SOCIETY. INTEGRATION. EDUCATION
Proceedings of the International Scientific Conference. Volume II, May 24th, 2024. 156-166

IMPLEMENTATION OF INTEGRATED CYBER EDUCATION IN EUROPE

Iluta Arbidane
Rezekne Academy of Technologies, Latvia

Hanna Purii
State University of Economics and Technology, Ukraine

Maryna Baida
Kryvyi Rih National University, Ukraine

Oleh Padalka
Ukrainian State University named after Mykhailo Drahomanov, Ukraine

Volodymyr Kulishov
State University of Economics and Technology, Ukraine

Abstract. *The development of partnerships between European countries in the field of cyber education is currently playing a significant role in enhancing countries' cyber potential and comprehensive and systemic counteraction to cyber threats. The research aims to outline the main principles of implementing an integrated cyber education system in European countries. To solve the tasks set, the research uses the following methods: cognition methods to study theoretical foundations of digital education development; comparative and analytical methods to analyze National Cybersecurity Indices and Digital Development Level Indices of the EU and Ukraine; heuristic (expert) methods to formulate the goal, objectives, conclusions and recommendations to form a multilevel generalized model of cyber education; and logical and formalized methods to outline the relevance of cyber education to counter cyber threats.*

The research discusses the issue of digital education, presents National Cybersecurity Indices and Digital Development Level Indices of countries, explores the gaps between National Cybersecurity Indices and Digital Development Level Indices of the EU and Ukraine, and outlines the basic principles of the European Cybersecurity Taxonomy. The main research results are the proposed categorical apparatus of integrated cyber education in European countries and the multi-level generalized model of cyber education to gradually acquire skills and abilities to combat cyber threats introduced from primary school to adult education.

Thus, a comprehensive acquisition of skills to combat cyber threats will help to develop knowledge, skills and abilities of European citizens in the field of cybersecurity and improve the cyber potential of European countries. The introduction of unified regulatory courses and methodological support developed in accordance with the best international practices and harmonized with the terminology of EU and NATO member states will enable effective cooperation in a single information and cyber space.

Keywords: *cyber education, cyber threat counteraction, cybersecurity, digital skills, integrated cyber education system.*

https://doi.org/10.17770/sie2024vol2.7838

Introduction

In today's digital world, cybercrime is a key threat to global economic growth. Raising the culture of citizens' behavior on the Internet, information security, and dissemination of global rules for combating cybercrime can help combat such crimes. At the G20 meetings and those of Ministers of Telecommunications and Information Technology, the issues of information security and critical Internet infrastructure management are regularly discussed.

Digital education

The EU Cybersecurity Strategy published in 2020 *(The Cybersecurity Strategy, 2023)* aims to strengthen Europe's resilience against cyber threats and ensure that all citizens and businesses can fully benefit from trusted services and digital tools.

According to the strategy *(The Cybersecurity Strategy, 2023)*, approximately two-fifths of EU citizens have experienced security problems, and three out of five feel that they cannot protect themselves from cybercrimes. One third of citizens have received fraudulent emails or phone calls, but 83 % have never reported a cybercrime.

According to the strategy *(The Cybersecurity Strategy, 2023)*, the EU Action Plan for Digital Education will raise public awareness of cybersecurity (Digital Education Action Plan, 2020), with children, youth and organizations as the main target group. The strategy also states that cybersecurity skills should be further improved at the EU level through formal education and training (including vocational training), cybersecurity training and cyber exercises to ensure that all Internet users have a global, open, stable and secure cyberspace where everyone can live a safe digital life.

According to a study by the Cybersecurity Education Initiatives in the EU member states *(2022)*, schoolchildren are often seen as early adopters of digital technologies, and they are a critical group to address and ensure that the next generation has the required skills to use online space more safely.

According to Article 10 of the Cybersecurity Law *(The Cybersecurity Act , EU 881 / 2019)*, the European Union Agency for Cybersecurity (ENISA) has the mandate to "raise public awareness of cybersecurity risks and provide guidance on good practices for individual users, targeting citizens, organizations and businesses, including cyber hygiene and cyber literacy". This is demonstrated through initiatives such as the European Cyber Security Month, the European Cybersecurity Challenge, the European Cybersecurity Skills Framework, and the Cybersecurity Higher Education Database (CYBERHEAD). At the level of member states, simply introducing cybersecurity into school curricula can help ensure that young users are more familiar with and aware of the field and requirements of cybersecurity.

