NaSTech

JOURNAL OF NATURAL SCIENCES AND TECHNOLOGIES
2025, 4(1), pp. 371-379, DOI: 10.5281/zenodo.16478574

FORMATION OF A CYBER-RESILIENT ECOSYSTEM OF HIGHER EDUCATION: AN INTERDISCIPLINARY AND PRACTICAL APPROACH

Murad OMAROV[1], Maryna YEVDOKYMENKO[1]

[1]Faculty of Infocommunications, Kharkiv National University of Radio Electronics, Ukraine

ABSTRACT

In the context of growing global cyber threats, universities are increasingly seen as key actors in strengthening cyber resilience at the national and international levels. The article examines the strategic role of higher education institutions in the formation of a safe digital environment through educational, research and institutional activities. The review began with an analysis of the current threat landscape, including hybrid attacks, artificial intelligence challenges, and a shortage of qualified specialists. Further, the concept of the university as a multifunctional agent – educational, innovative and normative – was formed.

The paper carried out a comparative analysis of the best practices of the world's leading universities (including MIT, KU Leuven, NUS), which made it possible to identify common approaches: integration of cybersecurity into programs not only of IT specialties, creation of cyber laboratories, participation in international projects and the introduction of interdisciplinary training. Based on the results of the study, a set of practical recommendations for universities seeking to strengthen their own cyber resilience is formulated. We are talking about updating training programs, using simulation platforms, building partnerships with businesses, and implementing internal digital security policies. The article offers universities a roadmap for the transition from traditional educational institutions to institutions – centers of digital resilience.

Keywords: cybersecurity, higher education, cyber resilience, cyber labs, academic policy, digital skills.

1. INTRODUCTION

In the modern world, cybersecurity has long ceased to be just a matter for IT specialists – it has become a key element of national security, digital sovereignty, and social stability. With the development of digital technologies, every country faces new challenges that threaten its economy, political system, infrastructure, and citizens. The problem of cyber threats has become especially acute in the context of war, geopolitical instability, and hybrid aggression, which use cyberspace as another theater of war. According to ENISA, in 2023 alone, the number of high-risk cyberattacks increased by more than 40%. Critical infrastructure, the public sector, healthcare, telecommunications, and energy remain the most vulnerable.

Modern threats are becoming more and more sophisticated: the use of artificial intelligence to create phishing attacks, deepfake videos, and bypass detection systems is no longer a fantasy, but a reality. The proliferation of cloud services, the Internet of Things (IoT), and remote work leads to an increase in potential access points for attackers. But the technical side is only part of the problem. The human factor remains one of the main vulnerabilities: a low level of cyber hygiene, lack of awareness and a lack of qualified specialists lead to catastrophic consequences. In addition, attacks are increasingly accompanied by elements of psychological influence, disinformation and undermining trust in state institutions.

In this context, universities play a special role. They are becoming not only centers of knowledge, but also important players in the formation of a cyber-resilient society. It is universities that have the potential to train a new generation of specialists who are able to respond effectively to modern threats. In addition, they can be platforms for conducting interdisciplinary research, creating innovative solutions, and embedding digital culture in society. Their mission is especially relevant in the context of global instability, where rapid adaptation to new challenges is necessary. Universities can act as centers of resilience, cooperating with the state, business, and international partners. That is why it is important to reflect on their strategic role in strengthening cyber resilience. This article aims to analyze the key threats in cybersecurity and outline ways in which universities can contribute to overcoming them. Both educational and organizational approaches to improving digital security will be considered. Particular attention will be paid to practice-oriented learning, international cooperation and awareness-raising among students and the general public. By investing in education today, we are building the foundation for a secure digital tomorrow.

2. MODERN CYBER THREAT LANDSCAPE

In recent years, the global community has seen a rapid increase in the complexity and scale of cyber threats. According to the official *ENISA Threat Landscape 2023* report [1], the number of high-risk cyberattacks has increased by more than 40% compared to the previous year. critical infrastructure, government information systems, telecommunications operators, healthcare, and financial institutions.

