Analysis Of Existing Mechanisms And Methods For Training Cybersecurity Specialists

PhD, Dotsent Nishanov I.I Military Institute of Information and Communication Technologies and Communications

Tursunov T.M. Military Institute of Information and Communication Technologies and Communications

ABSTRACT

Cybersecurity specialists play an important role in combating risks and threats. With the development of the Internet and technologies, risks such as cyberattacks, data theft, and illegal access to systems are increasing. To combat these threats, it is necessary to train specialists. There is a shortage of qualified specialists in the field of cybersecurity, therefore, it is important to improve education systems and train them based on new methods. The knowledge and skills of specialists must be regularly updated, taking into account rapidly changing technologies. The introduction of innovative approaches and modern methods in ensuring cybersecurity helps to improve the skills of specialists.

Keywords: Cybersecurity, risks, threats, technology, cyberattack, system

1. General prospects for the development of systems and tools for training cybersecurity specialists.

Currently, the effective use of virtual laboratories in the training of cybersecurity specialists of the troops of the Cybersecurity Department of the Ministry of Defense of the Republic of Uzbekistan, and the use of training simulation simulators in improving the quality of training qualified military cybersecurity specialists, are of great practical importance.

provide comprehensive training for cybersecurity specialists, both individually and collectively. Taking into account the complexity of modern cyberattacks, the economic feasibility of using simulators in the education system is justified, taking into account the maximum use of modern scientific and technical achievements in the formation of practical qualifications and skills of future cybersecurity specialists and improving their skills [1; p. 23, 3; p. 5-6].

developed for the qualification training of cybersecurity specialists, meeting the requirements of teaching methods, implementing the system model, as well as providing control over the quality of the activities of cadets, specialists of the study area or the assessment system were analyzed [2; p. 1, 4; p. 3].

Training cybersecurity specialists is a particularly important area that is developing at a rapid pace, such as artificial intelligence and digital technologies. Nowadays, cybersecurity has become one of the most pressing issues in the world. The widespread use of the Internet, cloud technologies, IoT (Internet of Things) devices and the development of artificial intelligence have significantly increased the number of cyberattacks. Therefore, we can see an increase in the demand for cybersecurity specialists and the rapid development of systems and tools for training qualified specialists in this field.

The system of training cybersecurity specialists has already expanded and strengthened in many countries, especially in developed countries. This, in turn, is divided into several main areas of development of the system:

Training cybersecurity professionals through educational institutions:

1. Cybersecurity training in Uzbekistan is carried out in a number of higher educational institutions. In particular, large educational institutions such as Tashkent University of Information Technologies (TUIT) and the National University of Uzbekistan (NUU), etc., pay great attention to training cybersecurity specialists. These institutions have bachelor's and master's programs in cybersecurity.

New programs and courses are also being developed, for example, there are opportunities to study in areas such as “Cybersecurity”, “Information Security”, “Network Security”, and “Software Security”.

2. Some IT companies and educational centers in Uzbekistan are organizing short-term training courses on cybersecurity. For example, through events such as the Uzbekistan Cybersecurity Summit, specialists are familiarizing themselves with new cybersecurity technologies and security issues, improving their knowledge and skills.

3. Cybersecurity certification programs are also available, and international certification systems have been introduced in Uzbekistan. Certifications such as CompTIA Security+, CISSP (Certified Information Systems Security Professional), and CEH (Certified Ethical Hacker) are widely used in training cybersecurity professionals. Through these programs, students acquire globally recognized knowledge and skills.

4. In accordance with the resolutions of the President of the Republic of Uzbekistan, the Cybersecurity Center and the Information Security Department have been established. These organizations provide education and training on ensuring cybersecurity, educating state organizations, and combating cyberattacks.

We can analyze the positive and negative aspects of cybersecurity training systems as follows:

Positive aspects:

1. Training highly qualified specialists.

Undergraduate and graduate courses, as well as short-term courses, at higher education institutions are proving effective in training professionals with the necessary knowledge and skills in the field of cybersecurity. These systems help prepare students for real-world situations while teaching new and advanced security technologies.