However, knowledge of the country's cybersecurity level, its readiness to prevent cyber threats, and its ability to manage cyber incidents and criminal activity in cyberspace are closely related to the country's level of digitalization, which is an important element of strategic analysis and forecasting of economic development. This information, in turn, is used to develop and implement cyber capacity building programs.

National Cybersecurity Indices and Digital Development Levels of Countries

Since 2016, with the support of the Estonian Development Cooperation and Humanitarian Aid, which is managed by a program of the Ministry of Foreign Affairs of Estonia, the E-Governance Academy has developed the National Cybersecurity Index *(NCSI, 2023)*, which provides an assessment of a country's cybersecurity and also enables seeing the criteria and sources on which the assessment is based. Thus, the NCSI is a database with publicly available evidence and a tool for building national cybersecurity capacity.

So, Table 1 presents NCSIs and Digital Development Level Indices (DDLIs) of the EU and Ukraine for 2023.

Table 1 ***NCSIs and DDLIs of the EU and Ukraine for 2023***
(The National Cyber Security Index Ranking, 2023)

Rank	Country	NCSI	DDLI	NCSI-DDLI gap
1.	Belgium	94.81	74.07	20.74
2.	Lithuania	93.51	67.34	26.17
3.	Estonia	93.51	75.59	17.92
4.	Czech Republic	90.91	69.21	21.70
5.	Germany	90.91	80.01	10.90
6.	Romania	89.61	59.84	29.77
7.	Greece	89.61	64.02	25.59
8.	Portugal	89.61	68.46	21.15
10.	Spain	88.31	72.21	16.10
11.	Poland	87.01	65.03	21.98
12.	Austria	85.71	75.76	9.95
13.	Finland	85.71	78.35	7.36
15.	France	84.42	77.29	7.13
16.	Sweden	84.42	81.51	2.91
17.	Denmark	84.42	82.68	1.74
18.	Croatia	83.12	64.63	18.49
19.	Slovakia	83.12	65.44	17.68
20.	Netherlands	83.12	81.86	1.26
23.	Italy	79.22	67.26	11.96

25.	Latvia	75.32	66.23	9.09
26.	Ireland	75.32	75.18	0.14
28.	Bulgaria	74.03	62.06	11.97
37.	Hungary	67.53	64.25	3.28
38.	Slovenia	67.53	69.74	-2.21
41.	Cyprus	66.23	68.83	-2.60
43.	Luxembourg	66.23	78.40	-12.17
76.	Malta	50.65	71.74	-21.09
24.	Ukraine*	75.32	55.96	19.36

Source: (The National Cyber Security Index Ranking, 2023).
** is not a member of the EU*

As can be seen from Table 1, the top 8 positions among the world's countries in terms of cybersecurity are occupied by EU countries, in particular Belgium, Libya, Estonia, Czech Republic, Germany, Romania, Greece, and Portugal. Malta shows the lowest levels of cybersecurity among EU countries.

The DDLIs of the EU and Ukraine in 2023 range from 59.84 to 82.68 points. The following countries have a lower level of digital development: Romania, Greece, Croatia, and Bulgaria. Sweden, Denmark, and the Netherlands showed the highest levels of digital development in 2023 among EU countries.

The analysis of the data in Table 1, namely the gap between the NCSIs and DDLIs of the EU and Ukraine in 2023, reveals a significant gap between the analyzed indicators (Fig. 1).

