the human resource potential of the teaching staff. Fragmented implementation of individual digital tools without a comprehensive restructuring of the entire system does not give the expected effect and may even lead to a decrease in the quality of the educational process. It is important to understand that digitalization should become an organic part of the overall development strategy of an educational organization, and not a separate project or initiative.

The conceptual principles of digitalization of education in the security and defense sector should take into account the specifics of the activities of the relevant bodies and the special requirements for the training of specialists. Unlike the civilian sphere, where digital transformation is carried out mainly in an evolutionary way, the security sector requires more dynamic adaptation to new challenges. The events of recent years have demonstrated the critical importance of cyberspace as a separate sphere of confrontation, which requires the training of a new type of specialists capable of operating in conditions of uncertainty and rapid change in the operational environment [4]. This necessitates the formation of flexible educational models that can respond promptly to changes in the nature of threats and technological capabilities. It should be taken into account that cyber threats are constantly evolving, new methods of attacks and vulnerabilities of information systems appear, which makes it impossible to create static educational programs with fixed content.

An important theoretical aspect is the understanding of digital competence as an integral characteristic of a cybersecurity specialist. Digital competence is not limited to technical skills in working with computer systems, but also includes the ability to critically evaluate information, understand the principles of digital technology functioning, anticipate potential vulnerabilities in information systems, and develop effective protection strategies. The formation of such a comprehensive competence is possible only in the context of integration of theoretical training with practical activities, which actualizes the role of simulation technologies and virtual laboratories in the process of personnel training [5]. Simulation environments allow to reproduce realistic scenarios of cyber incidents, providing an opportunity to practice decision-making under stress and time constraints, which is critically important for the formation of professional qualities of cybersecurity specialists.

Methodologically important is also the issue of the ratio of standardization and individualization in the process of digital transformation of education. On the one hand, training specialists for security sector bodies requires compliance with uniform standards and requirements, which ensures the compatibility of actions of different units and the possibility of interaction within integrated security systems. On the other hand, digitalization opens up opportunities for individualization of educational trajectories, taking into account the specific needs of individual categories of students, adapting the pace and depth of studying the material to individual characteristics. Finding the optimal balance between these requirements is one of the key tasks of modernizing the personnel training system. Individualization of training is especially relevant for advanced training and retraining of existing specialists who have different levels of basic training and practical work experience.

Theoretical analysis shows that the successful digital transformation of education is impossible without changes in the corporate culture of educational institutions and the organizational environment. The introduction of digital technologies often encounters resistance from the teaching staff, who are used to working in traditional formats. Overcoming this resistance requires not only technical training of teachers but also the formation of a new understanding of the role of a teacher in a digital educational environment. The teacher ceases to be the only source of knowledge and is transformed into a facilitator of the educational process, who helps students navigate the information space and form their own competencies [6]. This change in the role of the teacher requires significant efforts from the management of educational institutions, the creation of motivation systems, and support for teaching staff in the process of mastering new work methods.

Special attention is paid to the methodological analysis of blended learning as a key model for digitalizing the educational process. Blended learning combines traditional forms of classroom work with the use of digital technologies and distance formats, which allows optimizing the educational process and increasing its efficiency. Blended learning is of particular importance for training cybersecurity specialists, as it allows for access to

relevant educational materials and practical tasks regardless of the location of the students. In conditions of martial law, when part of the staff may be in different regions of the country or perform official duties, the possibility of distance learning becomes critically important for maintaining the continuity of the educational process. At the same time, it is important to understand that blended learning is not simply a mechanical combination of face-to-face and distance formats, but requires careful pedagogical design that takes into account the specifics of different forms of educational interaction.

Methodological significance also lies in the analysis of international experience in digitalization of training of cybersecurity specialists. NATO member states have accumulated significant experience in creating professional education systems that provide training of highly qualified specialists to counter cyber threats. A feature of these systems is the close integration of educational institutions with practical units, the involvement of current practitioners in teaching, and the widespread use of international educational platforms and experience exchange programs. Adapting this experience to Ukrainian realities, taking into account the specifics of the domestic security system, is an important task for ensuring Ukraine's Euro-Atlantic integration. In particular, the experience of creating specialized centers of competence in cybersecurity that combine the functions of training, scientific research, and practical support of operational units deserves attention.