2. International experience and certifications.

The introduction of international certification systems will allow Uzbek cybersecurity professionals to acquire knowledge and skills that meet global standards. This will help not only to find employment, but also to be competitive internationally.

3. Increased social demand for cybersecurity.

Paying special attention to cybersecurity increases the opportunities needed to train specialists in a changing technological environment. The attention of state policy to cybersecurity has a positive impact on the development of the system.

4. Practice-based learning.

Universities and training centers offer cybersecurity workshops and labs, allowing students to learn about security in a real-world setting.

Negative aspects:

1. The outdated education system.

Some curricula and education systems are based on outdated approaches and fail to respond to new cybersecurity threats. For example, curricula are not updated quickly enough to combat cyberattacks and new threats , which does not prepare students for the most modern threats in the industry.

2. Lack of qualified teachers.

The lack of highly qualified cybersecurity educators, including those who deliver research-based and practice-based education, has not been addressed. Becoming a cybersecurity educator requires constant

awareness of new threats and technologies, which poses challenges for many educators.

3. The gap between education and the job market.

Many cybersecurity professionals are not prepared to solve real-world problems in the workplace. Higher education is focused more on theoretical knowledge, while practical skills are not developed sufficiently.

4. Limited resources.

The technical resources (simulation platforms, security labs, advanced computing equipment, and other tools) needed to train cybersecurity professionals can be limited. These limited resources make it difficult for students to develop high-level skills.

It is a direction intended for professional activities in the Cybersecurity Department of the Ministry of Defense of the Republic of Uzbekistan and the cybersecurity centers of military districts in fulfilling the tasks of protecting the independence and territorial integrity of the Republic of Uzbekistan in peacetime and wartime, and covers the specialization of professional areas of military service, consisting of a set of tools, methods and techniques aimed at fulfilling service obligations in leadership in these units.

Specialists in the "Army Tactical Command Engineering (Network and Information Systems Security)" specialty are required to have the following skills:

development of recommendations and proposals for the rapid adoption of effective organizational and software-technical solutions that ensure the collection, analysis and accumulation of information on modern cyber threats to information security, the prevention of illegal access to information systems, resources, telecommunication networks and databases of military organizations ;

planning the resources necessary to implement processes related to ensuring cybersecurity in information and communication systems;

Designing cybersecurity systems in information and communication systems, configuring security tools, creating and implementing hardware and software tools used to ensure cybersecurity;

operational and maintenance services: ensuring cybersecurity of military technical equipment, devices and telecommunications systems, organizing maintenance and repair, as well as testing in accordance with security requirements;

be able to use information technologies in their professional activities, master the methods of safely collecting, storing, processing and using information, and be able to make independent, informed decisions in their activities;

acquire skills in searching for, analyzing and using regulatory and legal documents in professional activities;

Analysis of the security of computer systems for compliance with local and foreign standards for information and cybersecurity.

Implementation and development of cybersecurity policy for information and communication technologies in formations, military units and institutions, as well as control, monitoring, study and verification of the state of information security;

Studying problems related to cybersecurity and developing and implementing measures to solve them;

Planning the resources necessary to implement processes related to ensuring cybersecurity in information and communication systems;

Design and implementation of a cybersecurity system for formations, military units, and institutions;

Must have knowledge and skills in planning and implementing cybersecurity measures for information and communication systems, security devices, and information transmission, storage, and processing systems.

In military research activities:

Participate in conducting research on cybersecurity topics at research institutes and research centers;

Study of scientific sources of scientific and practical information related to the military field published in the republic and abroad;

Participate in the collection, processing, analysis and systematization of scientific data on the topic (task);

Participate in the implementation of scientific research results and developments into practice;

Direct participation in testing and experiments of military equipment, weapons, and communications equipment during special tactical exercises conducted on the implementation of progressive tactical methods and techniques;

Participate in conducting experimental research, processing and evaluating their results, and performing other types of professional activities at research institutes and scientific centers;

Participate in the preparation of scientific research papers and the examination of industry literature;

Purposefully search and find information on the Internet about the latest scientific and technological achievements in the field;

Must have knowledge and skills to solve professional problems (in accordance with the training profile) as part of the research and production team.