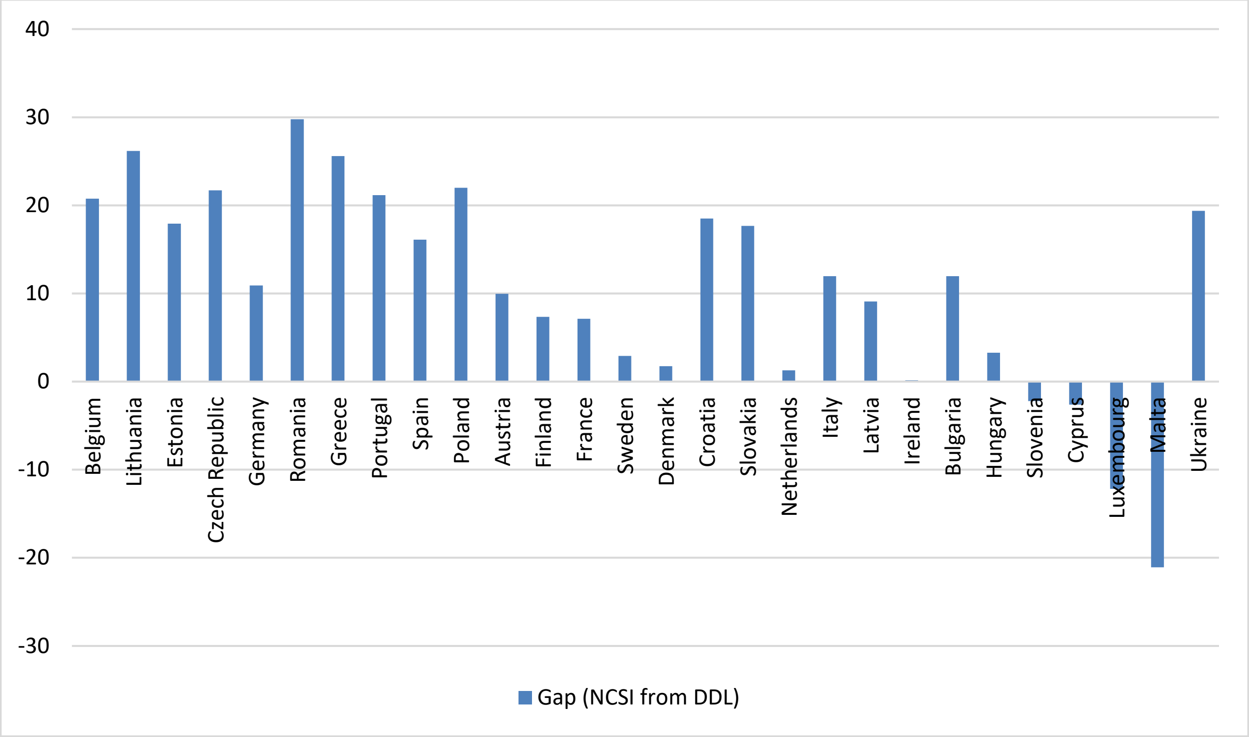


Figure 1 ***The gap between the NCSIs and DDLIs of the EU and Ukraine in 2023***
(Developed by the authors)

Taking into account the results of the deviation between the NCSIs and DDLIs of the EU and Ukraine in 2023, it is recommended to consider the possibility of forming an integrated system of cyber education in Europe.

Promoting decent work and economic growth, building resilient infrastructure, fostering inclusive and sustainable industrialization and promoting innovation, and reducing inequalities within and between countries requires cybersecurity capacity development to strengthen processes, skills, resources, and research and development aimed at enhancing national capabilities *(Arbidane et al., 2021).* Cybersecurity capacity also strengthens the development of collective capabilities and the facilitation of international cooperation and partnerships to effectively respond to cybersecurity-related digital security challenges.

The increase in effective cybersecurity awareness is essential to maintain vigilance among citizens, companies, governments, youth and organizations. With the current shift to digital services, governments need to ensure that all users are aware of the risks they face when conducting digital activities.

The rapid pace of technological development of society and its comprehensive digitalization are driving the growth of technological complexity and the scale of cyber threats in both the private and public sectors of the economy. All of this requires continuous improvement of the training program for professionals in cybersecurity with new hands-on knowledge and skills.

European cybersecurity taxonomy

The European cybersecurity taxonomy includes the following spatial dimensions *(Fovino et al., 2019)*:

- Areas of research and expertise in various aspects of cybersecurity, including human, legal, ethical, and technological areas.