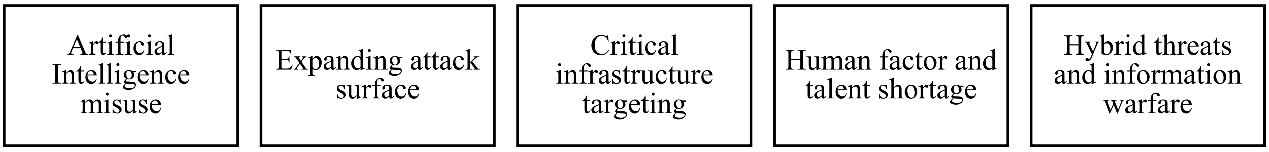
Critical infrastructure is the focus of both state APT groups and cybercriminal groups that use attacks on energy, transport, or water supply facilities as a tool of pressure. At the same time, healthcare facilities are increasingly under ransomware attacks, which not only disrupts their operations but also poses a threat to patients' lives. The telecommunications sector is also vulnerable: attackers can paralyze or intercept information flows that ensure the functioning of other sectors. It is also threatening that in many cases the infrastructure is based on outdated management systems that do not meet modern security requirements.

Particular attention should be paid to the latest challenges related to technological innovations, which are both drivers of digital progress and sources of new risks. Thus, the activities of APT groups that carry out multi-layered, long-term attacks with a high level of disguise and persistence have intensified. During 2023, numerous cases of artificial intelligence were recorded to generate personalized phishing messages, create video and audio deepfake content, and bypass systems multi-level authentication and undermining trust in digital services. In addition, the adversary uses adversarial AI – methods of creating malicious inputs that mislead machine learning models, including attack detection systems, recommendation algorithms, or automated log analysis services.

A number of new attack vectors are associated with the spread of cloud services, the Internet of Things (IoT), and the transition to remote work. A large number of connected devices with insufficient protection (for example, household cameras, sensors, modules in enterprise management systems) significantly expands the attack surface. Misconfiguration of cloud storage, open APIs, and vulnerabilities in containerized environments lead to leakage of sensitive information and compromise of systems. In the context of a hybrid war, the risk of using cloud infrastructure for malware, covert data exchange, or information sabotage remains relevant.

A separate block of threats is attacks that exploit the human factor. Phishing and social engineering remain the most common methods of initiating attacks. The use of psychological influence, imitation of authority, urgency or panic allow attackers to gain unauthorized access to systems, even if there is technical protection. In 2023, there is an increase in the integration of such methods with disinformation campaigns aimed at undermining trust in state institutions, the media, or increasing public alarm. Such hybrid attacks become a tool not only for cybercrime, but also for information warfare, which requires not only a technical, but also an interdisciplinary approach to counteraction.

A significant challenge to the resilience of the digital ecosystem is the lack of skilled personnel. *The ISC^2* estimates that the global shortage of cybersecurity professionals exceeds 4 million [2]. This creates a situation where even high-tech companies are not able to provide an adequate level of monitoring and response to incidents. The centers do not have time to train personnel that would meet modern challenges, especially under martial law and limited access to the material and technical base. The lack of sufficient staff in the public sector, in regional communities and small businesses makes critical facilities even more vulnerable. Figure 1 presents some of the most critical modern cybersecurity challenges [1-4].



Artificial Intelligence misuse

Expanding attack surface

Critical infrastructure targeting

Human factor and talent shortage

Hybrid threats and information warfare

Figure 1. The most critical modern challenges in cyber security

Thus, the modern cyber threat landscape is determined by a high level of complexity, unpredictability, and integration with information and psychological influences. Countering these threats requires not only technological solutions, but also a systematic approach to the training of specialists, intersectoral coordination and the development of digital culture among the general population. It is in this context that the strategic role of universities acquires special importance.

