Analysis Of Existing Methods And Study Of The Problems Of World Experience In 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

Training specialists in the field of cybersecurity is a highly relevant issue today, gaining even more importance with the global technological advancement and widespread use of the internet. The increasing number of cyberattacks and cybercrimes, as well as the need for governments and corporations to ensure information security, have intensified the demand for cybersecurity specialists. This article analyzes the existing experiences of training cybersecurity specialists in various countries around the world. Revisiting the development of cybersecurity and the training of specialists based on modern requirements will help strengthen cooperation between countries and create an opportunity to achieve global stability in the field of cybersecurity.

Keywords: Cybersecurity, Information Security, Cybersecurity Specialists, Education and Training, Global Experience, Specialist Training System, Future of Cybersecurity

I. Analysis of methods for training cybersecurity specialists based on world experience .

The world's experience in training cybersecurity specialists includes effective methods developed by various countries and leading organizations. Below, we will analyze the most important and widely used methods and consider their strengths and weaknesses:

Analysis of Cybersecurity Specialist Training Methods Based on Global Experience

Global experience in training cybersecurity specialists includes effective methods developed by various countries and leading organizations. Below, we will analyze the most important and widely used methods, considering their strengths and weaknesses:

1. University and academic programs.

Many countries offer bachelor's, master's, and doctoral programs in cybersecurity. The most prestigious universities offer training in the following areas: information security, network security, cryptography and encryption, and ethical hacking.

Leading universities:

- MIT (USA) – “Cybersecurity at MIT Sloan” program;
- Stanford University (USA) – "Advanced Cybersecurity Program";
- Carnegie Mellon University (USA) - "Information Security Policy & Management";
- Oxford University (Great Britain) – "Cyber Security Center";
- Moscow State University (MSU, Russia) – “Cybersecurity” major.

Disadvantages:

• Lack of practical experience: Programs are often theory-based and do not provide sufficient training in handling real cybersecurity incidents.

• Expensive and long-lasting: It takes 4-6 years to complete the full education.

• Lack of Updates: Cybersecurity is a rapidly evolving field, and university programs do not always include the latest innovations.

2. Certification and international standards.

There are internationally recognized certifications for professionals. They confirm the level of expertise and help to meet the requirements of the global market.

Popular certificates:

• Certified Ethical Hacker (CEH) – in ethical hacking;

• Certified Information Systems Security Professional (CISSP) – Security policy;

• CompTIA Security+ – Entry-level cybersecurity certification;

• GIAC Security Essentials (GSEC) – Advanced Security Technologies;

• Offensive Security Certified Professional (OSCP) – Practical offensive and defensive.

Disadvantages:

• Certification is expensive: Certifications like CISSP, OSCP are currently on the day It can go up to $500–$700.

• Lack of theoretical knowledge: Certificate courses are often practice-oriented and provide less fundamental theoretical knowledge.

• Requires real work experience: Some certifications (such as CISSP) require up to 5 years of experience before they can be earned.

3. International exchange of experience and trainings.

In many countries around the world, there is a strong focus on cybersecurity training programs and workshops.

Important programs:

• SANS Institute Training (USA) – Practical courses;

• Black Hat Conferences (Worldwide) – Attack and defense techniques;

• DEF CON (USA) – Forum of hackers and experts;

• European Union Agency for Cybersecurity (ENISA) – European Union projects;

• Cybersecurity Workforce Development (NIST, USA) – training based on US standards.

Disadvantages:

• The level of absorption depends on the individual: Conferences are short-term and it is difficult to learn all the information in depth.

• Can be expensive: Tickets and transportation costs for international conferences and trainings can be expensive.

• No certification: Most conferences are simply a knowledge-sharing platform and do not provide formal certification.

4. Practical labs and simulations.

Testing real-world attacks is essential in training cybersecurity professionals. Cyber Ranges and experimental laboratories are being created for this purpose.

The most popular platforms:

• Cyber Range by IBM – Corporate security simulation;

• Cisco Cybersecurity Sandbox – Practical training in network security;

• Hack The Box (HTB) – Ethical hacking platform;

• TryHackMe – Security lab for beginners.

Disadvantages:

• Requires independent learning: Since there is no mentor or coach, students must work independently.

• Specialized in a specific area: May be limited to “penetration testing” or “red teaming”.

• Not enough theoretical knowledge is provided: It is difficult to gain fundamental knowledge through practical training alone.

5. Government programs and special organizations.

Many countries have established special programs to train specialists in the field of cybersecurity.

Government initiatives around the world:

• NSA's Centers of Academic Excellence in Cybersecurity (USA) – Training students;

• UK Cyber Security Strategy (Great Britain) – Strengthening national security;

- Russia Cybersecurity Academy (Russia) – training in state defense systems;
- European Cybersecurity Competence Centre (European Union) – Developing cybersecurity.