Examples of research areas include theoretical foundations of cybersecurity, warranty, audit and certification, cryptology (cryptography and cryptanalysis), data security and privacy, human aspects, identity management, incident handling and digital forensics, legal aspects, network and distributed systems, security management and leadership, security measurement, software and hardware security engineering, fiduciary management and responsibility.

- The sectoral dimension focuses on various cybersecurity issues and challenges in relation to specific industry sectors, such as energy, transportation, or financial services.

Examples of industrial sectors include audiovisual and media sectors, the chemical sector, defense, digital services and platforms, the energy sector, the financial sector, the food and beverage sector, the state, the health sector, production and supply chains, the nuclear power sector, safety and security, space, telecommunications infrastructure, and transportation.

• The technology dimension, which covers cybersecurity issues for a wide range of key technologies used in the interests of various programs and industry sectors.

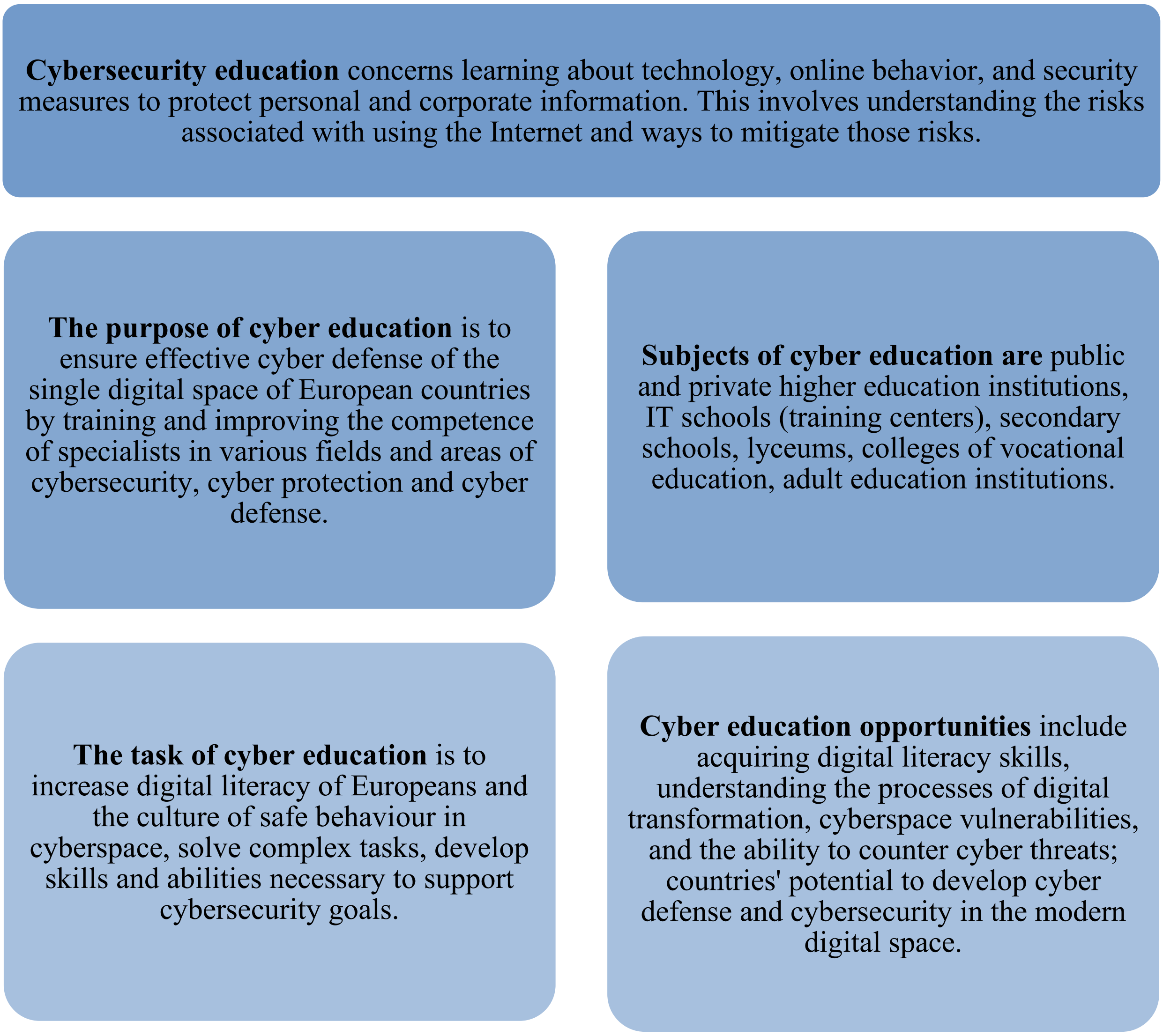
Examples of technological dimension elements include artificial intelligence, big data, blockchain and distributed ledger technology, clouds, edge computing, virtualization, protection of critical infrastructure, disaster resilience and crisis management, hardware technologies (chips, sensors, networks, etc.), high-performance computing, human-machine interface, industrial control systems, information systems, Internet of Things, embedded systems, mobile devices, operating systems, quantum technologies, robotics, satellite systems and applications, automotive systems, and unmanned aerial vehicles (UAVs).