3. UNIVERSITIES AS DRIVERS OF CYBER RESILIENCE

In the context of the rapid evolution of cyber threats and the digital transformation of society, universities are increasingly seen not only as educational institutions, but as strategic centers for strengthening cyber resilience. Their potential covers several interrelated functions: educational, research and institutional (Table 1). The realization of this potential can ensure the long-term readiness of the state and society to counter the latest cyber threats.

Table 1. Functional areas of universities' contribution to cyber resilience

Function	Sub-functions / Directions of implementation
1. Education (Formation of the Workforce)	- Educational program updates: AI in cyber threats, Cloud Security, OSINT, DevSecOps
	- Practice-oriented training: cyber labs, CTF, case study
	- Certification: CompTIA, ISC², ISO/IEC 27001
	- Interdisciplinary tracks: technical, legal, ethical and social aspects of cybersecurity
2. Research (Innovation & Knowledge Creation)	- Applied research: adaptive protection, Zero Trust, ML/AI security
	- Interdisciplinary projects: cyberethics, disinformation, digital rights
	- Participation in programs: Horizon Europe, Erasmus+, NATO SPS
	- Competence centers and startup incubators
3. Institutional (Digital Culture & Public Engagement)	- Promotion of digital hygiene among all students and employees
	- Educational initiatives for non-professionals and the public
	- Consulting the state and business, participation in policy-making
	- Building partnerships with public, private and international structures

3.1. Educational role: training a new generation of specialists

Education is the foundation for shaping a sustainable digital future. Universities play a key role in providing high-quality and up-to-date training for cybersecurity specialists. Modern challenges require updating the content of educational programs, including the introduction of topics such as artificial intelligence in cybersecurity, cloud security, DevSecOps, OSINT, threat analysis, and incident management. It is also important to cultivate students' ability to think critically, be ethically responsible, and adapt to new technological paradigms.

In addition, universities can create conditions for practice-oriented learning: cyber laboratories, Capture the Flag (CTF), simulation trainings and participation in international competitions. This allows students not only to gain theoretical knowledge, but also to develop applied skills in conditions close to real cyber incidents. Participation in certification programs (e.g. CompTIA, EC-Council, ISC²) as part of the educational process increases the competitiveness of graduates in the labor market.

It is especially important that universities not only train engineers, but also develop interdisciplinary educational trajectories: specialists with legal, social, political and ethical understanding of cyberspace problems. This will allow us to form a sustainable ecosystem of specialists who are able to act not only at the level of technology, but also at the level of strategies, policies and management decisions.

3.2. Research function: innovations, interdisciplinary solutions

Universities also play a critical role in developing innovative approaches to cyber resilience. University research is a source of new methods for detecting threats, analyzing vulnerabilities, building adaptive protection systems and automating response processes. Active involvement in scientific projects at the national and international levels (including Horizon Europe, Erasmus+, Jean Monnet, NATO SPS) allows Ukrainian universities to integrate into global research initiatives.

Of particular value is an interdisciplinary approach to research. Effective cybersecurity requires not only technical, but also legal, social, and behavioral tools. Universities can provide a platform for cooperation between the faculties of computer science, law, psychology, sociology, international relations. This opens up new opportunities for studying topics such as countering disinformation, cyberethics, digital rights, personal data protection, etc.

The role of universities in the creation of research laboratories and centers of competence is also growing. Such structures not only conduct applied research, but also interact with business and government agencies, developing solutions for the real sector. They become platforms for technology transfer, the implementation of pilot projects, and the training of startups in the field of cybersecurity.

3.3. Institutional function: the role of universities in the formation of digital culture

In addition to educational and scientific functions, universities fulfill an important institutional mission in shaping digital culture and raising cyber awareness in society. As large educational ecosystems, they are able to reach wide audiences: students of all specialties, teachers, administrative staff, representatives of local communities. Universities should play the role of conductors of the principles of digital hygiene, responsible use of ICT and building trust in the digital environment.

Disseminating basic knowledge about cybersecurity among non-specialists is an important step towards increasing the overall cyber resilience of society. This can be implemented through courses for all specialties, open trainings, awareness campaigns, online self-study platforms. Such initiatives are especially important in regions at risk, in particular in conditions of war and enemy cyber activity.