Table 1. shows the structure of the catalog of subjects for the specialty "Network and Information Systems Security".

Table 1.

Structure table of the catalog of subjects for the specialty "Network and Information Systems Security":

Tr	Science qualification code	Names of academic subjects, blocks and types of activities	Total load capacity, in hours	Credit amount	Semester
1.00	**Compulsory subjects**		**1500**	**50**	**7-10**
1.01	OTX9-109	Operating systems security	270	9	9-10
1.02	TXT8-97	Network and information systems security	210	7	8-9
1.03	KH8-95	Cyber law	150	5	8-9
1.04	KKEH8-1010	Cyber forensics and ethical hacking	300	10	9-10
1.05	WTX9-108	Cryptography methods	240	8	7
1.06	KU74	Web systems security	120	4	9-10
1.07	*JT7-107*	*Physical training*	*210*	*7*	*8-10*
2.00	**General professional subjects**				
2.00		*General professional subjects*	**510**	**17**	**7-10**
3.00	**Humanities**				
3.00		*Humanities*	**300**	**10**	**7,9,10**
2.00	**Elective subjects**				
2.00		*Elective subjects*	**690**	**23**	**7.8**
Qualification		Cybersecurity Engineering			
4.00		**TOTAL:**	**3000**	**100**	**7-10**
4.00		**Introductory training**	120	4	7
4.00		**Military games**	90	3	7-9
4.00		**General army field exercise**	90	3	8, 9
4.00		**Army practice**	240	8	8, 10
4.00		**Final state certification**	60	2	10
4.00		**TOTAL:**	**600**	**20**	**7-10**
ALL:			**3600**	**120**	**7-10**

A comparison diagram of lectures and practical exercises in the curriculum section of the subjects taught in the training of specialists in "Network and Information Systems Security" is presented in Figure 1.