These dimensions cover a wide range of cybersecurity issues *(Lloyd's, 2023)*. Spatial dimensions include all spheres of modern life and require a comprehensive, step-by-step approach for Europe's cyber citizens to acquire both hard and soft skills.

Currently, taking into account the opinions and research of modern scholars, we can state the problem of the lack of a unified methodology in the EU cybersecurity training system for all specialists, both at the public and private levels. The lack of unified guidelines, methodological support for training, and divergent views on the purpose, objectives, and content of cybersecurity training reduces the effectiveness and quality of training of internationally recognized cyber specialists.

Multi-level generalized model of cyber education

In view of the above, in order to develop European cooperation in the field of cyber education, it is necessary to improve the implementation of the relevant framework by studying international experience and generalizing best practices (Fig. 2).



Cybersecurity education concerns learning about technology, online behavior, and security measures to protect personal and corporate information. This involves understanding the risks associated with using the Internet and ways to mitigate those risks.

The purpose of cyber education is to ensure effective cyber defense of the single digital space of European countries by training and improving the competence of specialists in various fields and areas of cybersecurity, cyber protection and cyber defense.

Subjects of cyber education are public and private higher education institutions, IT schools (training centers), secondary schools, lyceums, colleges of vocational education, adult education institutions.

The task of cyber education is to increase digital literacy of Europeans and the culture of safe behaviour in cyberspace, solve complex tasks, develop skills and abilities necessary to support cybersecurity goals.

Cyber education opportunities include acquiring digital literacy skills, understanding the processes of digital transformation, cyberspace vulnerabilities, and the ability to counter cyber threats; countries' potential to develop cyber defense and cybersecurity in the modern digital space.

Figure 2 ***Categorical apparatus of cyber education***
(Developed by the authors)

The introduction of educational innovations, enhancement of their effectiveness, and creation of a comprehensive system of practical training will enable:

- creating a modern holistic and flexible system of professional development;
- ensuring the quality and continuity of experience through professional development and self-education;
- creating appropriate conditions for the realization of employees’ right to professional growth; and
- developing professional competence.

To increase the level of digital skills to counter cyber threats to cyber citizens, awareness about cybersecurity needs to be raised at the citizen, government and organizational levels *(Tanriverdiyev, 2022)*. This means that cybersecurity issues are included in the national curriculum, from primary and secondary education to the academic environment.

For the practical implementation of the first (preschool) stage of cybersecurity education, it is advisable to introduce the course *Elementary Cyber Hygiene* into the variable subject *Computer Literacy*, which should be developed by specialists in the field of preschool education in close cooperation with professionals in all areas of cybersecurity.

The second stage of cybersecurity training is school-age training. It can be divided into several courses according to the level of school education: primary education, basic secondary education, and high school. For primary school education, cybersecurity training should be a continuation of pre-school training at a higher level of understanding (the *Cyber Hygiene* course).

For basic secondary education and high school, it is considered appropriate to include cybersecurity issues in the independent subject *General Cybersecurity* and to develop competences in the safe use of electronic devices, networks, software, passwords, mail, electronic accounts, safe behavior when using social networks, protection of personal data, prevention of violations of international and national legislation on cybersecurity, etc. Another task of high school is to form a correct idea of a possible future profession of a cybersecurity specialist, identify talented students and give them an impetus for development.