Universities can also participate in national digital transformation programs, work as expert platforms for the development of policies, standards and regulatory documents. Through partnerships with government agencies, business and international structures, universities strengthen their own institutional capacity, enhancing the effect at the level of society.

4. KEY AREAS OF ACTION OF UNIVERSITIES

When outlining the strategic role of universities in strengthening cyber resilience, it is necessary to move from a general awareness of potential to specific tools and implementation mechanisms. Today, universities are faced with the task not only to adapt to changes in the cyber environment, but also to actively influence its development by introducing innovative practices into the educational, research and public space. In this context, it is advisable to identify six key areas of action that ensure the systemic strengthening of cyber resilience at the institutional and cross-sectoral levels.

4.1. Directed updating of the content of training

Universities should reconsider the traditional logic of curriculum formation, based on the needs of the modern digital environment. It is not only about introducing new disciplines, but about changing the approach: instead of focusing on individual technologies, we need to teach systems thinking in the face of constant threat dynamics. A combination of knowledge about the interaction of artificial intelligence and attack techniques (for example, phishing generation with LLM), understanding the principles of "security by design" (DevSecOps), critical assessment of cloud architectures in terms of risks, as well as the practical application of OSINT to identify open attack vectors is relevant.

Integration with European competency frameworks, such as ENISA CSF or ECCC recommendations [2-4], allows for compatibility of training with pan-European standards and simplifies the recognition of graduates' qualifications on the international market.

4.2. Development of the infrastructure for practical threat modeling

To bridge the gap between academic training and real security requirements, the implementation of virtualized cyber incident simulation systems is critically needed. This includes creating lab environments for attack replication, configuring network architectures with simulated vulnerabilities, analyzing event logs, responding to intrusions, and recovering from attacks.

Platforms such as CYBER RANGES, Haaukins, TryHackMe, Hack The Box, RangeForce, IMMUNE (by EC-Council), or in-house university training stands can be used to form a comprehensive vision of cyber threats. These environments allow you to create customized scenarios with simulation of attacks on realistic infrastructures, covering both technical vectors (vulnerability exploitation, lateral movement, privilege escalation) and managerial aspects of response (incident management, reporting, consequence analysis).

This allows students to develop skills not only in the field of technical protection, but also in the areas of threat behavior profiling, digital forensics, incident response, business impact assessment, and teamwork in the SOC/Blue Team/Red Team format.

Such platforms also integrate systems for automatic skills assessment, progress tracking, and certification, making them an effective tool for non-formal education in the field of cybersecurity.

4.3. Formation of new profiles through intersectoral integration

Unlike classical approaches to training a "universal IT specialist", modern challenges require deep profiling. Universities can become platforms for training highly specialized specialists: information security auditors, DevSecOps architects, digital forensics specialists, or supply chain risk analysts.

To do this, it is important to involve not only technical departments, but also to build joint tracks with law, economics, sociology, philosophy – forming a new quality of training that corresponds to the complexity of real threats. It is through intersectoral interaction that the ability to assess risks in the context of law, privacy policy, reputational consequences, regulatory compliance, etc. arises.

4.4. Impact on the digital behavior of society

Cyber resilience as a phenomenon is formed not only at the level of expert communities, but also at the level of citizens' digital habits. Universities have a unique opportunity to work with young people – future workers, entrepreneurs, officials, educators – even before they enter professional roles.

Training modules on digital hygiene, dissemination of knowledge about the basics of information security, trainings on resistance to fake information, recognition of social engineering – all this forms a culture of responsible use of digital services. Public lectures, educational podcasts, open resources on the Internet can significantly enhance the effect of influence in the long run.

4.5. Platform for Interaction with External Stakeholders

One of the key roles of universities is to mediate knowledge and practice. In this context, educational institutions can act as integrators of interaction between students, employers, government agencies and international organizations. The introduction of dual education programs, academic hackathons with the participation of companies, and joint projects with business makes it possible to bring education closer to the real conditions of the industry.

