Training specialists in cybersecurity and information protection as a component of the national strategy under the condition of hybrid warfare[1]

Larysa Prodanova[1,*,†], Oksana Zakharova[1,†], Oksana Yakusheva[1,†] and Nelia Nagaichuk[1,†1]

Cherkasy State Technological University of Cherkasy, Shevchenko blvd. 460, 18006 Cherkasy, Ukraine

Abstract

The paper assesses the current state of the system of training specialists in cybersecurity and information protection in Ukraine. A set of factors of an international, national, and technological nature that confirm the need for a radical restructuring of the system of training specialists in information protection and cybersecurity is substantiated. A ranking of higher education institutions in Ukraine is compiled based on the total number of students enrolled in specialty 125 "Cybersecurity and Information Protection". The ways to adapting the national system of training cybersecurity and information protection specialists to the challenges of hybrid warfare are determined.

Keywords

national security system, forms of cybersecurity breaches, consequences of cyber incidents, state policy of education, higher education system, digital sustainability, critical infrastructure

1. Introduction

Modern challenges to the national security of Ukraine in the context of russia's hybrid war against Ukraine make the problem of training highly qualified specialists in information protection and cybersecurity relevant. Information and communication technologies have become not only the basis for the functioning of the state and society, but also a battlefield where cyber threats are taking on the character of a strategic weapon.

Hybrid warfare is characterized by the integrated use of traditional military means along with cyberattacks on critical infrastructure, state institutions, and the private sector. In such conditions, the national security system needs specialists who are able not only to respond to existing threats, but also to predict new challenges in cyberspace.

The problem of staffing in the cybersecurity sector is becoming particularly acute, as traditional approaches to training specialists lag behind the dynamics of cyberthreats. At the same time, Ukraine's integration into European and Euro-Atlantic security structures requires bringing national standards for training specialists into line with international requirements.

The purpose of the paper consists in assessing the current state of the system of training specialists in cybersecurity and information protection in Ukraine and determining ways to adapt it to the challenges of hybrid warfare.

2. Results

The need for a radical restructuring of the system of training specialists in information protection and cybersecurity is confirmed by a complex of factors of an international, national, and technological nature.

The international context demonstrates the critical importance of the problem. According to The World Economic Forum "Global Risks Report 2025", cyber threats are among the ten most likely

[1]*SMICS'25: Workshop on Cryptology and Data Security, October 16-18, 2025, Lviv, Ukraine*

[*] Corresponding author.

[†] These authors contributed equally.

l.prodanova@chdtu.edu.ua (L. Prodanova); o.zakharova@chdtu.edu.ua (O. Zakharova); o.yakusheva14@gmail.com (O. Yakusheva); nagaichuk_n@ukr.net (N. Nagaichuk)

0000-0003-4280-6013 (L. Prodanova); 0000-0001-5793-6203 (O. Zakharova); 0000-0002-4849-0323 (O. Yakusheva); 0000-0002-2014-3151 (N. Nagaichuk)

global risks of the next decade [1] (Table 1). The International Information System Security Certification Consortium (ISC)² Cybersecurity Workforce Study records a 4.76 million specialists global shortage of cybersecurity professionals, which undermines the ability of both national security systems and business structures to adequately respond to the evolution of cyber threats and provide an adequate level of cyber protection [2]. The Cybersecurity Capacity Maturity Model for Nations, developed by the Global Cyber Security Capacity Centre at Oxford University, confirms the direct correlation between the level of training (development of knowledge and capabilities) in the field of cybersecurity and the cybersecurity capability of the state [3].

Table 1

Global Risks Ranked by Severity (Short-Term and Long-Term) based on the World Economic Forum's Global Risks Perception Surveys (2023-2025)

	2023		2024		2025	
	2 years	10 years	2 years	10 years	2 years	10 years
1	Cost-of-living crisis	Failure to mitigate climate change	Misinfor-mation and disinfor-mation	Extreme weather events	Misinfor-mation and disinfor-mation	Extreme weather events
2	Natural disasters and extreme weather events	Failure of climate-change adaptation	Extreme weather events	Critical change to Earth systems	Extreme weather events	Biodiversity loss and ecosystem collapse
3	Geoeconomic confrontation	Natural disasters and extreme weather events	Societal polarization	Biodiversity loss and ecosystem collapse	State-based armed conflict	Critical change to Earth systems
4	Failure to mitigate climate change	Biodiversity loss and ecosystem collapse	Cyber insecurity	Natural resource shortages	Societal polarization	Natural resources shortages
5	Erosion of social cohesion and societal polarization	Large-scale involuntary migration	Interstate armed conflict	Misinfor-mation and disinfor-mation	Cyber espionage and warfare	Misinfor-mation and disinfor-mation
6	Large-scale environmental damage incidents	Natural resource crises	Lack of economic opportunity	Adverse outcomes of AI technologies	Pollution	Adverse outcomes of AI technologies
7	Failure of climate change adaptation	Erosion of social cohesion and societal polarization	Inflation	Involuntary migration	Inequality	Inequality