Disadvantages:

- May be limited at the local level: Programs may be focused only on the security needs of that country.
- Confidentiality and restrictions: Special screening may be required to attend publicly funded courses.

6. Private sector and company training.

Large IT companies are also developing special courses and certification programs for their employees and external specialists.

Courses offered by leading companies:

- Google Cybersecurity Certification – Basic security courses;
- Microsoft Security Training – Corporate security courses;
- IBM Cybersecurity Analyst Professional Certificate – Practical analysis courses;
- Palo Alto Networks Cybersecurity Academy – Network Security.

Disadvantages:

- Company-specific: Training courses may be focused only on that company's tools and systems.
- May not be free: Some large companies may charge for their courses.

7. Ethical hacking and “ Bug bounty ” programs.

Becoming a skilled cybersecurity professional requires hands-on experience, which is why many professionals participate in bug bounty programs .

Popular “ Bug bounty ” platforms:

- HackerOne – Hacker support for companies;
- Bugcrowd – Find cybersecurity issues;
- Synack Red Team – Professional security testing.

Disadvantages:

- Difficult for beginners: New learners may find it difficult to make immediate progress.
- Does not provide official certification: Many “ Bug bounty ” programs do not certify participants.

Each method has its own advantages and disadvantages when training cybersecurity professionals. For the most effective results, it is recommended to combine theoretical education with practical labs and certification courses.

we can see the advantages and disadvantages of training methods for cybersecurity professionals in the example of Table 1.

Table 1.

Methods of training cybersecurity professionals advantages and disadvantages

T/r	Method name	Advantages	Disadvantages

1.	**University and academic programs**	Deep theoretical knowledge;
		International recognition of the diploma;
		Scientific research opportunities;
			Lack of practical experience;
			Expensive and long-lasting; Programs are not updated quickly;

2.	**Certification (CISSP, CEH, OSCP)**	Globally recognized;
		Based on practical training;
		Fast training (3-6 months);
			High price;
			Insufficient fundamental theoretical knowledge;
			Work experience may be required.

3.	**International conferences and trainings (Black Hat, DEF CON)**	Familiarity with the latest technologies;	The dependence of mastery on the individual;

		The ability to contact specialists; Based on practical training;	High price; Not issuing an official certificate.
4.	**Hands-on labs and simulations (Cyber Range, HTB, TryHackMe)**	Real-life experience; Interactive and interesting learning process; There are free or low-cost options;	Independent study required; Specializing only in a specific area; Insufficient theoretical knowledge.
5.	**Government programs and special organizations (NSA, ENISA)**	Financial assistance and grants; Specialized training tailored to state systems; High employment opportunities;	May have local restrictions; Confidentiality may be required.

6.	**Private sector and company training (Google, Microsoft, IBM)**	Work-related internship;
		High employment opportunities;
		Teaches modern tools.
			Focused solely on the company's needs;
			Some courses are paid.

7.	**Ethical hacking and bug bounty programs (HackerOne, Bugcrowd)**	Real experience and the opportunity to earn money; It is constantly updated; Development through community projects.	Difficulty for beginners; Not issuing an official certificate.

Figure 1 also shows the comparative dynamics of training methods for cybersecurity professionals.