In addition, universities can contribute to the development of a talent pool for the public sector, especially in the context of the war and post-war period, when the need for cyber defense specialists for authorities, regional administrations, social institutions, etc. is growing.

4.6. Inclusion in the international educational and security architecture

International educational programs and academic networks provide universities with the opportunity not only to access advanced methodologies, but also to promote their own models of cyber resilience at the level of global expert discourse. Participation in Erasmus+, Horizon Europe, Jean Monnet projects and cyber education initiatives ITU, ENISA, NATO SPS allows you to exchange knowledge, jointly build educational products, standards, and training modules.

Moreover, international integration strengthens the academic mobility of students and teachers, opens up access to grant programs, and also creates conditions for positioning the university as a center of competence in the region. In modern conditions, such network formations are the source of resilience, adaptability and innovative breakthrough in the field of cybersecurity [5-11] .

Thus, given the strategic role of universities in the formation of cyber resilience through updating the content of education, developing practical learning, interdisciplinary integration, promoting digital culture and cooperation with industry, there is a need for these areas to become applied and systemic, it is important to study and compare existing international experience. The world's leading universities already have established models for implementing innovations in the field of cybersecurity – both at the level of educational programs and through research and partnerships. That is why it is advisable to carry out a comparative analysis of these approaches in order to identify effective practices that can serve as a reference or source for adaptation in any national or regional context. Below is an analytical overview of key cybersecurity education strategies implemented at seven of the world's leading universities.

5. COMPARATIVE ANALYSIS OF CYBER EDUCATION MODELS IN THE WORLD'S LEADING UNIVERSITIES

For the implementation of the comparative analysis, seven universities representing the leading educational and scientific systems in the USA, Europe and Asia were selected. The following key criteria were used to form a representative sample of universities within the framework of the comparative analysis:

1. Global academic leadership in the field of IT and cybersecurity, which is confirmed by ratings (QS, THE), alumni authority, research publications, and participation in global technology trends.
2. Availability of specialized cybersecurity centers and applied laboratories, including CERT, SOC, cryptographic and interfaculty initiatives, providing a practical component of training.
3. Integration of interdisciplinary approaches into educational programs, namely a combination of technical training with modules on law, ethics, digital policy, risk management, which form a holistic vision of security.
4. Active participation in the development of state, international and industrial initiatives in the field of cyber resilience, i.e. cooperation with government agencies, regulators, standards organizations (for example, NIST, ENISA, Horizon Europe, NSA CAE, GovTech).

According to these criteria, the following universities were selected:

1. The Massachusetts Institute of Technology (MIT) is one of the global leaders in engineering education, artificial intelligence research, and digital technologies. Its Internet Policy Research Initiative at the CSAIL laboratory is actively developing digital security strategies and researching the risks associated with AI infrastructures. The MIT xPRO cybersecurity program combines a deep technical base with cases from the practice of leading companies.
2. Carnegie Mellon University (CMU) is a recognized cybersecurity training center in the United States, where the CERT Division at the Software Engineering Institute operates. It was here that the first incident response center was established in 1988. CMU also has a strong scientific base through CyLab and Heinz College, and its cybermanagement programs are accredited by the CISA Security Agency and the U.S. National Security Agency (NSA).
3. Stanford University is a university that presents an interdisciplinary approach to cybersecurity, bringing engineering, law, ethics, and policy together within the activities of the Stanford Cyber Policy Center.

Cybersecurity programs actively cooperate with Silicon Valley companies and are focused on developing next-generation digital policies.