Theoretical analysis also reveals the need to consider the digital transformation of education in the context of broader processes of reforming the security and defense sector. Modernization of the personnel training system cannot occur in isolation from changes in organizational structures, operating procedures, and technical equipment of security agencies. Graduates of educational institutions should come to organizations that are ready to effectively use their competencies, have the appropriate technical infrastructure and organizational culture. This requires consistency between educational and personnel policies, strategic planning for the development of human capital in the security sector. An important element of such consistency is the establishment of effective feedback between educational institutions and organizations that order personnel, which allows for prompt adjustment of the content and methods of training in accordance with the real needs of practice.

Conceptually important is also the understanding of the ethical and legal aspects of digitalization of education in the field of cybersecurity. Training of specialists involves familiarization with technologies that can potentially be used for unauthorized access to information systems or cyberattacks. This requires special attention to the formation of professional ethics and legal culture of future specialists, ensuring proper control over the use of educational materials and tools. Curriculums should include not only technical disciplines, but also courses on legal and ethical aspects of information security, which form a responsible attitude to professional activity [7].

Methodological analysis of the digital transformation of education also involves considering the issue of assessing learning outcomes in a digital

environment. Traditional forms of certification, focused on testing knowledge of theoretical material, are insufficient to assess the formation of complex cybersecurity competencies. New approaches to assessment are needed, based on the analysis of students' practical activities in simulation environments, the implementation of complex project tasks, and the demonstration of the ability to solve non-standard situations. Digital technologies open up opportunities for automated monitoring of learning activities, the accumulation of data on the progress of each student, which allows for a more objective and comprehensive assessment of learning outcomes.

The practical implementation of the digital transformation of the training system for cybersecurity of security and defense sector bodies in Ukraine is characterized by a number of specific features, caused by both the general challenges of education modernization and the special conditions of the functioning of the security system during a full-scale war. An analysis of existing practice indicates significant achievements in the implementation of digital technologies in the educational process, while at the same time identifying systemic problems and barriers, overcoming which requires a strategic approach and coordination of efforts of various entities.

A key direction of digitalization of cybersecurity training is the implementation of online educational platforms that provide remote access to educational materials, interactive interaction between teachers and students, automated knowledge testing and monitoring of educational progress. The experience of recent years shows that the most effective are platforms that integrate various forms of educational activities in a single digital environment. This allows students to access video lectures, text materials, practical tasks, participate in forums and discussions, and take tests without switching between different systems. At the same time, the creation and content of such platforms requires significant resources, both financial and human, which poses a serious challenge for educational institutions in the security sector.

The possibility of organizing the educational process in a distance format becomes particularly relevant in conditions of martial law. The beginning of a full-scale invasion demonstrated the critical importance of the readiness of educational institutions to quickly transition to remote forms of work. Those institutions that already had a developed digital infrastructure and experience in using online technologies were able to quickly adapt to the new conditions and ensure the continuity of the educational process. In contrast, organizations that relied exclusively on traditional forms of education faced serious difficulties in organizing educational activities [8]. This experience emphasizes the need to consider digitalization not as an optional addition to traditional methods, but as a critically important component of ensuring the sustainability and adaptability of the training system.

An analysis of the practice of implementing blended learning in the cybersecurity training system reveals different models of combining face-to-face and distance learning components. The most common model is one in

which students learn theoretical material independently through online platforms, and classroom sessions are devoted to practical exercises, discussion of complex issues, work on cases and projects. This model allows for more effective use of time spent directly interacting with the teacher, focusing on those aspects of learning that require personal contact and teamwork. At the same time, the implementation of this model requires a high level of self-discipline and motivation of students, as well as high-quality content for independent study.