8	Widespread cybercrime and cyber insecurity	Widespread cybercrime and cyber insecurity	Involuntary migration	Cyber insecurity	Involuntary migration or displacement	Societal polarization
9	Natural resource crises	Geoeconomic confrontation	Economic downturn	Societal polarization	Geoeconomic confrontation	Cyber espionage and warfare
10	Large-scale involuntary migration	Large-scale environmental damage incidents	Pollution	Pollution	Erosion of human rights and/or civic freedoms	Pollution

The national legislation of Ukraine forms the legal basis for strengthening cybersecurity training. The Cybersecurity Strategy of Ukraine (for 2021-2025) identifies human resources as one of the strategic priorities [4]. The Law of Ukraine "On Amendments to Certain Laws of Ukraine on Information Protection and Cybersecurity of State Information Resources and Critical Information Infrastructure Objects" (No. 4336-IX of March 27, 2025) [5], which is currently one of the key laws in the field of cybersecurity, also affects to a certain extent the requirements for professional training of specialists. The law provides for the following: the introduction of full-time positions for cyber protection specialists in government agencies and critical infrastructure facilities – this is a direct requirement for the availability of qualified specialists; the creation and operation of a national cyber incident response system – this requires specialists not only to have knowledge in the field of defense, but also skills in investigating cyberattacks, restoring systems, and exchanging information about threats. Thus, Law No. 4336-IX actually establishes specific, albeit general, requirements for the staff and functionality of specialists, which in turn stimulates the development of their professional training.

Technological challenges cause a radical change in professional competencies. Technological developments and accelerating digital transformation create new challenges for ensuring cyber security. Cybersecurity breaches in modern conditions can take the following forms: identity fraud, data theft, ransomware attacks, cyberattacks on critical infrastructure, or phishing campaigns, etc. [6, 7]. According to the research by Cyber Management Alliance Ltd.: IoT malware attacks grew by 107% by the end of 2024; ransomware affected 59% of respondents; phishing attacks have increased dramatically by 4151% since the public release of ChatGPT (late 2022); about 8 million DDoS attacks were recorded in the first half of 2024; the average total cost of data breaches in 2024 was $4.88 million [8]. The most common consequences of cyber incidents and cybersecurity breaches in business are: loss of trust in technology, disruption of operations (including supply chain or partner ecosystem), loss of reputation, negative impact on talent recruitment and retention, loss of revenue, loss of customer trust and negative impact on brand, theft of intellectual property, regulatory fines, falling stock prices, termination of funding for a strategic initiative, deterioration of competitive positions [6, 9]. The emergence of new types of threats, including AI-driven attacks and potential threats from quantum computing, requires fundamentally new approaches to training specialists.

As of September 6, 2025, 58 higher education institutions in Ukraine provide training for cybersecurity and information protection specialists (specialty 125 "Cybersecurity and Information Protection" and 125 "Cybersecurity") at various educational levels (bachelor's, master's and postgraduate studies). This number indicates a significant development of the education system in this field and an increase in its relevance in modern conditions. Table 2 shows the rating of higher education institutions in Ukraine (Top 10) that have the largest number of students (totally at all the education levels and forms of study). According to the results of the analysis of data from the Register of Educational Activity Subjects of the Unified State Electronic Database on Education of Ukraine [10], it was found that the total number of higher education applicants in the analyzed specialty in

Ukrainian higher education institutions as of September 6, 2025 is 10,214 people, including 8,672 people at the first (bachelor's) level, 1,285 at the second (master's) level, and 257 at the third (educational and scientific, PhD) level.

To assess the quality of specialist training, it is advisable to use a comprehensive approach that includes academic indicators, professional training results, and evaluation of the educational program and environment [11]. According to the Scientific and Methodological Center for Higher and Professional Pre-Higher Education of the Ministry of Education and Science of Ukraine, the average percentage of correct answers on the Unified State Qualification Exam (USQE) among applicants for the first (bachelor's) level of higher education in specialty 125 "Cybersecurity", whose educational program ends in the 2023-2024 academic year, is 41.97% (the threshold score is set at 28 correct answers out of 93 test items). The specific share of students who did not pass the exam is 7.99% of the total number of those who took it [12]. The best results among the universities from the TOP-10, according to the exam results, were shown by students from Taras Shevchenko National University of Kyiv – 100.0% of those who took the exam, National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute" – 99.2%, and State University of Intelligent Technologies and Telecommunications – 97.6%.