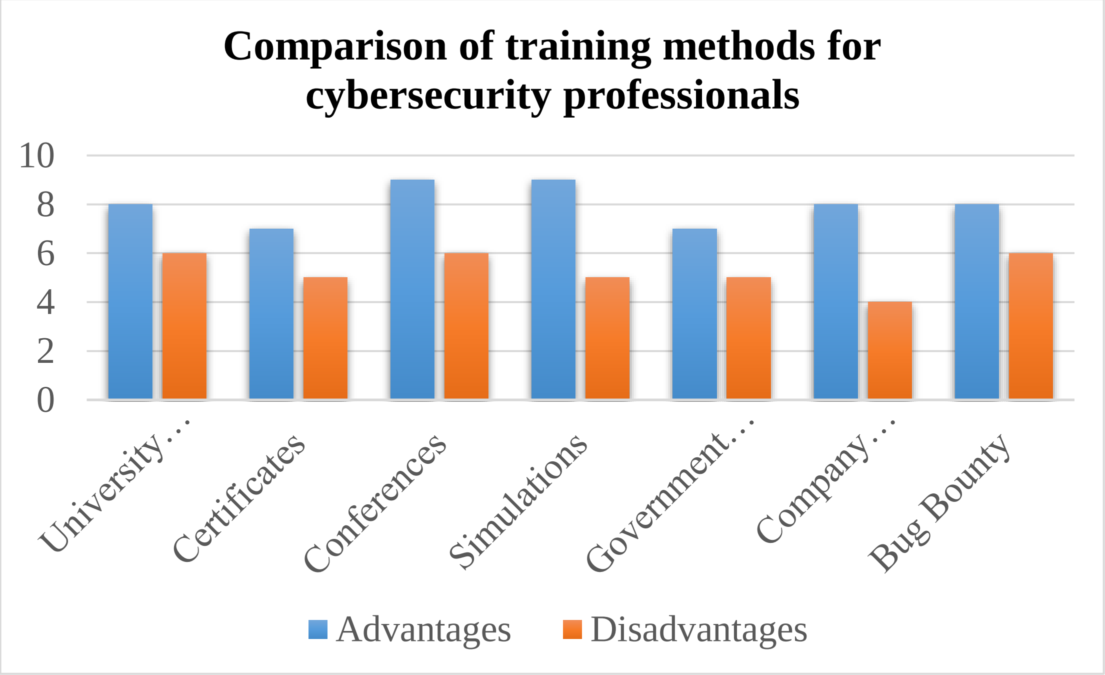

Figure 1. Methods of training cybersecurity professionals

comparison dynamics

The graph above compares the advantages (green) and disadvantages (red) of each cybersecurity training method. The higher the advantages, the more effective the method, and the lower the disadvantages, the more convenient.

• Conferences and simulations have the most advantages because they provide practical experience.

• University programs have strong theory, but are long and expensive.

• Certifications allow for quick learning but require experience.

• Bug bounty is based on real experience, but does not provide a certificate.

It is clear from this that all methods have their own shortcomings.

In conclusion, we can say that seven methods of training cybersecurity specialists based on world experience in training cybersecurity specialists were analyzed: University and academic programs; Certification
(CISSP, CEH, OSCP); International conferences and trainings (Black Hat, DEF CON); Practical laboratories and simulations (Cyber Range, HTB, TryHackMe); Government programs and special organizations (NSA, ENISA); Private sector and company trainings (Google, Microsoft, IBM); Ethical hacking and "Bug bounty" programs (HackerOne, Bugcrowd) . Their advantages and disadvantages were compared. It was found that the higher the advantages, the more effective the method, and the lower the disadvantages, the more convenient it is.

II . Studying existing problems in training cybersecurity specialists using the example of world experience .

Training cybersecurity professionals is a global challenge, and even developed countries face serious challenges in this area. Below are the main challenges and their possible solutions:

1. Lack of specialists

The problem: There is a global shortage of cybersecurity professionals. According to ISC^2, there will be a need for 3.4 million cybersecurity professionals worldwide by 2023.

Reasons: Cybersecurity education is expensive and time-consuming, there is a lack of practical training and labs for students, and most countries do not invest enough in this area.

Solutions: develop cooperation between the government and the private sector, increase the number of online education and training on cybersecurity, and involve young people in STEM (Science, Technology, Engineering, Mathematics) programs.

2. Lack of practical experience and training in a real environment.

Problem: Many universities and training centers only provide theoretical knowledge and do not focus on practical training. Many graduates are not prepared for real cybersecurity threats.

Reasons: lack of cybersecurity laboratories and simulation environments, weak university-industry collaboration, lack of real-time training and experienced professionals.

Solutions: through the widespread use of virtual labs such as Cyber Range and Hack The Box, TryHackMe, through government agencies and private companies allocating more funds for practical training and internships, through involving young people in " Bug Bounty " programs, and through the development of cybersecurity competitions.

3. Lack of continuous updating of educational programs.

Problem: Cybersecurity technologies are advancing rapidly, but most university courses are outdated.

Reasons: slow modernization of curricula, difficulty in adapting to technological innovations.

Solutions: Establishing permanent cooperation between the institute and the manufacturing industry. Involving teachers in international trainings and practical laboratories. Incorporating practical courses and certificate programs (CISSP, CEH, OSCP) into the institute's curricula.

4. The complexity and high cost of the international certification system.

Problem: International cybersecurity certifications such as CISSP, CEH, OSCP are expensive, making them financially unaffordable for most students and professionals.

Reasons: The certification process is complex and expensive (currently Between $300–$700). Some countries do not have special examination centers for obtaining certificates. International certificates are not recognized equally by all countries.

Solutions: Government grants and scholarships should be provided. Private companies should encourage their employees to get certified. Create cheaper or free alternatives through online courses.

5. Insufficient cooperation between governments and the private sector

Problem: There is insufficient cooperation between the government and the private sector, which leads to a shortage of qualified specialists.

Reasons: There is low information exchange between government agencies and the private sector. Insufficient financial resources are allocated to develop cybersecurity infrastructure. Government laws and regulations on cybersecurity vary from country to country.