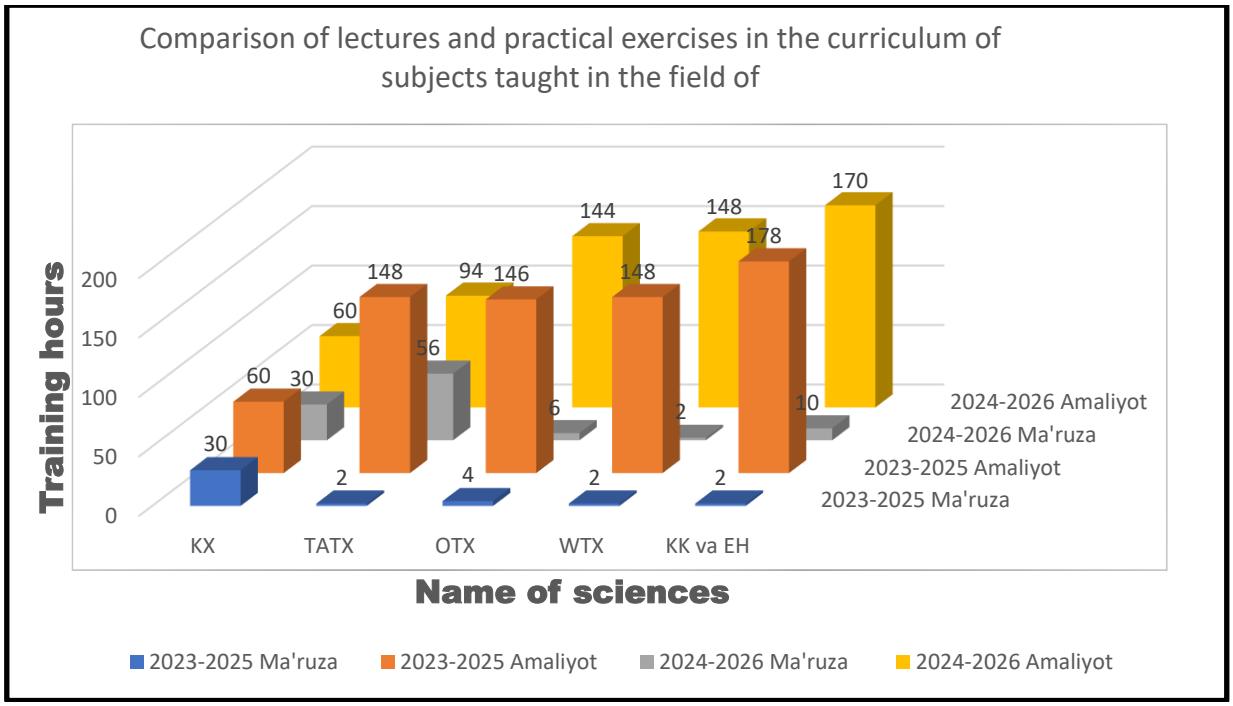

Figure 1. Comparative diagram of lectures and practical exercises in the curriculum of the subjects taught

It is clear that the education system for training cybersecurity professionals is currently facing a number of challenges. For this system to function effectively, it is necessary to improve both technologies and curricula, as mentioned above.

1. The difficulty of adapting to rapidly changing technologies and threats.

Problem: Delay in updating educational programs and adapting them to modern cybersecurity threats.

2. More emphasis on theoretical knowledge, less practice.

Problem: Lack of practice and real-world experience, which creates obstacles in preparing cadets for their future functional roles.

3. Low teacher qualifications.

Problem: Difficulty for instructors to quickly learn new security technologies and techniques and convey them to cadets.

4. Insufficient learning resources.

Problem: Lack of security labs, simulation platforms, and other necessary technical resources.

5. Educational programs that do not fully specialize in cybersecurity.

Problem: Lack of fully specialized cybersecurity education programs and faculty.

6. The gap between market needs and the education system.

Problem: Training programs and methodologies that do not meet market requirements.

7. Limited international cooperation.

Problem: Lack of international cooperation and limited opportunities for global experience sharing.

General prospects for the development of systems and tools for training cybersecurity specialists are very important today, as technologies and threats are constantly changing. For the effective training of specialists in the field of cybersecurity, it is necessary to develop modern systems and tools. Table 2. presents the main prospects for the

development of systems and tools for training cybersecurity specialists.

Table 2.

The needs and challenges in training cybersecurity professionals future implementation paths

Requirements for training cybersecurity professionals	Future implementation paths
1. Modernization of educational programs.	
Updating and modernizing cybersecurity curricula is one of the most urgent tasks today. For the system to be effective, curricula on cybersecurity science, technologies, and risks must be constantly updated. When training cybersecurity professionals, it is necessary to take into account not only old threats, but also new ones.	Creating new cybersecurity curricula and courses. Taking into account rapidly changing threats and technologies. Strengthening practice-oriented education.
2. Introduction of interactive and practical learning tools.	
Practical experience and interactive learning tools play an important role in training cybersecurity professionals. Students and professionals need to acquire practical skills in ensuring security, auditing networks, and preventing cyberattacks. To achieve this goal, it is necessary to introduce new technologies and simulations.	Simulation and virtual labs: Develop interactive training platforms to simulate cybersecurity threats in real time and prevent cyberattacks. Simulation games and labs: Cadets can practice safety protocols. Online courses and resources: Expanding learning resources and implementing curricula on private platforms.
3. Artificial intelligence and automated technologies to integrate.	
Artificial intelligence (AI) and machine learning (ML) technologies are being widely used in the cybersecurity field. They can be effective tools in detecting and preventing threats, as well as protecting systems. Integrating AI and automation in the training of cybersecurity professionals will make the learning process more effective.	Threat Detection Using Artificial Intelligence: Applying Artificial Intelligence Technologies in Educational Programs. Implementing automated systems to predict and automatically detect cyberattacks . Data Analysis: Using Artificial Intelligence to Analyze Cyberattacks and Security Vulnerabilities.
4. International cooperation and exchange of experience.	
Cybersecurity is a globally evolving field, with threats and security policies constantly changing around the world. International experience and knowledge sharing are of great importance in training cybersecurity professionals. It is necessary to introduce best practices from other countries through curricula and training.	International cooperation and conferences: To develop international cooperation and create opportunities for global experience sharing. Global certification and training programs: Implementing certification systems that meet international standards.