An important element of the digitalization of practical training is the creation of specialized virtual laboratories and training grounds for practicing cyber incident response skills. Such environments allow you to simulate realistic cyber attack scenarios, provide an opportunity to practice in threat diagnostics, selection and implementation of countermeasures without risk to real information systems. The advantage of virtual laboratories is the possibility of multiple repetition of exercises, variation of scenario parameters, work at an individual pace. In addition, virtual environments allow you to simulate situations that would be dangerous or impossible to recreate in real conditions, in particular large-scale cyber attacks on critical infrastructure [9].

The practical implementation of digital transformation also involves the development of remote mentoring and consulting systems. Modern communication technologies allow for effective interaction between experienced practitioners and students of educational programs regardless of their geographical location. This is especially relevant for involving specialists in the educational process who are unable to regularly attend an educational institution due to their official duties. Video conferences, specialized chats, and document collaboration systems create opportunities for the transfer of practical experience and consultations on specific cybersecurity issues in real time.

Analysis of the experience of implementing digital technologies also reveals a number of problems and challenges that require a systematic solution. One of the most significant is the problem of digital inequality, when different categories of students have unequal access to technical means and Internet connections of the required quality. This can lead to a deterioration in the quality of education for certain categories of students, create barriers to their full participation in the educational process. Solving this problem requires not only technical measures, but also organizational solutions, in particular, providing the opportunity to use the technical means of the educational institution, creating local access points in different regions.

A significant challenge is also ensuring the cybersecurity of the educational process itself. The use of digital platforms and online tools creates additional risks of unauthorized access to educational materials, personal data of students, and assessment results. Special attention is required to protect information in specialized educational environments where students work with real cybersecurity tools and technologies. Reliable authentication systems,

data encryption, and user activity monitoring are required, which requires additional investments and qualified technical personnel [10].

Practical experience also shows the importance of developing digital competencies of teaching staff. Even the most advanced technical solutions will not produce the expected effect if teachers do not have the necessary skills to use them or do not understand the pedagogical capabilities of digital tools. This requires the organization of systematic training and advanced training of teaching staff, the creation of conditions for the exchange of experience, the support of pedagogical experiments and innovations. It is also important to form the motivation of teachers to master new technologies, which can be achieved through a system of incentives, recognition of achievements, and the creation of a community of practitioners.

The issue of integrating the Ukrainian system of training cybersecurity specialists into the international educational space deserves special attention. Digital technologies significantly simplify the organization of international cooperation, participation in joint training programs, and exchange of experience with colleagues from other countries. Ukraine is actively developing partnerships with educational institutions in NATO countries, which involves mutual recognition of qualifications, participation in academic mobility programs, and joint research projects. Digitalization of education facilitates such cooperation, allowing Ukrainian students to access courses from leading international experts, participate in international training exercises and simulations, and exchange experience with colleagues from different countries [11].

Analysis of the practice of digital transformation also reveals the need to create effective mechanisms for monitoring and assessing the quality of the educational process in a digital environment. Digital platforms generate large amounts of data on students' learning activities, which can be used to analyze the effectiveness of various teaching methods, identify difficulties encountered by students, and timely adjust educational programs. At the same time, the use of such analytical capabilities requires appropriate competencies from managers and teachers, understanding the principles of working with educational analytics, and compliance with ethical norms for the use of personal data.

The practical implementation of the digital transformation of cybersecurity training is also closely related to the issue of financial support. The creation of a modern digital infrastructure, the development of high-quality electronic content, the purchase of licenses for specialized software, and the support of the technical functioning of systems require significant financial resources. In conditions of limited budget funding, educational institutions are forced to look for additional sources of resources, in particular through international grants, partnership programs with the private sector, and the provision of paid educational services. It is important to ensure the sustainability of funding, since digital infrastructure requires not only initial investments, but also ongoing costs for support, updating, and development [12].

The experience of recent years also demonstrates the importance of flexibility and adaptability of educational programs in the field of cybersecurity. The dynamic nature of cyber threats, the emergence of new attack and protection technologies require rapid updating of training content. Digital platforms create technical opportunities for quickly making changes to training materials, adding new modules, and updating practical tasks. At the same time, it is important to provide organizational mechanisms for such updating, including procedures for reviewing and approving changes, involving practical experts in the development of new content, and testing innovative approaches before their widespread implementation.