4. KU Leuven (Belgium) is a leading technical university in Europe, known for the COSIC (Computer Security and Industrial Cryptography) Center. The university is actively involved in the initiatives of the European Cybersecurity Agency (ENISA), the EU Cybersecurity Competence Center (ECCC) and participates in the standardization of cryptographic algorithms within the framework of NIST projects.
5. Technische Universität München (TUM) is one of the best universities in Germany with a strong engineering school that implements IoT, SCADA, and critical infrastructure security projects in cooperation with Siemens, SAP, BMW. Cybersecurity programs here combine technical depth with industrial applications and are part of the Horizon Europe clusters.
6. University of Oxford (Great Britain) is a representative of the British model of interdisciplinary cyber education. The Centre for Doctoral Training in Cyber Security operates here, which brings together research in the field of digital threats, policy, user behavior, disinformation and risk management.
7. National University of Singapore (NUS) is one of the most influential universities in Asia, working closely with the government agencies of Singapore (GovTech, Cyber Security Agency of Singapore). NUS implements national training cyber training, has specialized cyber laboratories (Cybersecurity Lab, CISO Lab), and actively develops the areas of digital forensics and critical infrastructure security.

Thus, the selected universities not only have a high academic reputation, but also play a system-forming role in the development of the global cybersecurity market through education, research, and political interaction. This allows us to consider their models as applied and universal for adaptation in other educational ecosystems.

A comparative analysis of the leading universities in the USA, Europe and Asia, presented in Table 1, showed the presence of common approaches to the development of cyber education, which can serve as guidelines for countries that form or modernize their own educational systems. Leading universities demonstrate a range of best practices that combine scientific, educational and institutional activities into a strategy for sustainable strengthening of digital security.

Firstly, one of the determining factors for successful training of personnel is the presence of powerful research centers on cybersecurity. Structures such as CSAIL at MIT, CyLab at Carnegie Mellon or COSIC at KU Leuven combine deep fundamental research with applied solutions for the real sector. They act not only as centers of knowledge, but also as platforms for interaction with government agencies, business and international organizations.

Secondly, universities are actively implementing interdisciplinary learning models that cover not only technical knowledge, but also aspects of digital law, ethics, risk management, information policy, and even social psychology. This approach has been implemented, in particular, at the University of Oxford and Stanford University, where students analyze threats at the intersection of technology, politics and humanities.

A third characteristic practice is to create an environment for hands-on learning, including working in real-world security labs, using attack simulations (CTFs), simulating incidents, and training at cyber ranges. In particular, the National University of Singapore (NUS) and the Technical University of Munich (TUM) have created learning environments in collaboration with government agencies and tech giants, enabling students to gain not only knowledge but also combat experience in responding to threats.

It is also worth noting the active participation of universities in state and international initiatives. KU Leuven is a partner of ENISA and ECCC, Carnegie Mellon is a key CISA and NSA center in the United States, and UK universities are involved in government projects through EPSRC. This provides a direct link between teaching, research, and real-world government tasks in the field of security.

Another important component is certification support for training: leading universities integrate international certificates (CISSP, OSCP, CompTIA Security+) into their courses, which contributes to the better integration of graduates into the global labor market. In addition, the training of future specialists includes thematic areas of digital human rights, the fight against disinformation, privacy protection, and the ethics of the use of artificial intelligence.

Table 2. Comparative table of the world's leading universities according to the criteria of cyber educational excellence