Table 2

Top 10 higher education institutions of Ukraine by the number of students in the specialty 125 "Cybersecurity and Information Protection" and 125 "Cybersecurity", as of 06.09.2025 (persons, full-time/part-time forms of education)

Institutions rating		Educational degrees			
		Bachelor	Master	Doctor of Philosophy	Total
1	Lviv Polytechnic National University	873 / 81	127 / 8	42 / 3	1134
2	State University of Information and Communication Technology	582 / 3	154 / 0	35 / 4	778
3	State Non-Commercial Company «State University «Kyiv Aviation Institute»	548 / 51	95 / 10	10 / 3	717
4	National Technical University of Ukraine «Igor Sikorsky Kyiv Polytechnic Institute»	410 / 38	52 / 10	11 / 7	528
5	Kharkiv National University of Radio Electronics	258 / 11	75 / 19	25 / 5	393
6	Vinnytsia National Technical University	320/ 0	51 / 0	11 / 1	383
7	State University of Trade and Economics	294/ 22	34 / 7	-	357
8	Dnipro University of Technology	257 / 31	50 / 5	5 / 0	348
9	Taras Shevchenko National University of Kyiv	253 / 0	46 / 0	13 / 0	312
10	State University of Intelligent Technologies and Telecommunications	148 / 32	30 / 15	10 / 4	239

According to the State Service for Special Communications and Information Protection (State Special Communications), another important stage of reforming the specialized education and

training system in the field of cybersecurity in Ukraine was completed in 2024. The reform of specialized education was based on the creation of the National Cybersecurity Qualification Framework, the introduction of a system of professional standards, and the creation of a network of independent qualification centers in Ukraine. This approach takes into account the best global practices, is based on the experience of the European Qualifications Framework and the American Strategic Educational Initiative in the field of cybersecurity (in general, as of the end of 2024, specialists from the State Service for Special Communications developed, and the National Qualifications Agency approved changes to the State Classifier of Professions, which allowed adding 27 new professions in the field of cybersecurity and information security) [13].

Adapting the system of training cybersecurity specialists to the challenges of hybrid warfare requires a comprehensive approach that includes the modernization of educational programs, the development of infrastructure, and the formation of new mechanisms for interaction with the practical field. The primary task is to revise educational standards taking into account the specifics of hybrid threats. This involves including modules in the curriculum on analyzing wartime cyberattacks, protecting critical infrastructure, countering disinformation campaigns, and ensuring system resilience under stressful conditions. Particular attention should be paid to studying the experience of countering russian cyberattacks and analyzing the best global practices for ensuring cyber resilience in conflict situations. The training system requires a radical strengthening of the practical component and the development of practice-oriented training. This approach includes the creation of cyber training grounds to simulate real attack scenarios, conducting regular cyber training with the participation of students, developing cyber incident simulators, and introducing mandatory internships in key government institutions and private companies. Close integration of military and civilian components of specialist training is important in the context of hybrid warfare. This involves the creation of joint educational programs between civilian higher education institutions and military educational institutions, the development of courses on the basics of military cybersecurity for civilian specialists and, conversely, in-depth study of civilian aspects of cyber defense for military specialists. Adaptation also requires bringing the Ukrainian training system into line with NATO and EU standards. This includes the implementation of international educational standards, the development of academic mobility programs, the involvement of international experts in teaching, and the creation of joint educational programs with universities in partner countries. The system requires the creation of a modern digital training infrastructure and educational ecosystem, including cloud cybersecurity laboratories, virtual simulators for practicing incident response skills, and online platforms for distance learning with a high level of security. The development of distance learning opportunities to ensure the continuity of the educational process under martial law is particularly relevant. Hybrid warfare requires the formation of a system of continuous professional development and constant adaptation of the knowledge and skills of specialists to new realities. This necessitates the creation of a lifelong learning system that includes advanced training programs, certification courses, professional conferences and workshops. Effective training of specialists is impossible without a powerful scientific base, which involves the creation of specialized scientific centers for the study of cyber threats, the development of grant programs for young researchers, and the formation of consortiums of universities and businesses for joint R&D projects in the field of cybersecurity [14,15]. It is critically important to build partnerships with business, the IT industry, and cybersecurity companies: creating industry councils at higher education institutions, developing dual education programs, introducing a system of corporate scholarships and grants, and conducting joint projects and hackathons.

3. Conclusion

The modern challenges of hybrid warfare are radically changing the requirements for professional training of cybersecurity specialists, which necessitates the need for a comprehensive reform of the existing system of training specialists in the field of cybersecurity and information protection. Traditional approaches to training do not meet the dynamics of cyberthreats and the specifics of countering hybrid attacks.

The scale of cybersecurity training in Ukraine is significant: 58 higher education institutions train over 10,000 specialists at all educational levels. This demonstrates that the state and educational community are aware of the critical importance of staffing national cybersecurity.