Conclusions. The conducted study of the digital transformation of the personnel training system to ensure cybersecurity of security and defense sector bodies allows us to formulate a number of important conclusions. The digitalization of education is a fundamental transformation of the entire system of specialist training, which includes changes in the methodology of training, organizational forms of educational activities and the content of curricula. The systemic nature of this transformation requires coordination of efforts of various entities and strategic planning.

Theoretical analysis has shown that effective digital transformation is based on a combination of the concept of continuous learning, a systemic approach and a competency paradigm. The specificity of training cybersecurity specialists lies in the need to develop not only technical skills, but also the ability to quickly adapt, think critically and make decisions in conditions of uncertainty. The formation of such competencies is possible provided that different forms of learning are integrated and close ties are ensured between educational institutions and organizations that hire personnel.

The analysis of practical experience revealed both significant achievements and systemic problems. Among the positive results are the implementation of online platforms, the development of blended learning and the creation of virtual laboratories. The experience of organizing training under martial law has demonstrated the critical importance of digital infrastructure. At the same time, problems of insufficient digital competences of teachers, limited financial resources and digital inequality among students were identified.

The study confirmed that blended learning is the optimal model for training cybersecurity professionals. Effective implementation of this model requires careful pedagogical design and the creation of high-quality electronic content. The results indicate the need to strengthen the development of digital competencies of teaching staff and involve practitioners in teaching activities.

Strategic priorities should be the creation of an integrated digital educational environment, the development of specialized centers of competence, and the deepening of international cooperation in the context of Ukraine's Euro-Atlantic integration. The implementation of these priorities requires the formation of an appropriate regulatory framework, financing mechanisms, and the coordination of educational policy with the overall strategy for reforming the security and defense sector.

References:

1. Bykov V. Yu. Digital transformation of education and science in the context of the COVID-19 pandemic: new challenges and opportunities. Information technologies and learning tools. 2020. Vol. 80. No. 6. Pp. 1-12.
2. Gorbulin V. P., Dodonov O. G., Lande D. V. Information operations and social security: threats, countermeasures, modeling. Kyiv: Intertechnology, 2019. 280 p.
3. Petrov V. V., Kovalenko L. O. Training of cybersecurity specialists in the context of hybrid threats to national security. Bulletin of the National Academy of Public Administration. 2021. No. 2. Pp. 89-95.
4. Solovyov S. G. Cyberspace as a sphere of armed confrontation: experience, problems, prospects. Strategic Priorities. 2022. No. 1-2. Pp. 134-143.
5. Marushchak A. I., Ovcharuk O. V. Formation of digital competence of specialists in the security and defense sector: challenges and opportunities. Information and Law. 2021. No. 3(38). Pp. 67-76.
6. Kremen V. G. Education and science in Ukraine – innovative aspects. Strategy. Implementation. Results. Kyiv: Gramota, 2020. 464 p.
7. Baranov O. A. Legal aspects of cybersecurity: international and national dimensions. Information Law. 2020. No. 1. Pp. 12-24.
8. Lyashenko O. I., Protsenko O. S. Distance learning in the system of training security sector personnel under martial law: challenges and solutions. Collection of scientific works of the National Academy of the State Border Guard Service of Ukraine. 2022. No. 3. P. 156-168.
9. Korchenko O. G., Kazmirchuk S. V. Virtual laboratories in the system of training cybersecurity specialists. Information Protection. 2021. Vol. 23. No. 2. Pp. 78-86.
10. Bogush V. M., Yudin O. K. Information Security of the State: Textbook. Kyiv: MK-Press, 2020. 368 p.
11. Sitsinska M. V. International cooperation of Ukraine in the field of cybersecurity in the context of Euro-Atlantic integration. Strategic priorities. 2021. No. 3-4. P. 201-210.
12. Kudilina O. V., Savchenko S. V. Financial support for the digitalization of education in Ukraine: status and prospects. Finances of Ukraine. 2021. No. 10. pp. 93-107.

Received: 03.11.2024
Accepted: 17.11.2024
Published: 23.12.2024