University	Global academic leadership in IT and cybersecurity	Availability of specialized research centers	Interdisciplinary integration into educational programs	Participation in state and international initiatives
Massachusetts Institute of Technology (MIT), США	It is one of the top 3 universities in the world in the field of computer science; Computer Science and Artificial Intelligence Laboratory (CSAIL)	Internet Policy Research Initiative, IPRI, (CSAIL)	Educational programs combine engineering, digital policy, risk management	Cooperation with the US government, projects in the field of AI security, cloud services, digital regulation
Carnegie Mellon University (CMU), США	Recognized leader in cybersecurity, especially in software security and threat analysis	Software Engineering Institute and Computer Emergency Response Team (CERT); CyLab Privacy and Security Center	Training courses in digital ethics, government policy, forensics, threat analytics	Cybersecurity and Infrastructure Security Agency, (CISA), участь у програмах National Security Agency (NSA)
Stanford University, США	Ranked in the top 5 universities in the world in terms of impact in IT and security policy	Cyber Policy Center, Stanford Internet Observatory	Programs include digital law, public safety, internet policy, the impact of disinformation	Partnership with US government agencies, consulting on digital security policy
Catholic University of Leuven (KU Leuven), Бельгія	One of the most influential universities in Europe in the field of applied cryptography and security	Computer Security and Industrial Cryptography (COSIC), Centre for IT & IP Law (CiTiP)	Courses include regulatory requirements (e.g., General Data Protection Regulation, GDPR), cryptanalysis, security auditing	Участь у European Cybersecurity Competence Centre (ECCC), співпраця з European Union Agency for Cybersecurity (ENISA)
Technical University of Munich (TUM), Німеччина	Germany's leading technical university with a strong focus on IT systems security	IoT security laboratories together with Siemens, SAP, SCADA test centers	Applications integrate security technologies with digital management and industry standards	Participation in projects of the European Union (Horizon Europe), development of a dual model of education with enterprises
University of Oxford, United Kingdom	It is one of the top 10 universities in the world; Focus on security policy, law and cyber regulation	Centre for Doctoral Training in Cyber Security (CDT), Oxford Internet Institute	Broad combination of technical research with law, ethics, risk analysis	Public funding through the Engineering and Physical Sciences Research Council (EPSRC), collaboration with the UK Government
National University of Singapore (NUS), Сінгапур	Asia's top-ranked university for cybersecurity and digital forensics	Joint Cybersecurity Lab with the Cyber Security Agency, (CSA), Mobile and Industrial Systems Security Research Laboratory	Educational programs combine IT security, state security, digital law	Direct partnership with government agencies: CSA, GovTech, participation in national cyber exercises

6. TRANSFORMATION VECTOR: FROM ANALYSIS TO IMPLEMENTATION

Generalization of international experience and the results of comparative analysis of leading universities shows that cyber resilience is no longer exclusively a subject of technical protection but becomes an institutional characteristic of the educational environment. Universities are turning into strategic players that form not only specialists, but also a holistic digital ecosystem – with their own security culture, research infrastructure, and influence on public policy.

However, effective imitation of best practices requires not just copying models, but adaptation to the local context – taking into account human resources, regulatory environment, level of digital transformation and the specifics of threats [11] . With this in mind, recommendations are given that seek to play an active role in strengthening national and global cyber resilience:

1) *Integrate cybersecurity as a mandatory interdisciplinary component of education*

All students, regardless of major, must have basic training in digital security, media literacy, and digital rights. Cyber hygiene should become part of the general educational environment, not just IT specialties.

2) *Create your own cybersecurity research hubs and labs*

It is advisable for universities to initiate or expand existing centers that allow conducting applied research, attack simulations, and testing of the latest technologies. These can be centers for cyber defense, digital forensics, cyber law, etc.

3) *Introduce practice-oriented training through simulation platforms*

It is recommended to use modern training grounds such as CYBER RANGES, Haaukins or create your own training environments for CTF, real attack scenarios, incident response. It builds skills of quick thinking, team interaction, and realistic understanding of threats.

4) *Actively participate in international initiatives, projects and partnerships*

Universities should join the Erasmus+, Horizon Europe, Digital Europe, Jean Monnet programs, as well as initiate their own projects with the participation of international experts, the private sector, and regulators. This strengthens trust and opens up access to funding and the latest practices.

5) *Update educational programs in line with European and global frameworks*

For example, according to the ENISA Cybersecurity Skills Framework, ECCC Competence Framework or NICE Framework (USA). This will allow graduates to be competitive in the global market and reduce the gap between academic and practical training.

6) *Include certification modules in the educational process*

Universities can collaborate with international certification organizations (EC-Council, (ISC)^2, Offensive Security, etc.) to include certificates as an elective or part of the core program. This will increase the value of graduates to the labor market.

7) *Form communities of cyber enthusiasts, student clubs and hackathons*

Encouraging student activity in the format of cyber clubs, participation in national and international CTF competitions, mini-grants for research – this creates a dynamic culture around cybersecurity at the university.