Effective response to modern challenges in the field of cybersecurity in Ukraine requires a comprehensive transformation of the system of training specialists, which should be based on a practical orientation, constant adaptation to threats, and close cooperation between the state, education, and business. This will not only overcome the personnel shortage, but also ensure the country's stability in the conditions of hybrid warfare.

Declaration on Generative AI

During the preparation of this work, the authors used ChatGPT to: translate certain text fragments into English, perform grammar and spelling checks, and paraphrase or reword content. After using these tools, the authors carefully reviewed and edited the content as needed and take full responsibility for the publication's content.

References

[1] World Economic Forum. The Global Risks Report 2025. URL: https://www.weforum.org/publications/global-risks-report-2025/

[2] ISC2 Cybersecurity Workforce Study. Global Cybersecurity Workforce Prepares for an AI-Driven World. 2024. URL: https://edge.sitecorecloud.io/internationf173-xmc4e73-prodbc0f-9660/media/Project/ISC2/Main/Media/documents/research/2024-ISC2-WFS.pdf.

[3] Cybersecurity Capacity Maturity Model for Nations Global Cyber Security Capacity Centre. URL: https://gcscc.ox.ac.uk/the-cmm

[4] Decree of the President of Ukraine No. 447/2021 of August 26, 2021. On the decision of the National Security and Defense Council of Ukraine of May 14, 2021 "On the Cybersecurity Strategy of Ukraine." URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text

[5] Law of Ukraine No. 4336-IX of March 27, 2025. On amendments to certain laws of Ukraine regarding information protection and cyber protection of state information resources and critical information infrastructure facilities. URL: https://zakon.rada.gov.ua/laws/show/4336-20#Text

[6] Statista/ Cyber Crime & Security. URL: https://www.statista.com/markets/424/topic/1065/cyber-crime-security/#overview

[7] Savchuk, S. O. State policy on combating cybercrime : thesis. ... PhD (public administration): 25.00.05. Zhytomyr, 2024. 160 p.

[8] Top 10 Biggest Cyber Attacks of 2024 & 25 Other Attacks to Know About! URL: https://www.cm-alliance.com/cybersecurity-blog/top-10-biggest-cyber-attacks-of-2024-25-other-attacks-to-know-about

[9] Deloitte. Global Future of Cyber Survey, 4th Edition. 2024. URL: https://www.deloitte.com/content/dam/assets-shared/docs/services/risk-advisory/2024/deloitte-global-future-of-cyber-survey-4th-edition-the-promise-of-cyber.pdf

[10] Unified state electronic database on education of Ukraine. Register of educational activity subjects. URL: https://registry.edbo.gov.ua/search/

[11] Zakharova, O., Prodanova, L. (2023). The Potential of Higher Education in Ukraine in the Preparation of Competitive IT Specialists for the Post-War Recovery of the Country's Economy. In: Faure, E., Danchenko, O., Bondarenko, M., Tryus, Y., Bazilo, C., Zaspa, G. (eds). Information Technology for Education, Science, and Technics. ITEST 2022. Lecture Notes on Data Engineering and Communications Technologies, vol 178. Springer, Cham. Pp. 582–595.

[12] Ministry of Education and Science of Ukraine. Scientific and Methodological Center of HPHE. Report on the results of passing the state qualification exam in specialty 124 "Cybersecurity". Date: April 25, 2024. Kyiv, 2024. URL: https://nmc-vfpo.com/wp-content/uploads/2024/11/zvit-125.pdf

[13] Qualification Center for Information Technologies and and Cybersecurity State Research Institute of Cybersecurity Technologies. Another stage of reforming the cybersecurity training system has been completed: the National Qualifications Agency approved 7 more professional standards. URL: https://qc.csi.cip.gov.ua/uk/posts/7

[14] Plaksiuk, O., Prodanova, L., Yakusheva, O., Nagaichuk, N., Prikhno, I., & Jakubčinová, M. (2023). Human capital as a factor of socio-economic development of the state: the main trends of the Slovak Republic. Financial and Credit Activity Problems of Theory and Practice, 5(52), 283–298. https://doi.org/10.55643/fcaptp.5.52.2023.4150

[15] Yakushev, O., Moisieienko, L., Yakusheva, O., Prodanova, L., Plaksiuk, O., & Chepurda, L. (2024). Socio-economic sustainability of the tourism sector enterprises in the context of the COVID-19 pandemic: global and ukrainian dimensions. Financial & Credit Activity: Problems of Theory & Practice, 5(58). 484-499. DOI: https://doi.org/10.55643/fcaptp.5.58.2024.4377

[16] Nagaichuk, N., Tretyak, N., & Tkalenko, O. (2019). Insurance in the cyber risk management system of an enterprise in the conditions of the digital economy. Financial Space, 33(1).