	Scientific and applied research: Continuously updating curricula by integrating international research and laboratories.
5. On network security and systems protection specialized courses.	
Each area of cybersecurity requires its own specific knowledge and technologies. For example, there are areas such as network security, software security, and data protection. The training of cybersecurity professionals requires the introduction of specialized courses and training modules related to these areas.	Specialized courses and training: In-depth training and practice in each area. Training by direction: For example, developing training programs on network security or data encryption. Targeted learning platforms: Creating training programs that fit the needs of each professional.
6. Fully online and blended learning systems for cybersecurity.	
In recent years, online education systems have been playing a major role in the effective organization of the educational process. The use of blended learning systems and the organization of online courses in the training of cybersecurity specialists not only improves the quality of education, but also allows students to study from different parts of the world.	Online Courses and Certifications: Offering online cybersecurity courses for students. Blended Learning: Teaching theoretical knowledge online, while providing practical training offline or through virtual labs. Interactive learning platforms: Implementing interactive technologies to provide timely assistance to students and answer their questions.
7. Public-private partnership.	
Public-private partnerships are essential in cybersecurity. Private companies are developing advanced cybersecurity technologies, while the government is focusing on supporting education systems. Close collaboration between these two sectors can help improve the effectiveness of educational programs.	Private sector-based training programs: Developing training programs in partnership with large technology companies. Education with experienced professionals: Giving students hands-on experience through practice and real-time systems. Public-private partnerships: Developing education systems and supporting a practice-oriented approach.

Conclusion

The development of the cybersecurity specialist training system requires the introduction of modern technologies and effective methods of teaching knowledge. The above prospects will be important steps in developing education in the field of cybersecurity, adapting the process of training specialists to global needs. Innovative approaches to studying cybersecurity, practice and international exchange of experience will make this process more effective. Also, the simulator simulates the real operating conditions of the platforms, which allows cadets to gain more practical skills and experience than in traditional training. This increases the effectiveness of training and can lead to an increase in the skills of specialists in this field.

References List

1. Decree of the President of the Republic of Uzbekistan No. PF-60 dated January 28, 2022 “On the Development Strategy of New Uzbekistan for 2022-2026”.
2. Resolution of the President of the Republic of Uzbekistan on measures for the further development of the higher education system dated 20.04.2017, No. PQ-2909. Xalq so'zi newspaper, 2017, No. 79 (6773); NGO of the Republic of Uzbekistan, 2017.
3. SK Ganiyev, MM Karimov, KA Tashev. Information Security. -T.: “Science and Technology”, 2016, 372 pages.
4. SKGaniyev, AAGaniyev, ZTXhudoykulov. Fundamentals of cybersecurity: a textbook. – T.: “Alokachi”, 2020, 303 pp.
5. Ganiev SK, Karimov MM, Tashev KA Information Security. Textbook (Edited by Professor S.K. Ganiev) Tashkent-2016 366 p.
6. Yuldashev, UA, Khudoyberdiev, MZ, & Akhmedov, TB (2021). Using modern information technologies to improve the quality of the educational process. //Academic research in educational sciences, 2(3), 1262-1268.
7. Decree of the President of the Republic of Uzbekistan No. 4122 of January 17, 2019.

Websites

1. Open Source Cybersecurity Tools. Introduction | by Thesherghani | Medium
2. What are the Most Common Cyber Attacks? | Linode Docs
3. What Is a Cyber Attack? How It Works, Types oath Prevention Tips
4. Types of Cyber Attacks Explained [2025]