The next, third stage of cybersecurity training is the training of specialists in higher educational institutions, which can be conditionally divided into 4 groups.

The first group includes institutions that provide training in the fields of knowledge that cover the humanities, natural sciences, and other sciences not related to in-depth study of IT. In order to formulate common views on cybersecurity issues, these higher educational institutions should provide a general course on the basics of cybersecurity.

The second group is higher educational institutions that train specialists in technical fields with in-depth study of IT who will work at critical (in terms of cyber defense) infrastructure of the state. The third group includes higher educational institutions that train specialists in the fields of *Information Technology, Automation and Instrumentation, Electronics and Telecommunications*. The training of these specialists should be distinguished by more thorough knowledge compared to that of specialists in other fields of knowledge.

The fourth group is made up of higher educational institutions that train specialists in cybersecurity. The main content part of the curriculum for such specialists should be organically interconnected subjects in cybersecurity and information and communication technologies. It is impossible to train a cybersecurity specialist without a deep understanding of the essence of modern high technologies, including information and telecommunication technologies.

Adult education is a separate component of cyber education. Cyber education is vital for people of all ages, as technology and online behavior affect everyone *(World Economic Forum, 2022)*. However, the approach to cyber education may differ depending on the age group. For children and adolescents, cyber education can focus on online safety, responsible use of social media, and avoiding cyberbullying. For adults, cyber education can focus on protecting personal information, identifying and avoiding online fraud, and understanding the importance of strong passwords and security measures. It is crucial for people of all ages to receive cyber training to stay safe and informed in today's digital world.

Therefore, a multi-level generalized model of cyber education should provide for the gradual acquisition of skills and abilities to counter cyber threats (Fig. 3).

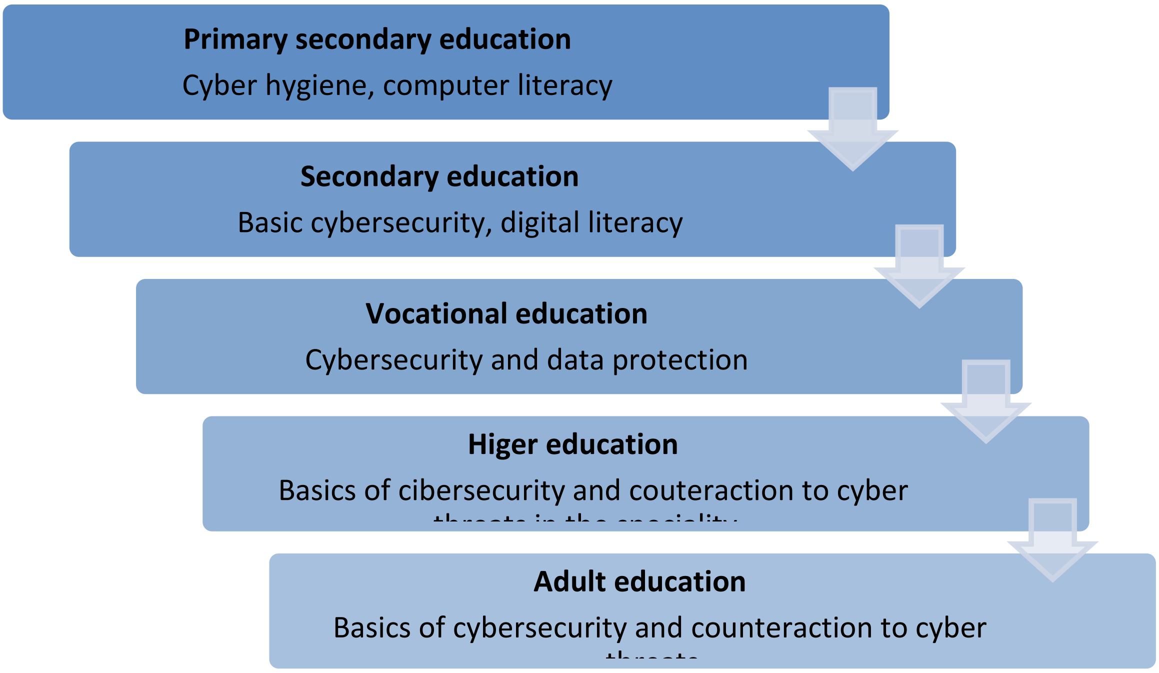

Primary secondary education
Cyber hygiene, computer literacy
Secondary education
Basic cybersecurity, digital literacy
Vocational education
Cybersecurity and data protection
Higer education
Basics of cibersecurity and couteraction to cyber threats in the speciality
Adult education
Basics of cybersecurity and counteraction to cyber threats