8) *Conduct regular trainings and seminars for teachers and administration*

Cybersecurity should become a culture within the institution. To do this, it is important to ensure awareness and continuous professional development of teachers, technical staff and managers.

9) *Collaborate with government agencies and the private sector*

It is important to build ties with government agencies on cybersecurity, CERT centers, business, and banking institutions. This allows you to ensure the relevance of training, internships and employment of graduates.

10) *Develop a university cybersecurity policy*

The university itself should be an example of a cyber-resilient institution: have secure access policies, incident monitoring tools, response, and staff training. It builds trust and demonstrates leadership.

7. CONCLUSION

Thus, the article presents the results of a study in the field of strategic development of cyber resilience with the participation of higher education institutions. The modern landscape of cyber threats is analyzed, taking into account the latest challenges – the increase in the complexity of attacks, the emergence of hybrid vectors, the activation of APT groups, as well as the role of social engineering and disinformation. cultural functions in the field of digital security.

A classification of the main areas of action of universities is proposed, which includes the updating of educational programs taking into account current topics (in particular, artificial intelligence, OSINT, DevSecOps), the development of a practical component with the help of cyber laboratories and training grounds (for example, CYBER RANGES, Haaukins), as well as an interdisciplinary approach to the training of specialists. The best international practices are highlighted on the basis of a comparative analysis of ten leading universities in the world involved in the formation of the global agenda in the field of cybersecurity.

As a result, a set of recommendations has been developed for universities that aim to strengthen their role in the digital transformation of society. In particular, the feasibility of integrating basic digital literacy for all students, creating research hubs, participating in international projects, as well as implementing internal cybersecurity policies is substantiated. The model of a cyber-resilient university as a subject that forms not only educational results, but also social and technological impact is outlined.

The results of this study can be used for strategic planning of the development of higher education institutions, adaptation of educational programs to modern digital security challenges, as well as as a conceptual basis for further interdisciplinary research in the field of cyber education, regulation and institutional development.

REFERENCES

[1] ENISA. Threat Landscape 2023: Looking back at the major cybersecurity events. European Union Agency for Cybersecurity. 2023. Available at: https://www.enisa.europa.eu

[2] ECCC. The European Cybersecurity Competence Centre and Network. 2023. Available at: https://www.eccc.europa.eu

[3] European Cybersecurity Skills Framework (ECSF). ENISA, 2022. Available at: https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework

[4] NICE Framework. National Initiative for Cybersecurity Education. National Institute of Standards and Technology (NIST), U.S. Department of Commerce. 2020. Available at: https://www.nist.gov/itl/applied-cybersecurity/nice

[5] Howard P., Prince J. Cybersecurity education in universities: best practices and trends. Journal of Cyber Policy. 2022. Vol. 7(1). pp. 85–98.

[6] Tsoumas B., Gritzalis D. Enhancing cyber resilience through academic-industry collaboration: A European perspective. Computers & Security. 2021. Vol. 104. Article 102185.

[7] Wangen G., Snekkenes E. A framework for managing cybersecurity risks in higher education institutions. Computers & Security. 2020. Vol. 92. Article 101752.

[8] Ahmad A., Hadgkiss J., Ruighaver A. Incident response teams—Challenges in supporting the organizational security function. Computers & Security. 2012. Vol. 31(5). pp. 643–652.

[9] Cyber Ranges and Simulation Platforms in Cybersecurity Education. European Cyber Security Organisation (ECSO). 2023. Available at: https://ecs-org.eu

[10] Khan S., Woodward A. Building effective cybersecurity curricula: a global benchmarking study. ACM Transactions on Computing Education. 2020. Vol. 20(3). Article 18. pp. 1–30

[11] Kuzminykh I., Yevdokymenko M., Yeremenko O., Lemeshko O. Increasing Teacher Competence in Cybersecurity Using the EU Security Frameworks. International Journal of Modern Education and Computer Science (IJMECS). 2021. №6. pp. 60–68. DOI: https://doi.org/10.5815/ijmecs.2021.06.06