Figure 3 ***Multi-level generalized model of cyber education***
(Developed by the authors)

The introduction of unified regulatory courses with methodological support, developed in accordance with the best international practices in harmony with the terminology of the EU and NATO member states, would enable avoiding differences in terminology and views on the content of cybersecurity issues, forming a common understanding of cybersecurity, ensuring unification and standardization of training with the leading countries of the world, and providing an opportunity to effectively cooperate in a single informational and cyber space.

Conclusions

The integration of higher education institutions, academic and industry sectors should help ensure high-quality training of cybersecurity specialists. In this context, the introduction of innovative technologies such as virtual laboratories into the activities of educational institutions should be of particular importance. After all, cyber education is currently characterized by an insufficient level of innovation activity. To some extent, this is due to the fact that science, which is currently divided into academic, industry-related, and university sciences, is unfortunately unbalanced in its efforts to develop and implement new organizational forms that fit the logic of market relations, including in the field of cyber education. Overcoming these shortcomings will help consolidate cyber education, engage employers in training IT specialists, and accelerate the formation of a competitive main productive force of society.

Lifelong learning is gaining prominence in global educational processes, as dictated by the basic trends of modern human development. In our opinion, this approach will fundamentally change the cybersecurity training system. Unfortunately, it is still overwhelmingly focused on the needs of the past.

The modern economy requires personnel ready to work in a competitive environment, i.e. in an innovative economy.

References

Arbidane, I., Purii, H., Mamanazarov, A., Hushko, S., Kulishov, V. (2021). Digital Transformation Modelling in the Context of Slowbalization. *Intern. Sc. Congr. Society of Ambient Intelligence (ISC-SAI), Series: Information Technologies and Business Innovations, 100,* 7. DOI: https://doi.org/10.1051/shsconf/202110001003.

Cybersecurity Education Initiatives in the EU Member States. (2022). *European Union Agency for Cybersecurity***.** Retrieved from: https://www.enisa.europa.eu/publications/cybersecurity-education-initiatives-in-the-eu-member-states

Digital Education Action Plan (2021-2027). (2020). *European Commission.* Retrieved from: https://education.ec.europa.eu/focus-topics/digital-education/action-plan

Fovino, N. I., & Neisse, R. & Hernández-Ramos, J. & Polemi, N., & Ruzzante, Gian-Luigi & Figwer, M., & Lazari, A. (2019). *A Proposal for a European Cybersecurity Taxonomy.* European Commission. DOI: https://doi.org/10.2760/106002.

Lloyd's – the world's insurance marketplace. (2023). Lloyd`s Systemic Cyber Risk Scenario: Potential Global Economic Losses of 3,5 trn. Retrieved from: https://beinsure.com/lloyds-systemic-cyber-risk-scenario/

Tanriverdiyev, E. (2022). The State of the Cyber Environment and National Cybersecurity Strategy in Developed Countries. *National Security Studies*, 23, 19-26. DOI: https://doi.org/10.37055/sbn/149510.

The Cybersecurity Act (EU 881 / 2019). *The Official Journal of the European Union*. Strasbourg. Retrieved from: https://eur-lex.europa.eu/eli/reg/2019/881/oj

The Cybersecurity Strategy. (2023). *European Commission*. Retrieved from: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy

The National Cyber Security Index Ranking [NCSI]. (2023). *E-Governance Academy Foundation Company*. Retrieved from: https://ncsi.ega.ee/ncsi-index/?type=c

World Economic Forum. (2022). *Which countries spend the most time on social media?* Retrieved from: https://www.weforum.org/agenda/2022/04/social-media-internet-connectivity/