Solutions: The public and private sectors should work together to establish cybersecurity academies and training centers. Private companies should provide grants and scholarships to train cybersecurity professionals. Governments should promote uniform cybersecurity standards through increased international cooperation.

6. Insufficient dissemination of cybersecurity knowledge

Problem: Most students do not fully understand the importance of cybersecurity and lack the motivation to enter the field.

Reasons: The benefits of working in cybersecurity are poorly promoted. There are few courses dedicated to cybersecurity in schools and universities. Young people are hesitant to choose careers related to cybersecurity.

Solutions: Introduce cybersecurity subjects in schools and institutes. Organize cybersecurity competitions and " hackathons " among youth . Create cybersecurity seminars and online courses for parents and teachers.

By addressing these challenges, we can ensure and strengthen cybersecurity globally. Figure 2 shows a breakdown of the main challenges in training cybersecurity professionals.

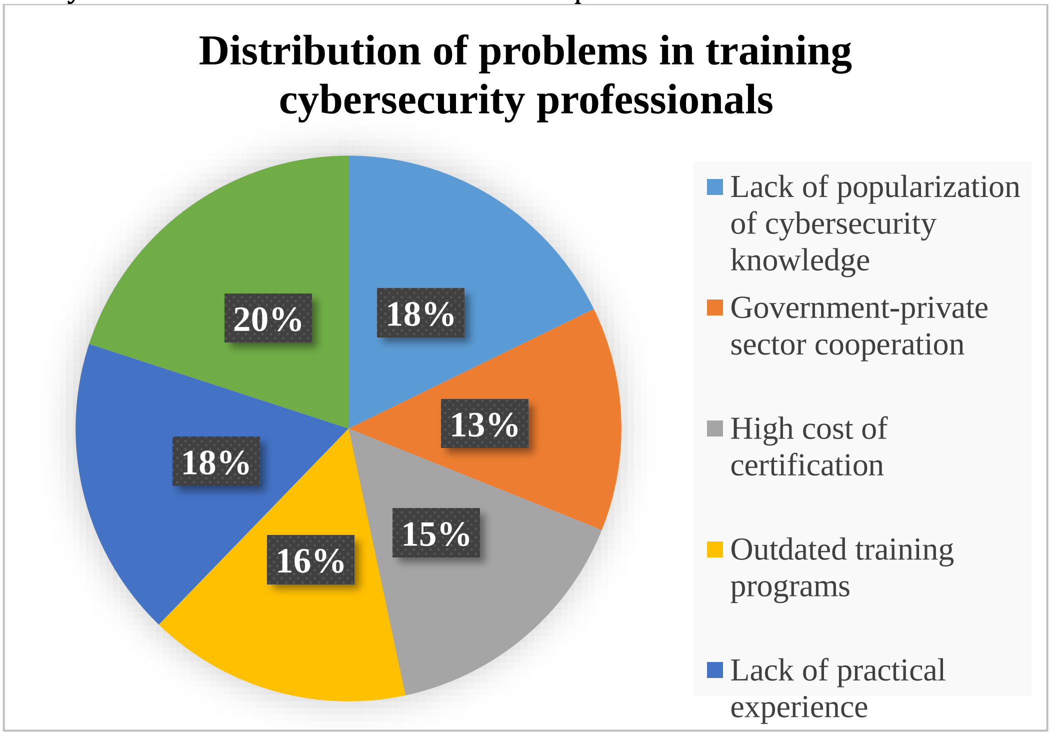

Figure 2. Training of cybersecurity professionals

problem distribution

This pie chart shows the distribution of challenges in training cybersecurity professionals:

• The lack of specialists and the lack of popularization of cybersecurity knowledge occupy the largest share.

• Lack of practical experience and the high cost of certificates also have a significant impact.

• Weak government-private sector cooperation is a relatively small but significant problem that needs to be addressed.

These visualizations will help you better understand the severity of problems and their distribution.

As can be seen from the table, the most important problems are the shortage of specialists, lack of practical experience, and lack of popularization of knowledge. To solve these problems, it is necessary to: increase the number of practical laboratories and trainings, strengthen cooperation between universities and companies, reduce the cost of certificates or provide grants.

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 experience exchange 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 training efficiency increases and this in the field of experts qualification to increase take arrival possible .

Used literature 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. High education system further develop measures about Uzbekistan Republic President's Resolution of 20.04.2017, No. PQ-2909. People word newspaper , 2017, issue 79 (6773); O' R NGO, 2017.
3. Akhmedov , TB (2021). Reading process quality in increasing modern information from technologies use //Academic research in educational sciences, 2(3), 1262-1268.
4. Yuldashev UA Use of video lesson creative technologies in the process of electronic education// Scientific-Methodical Journal-T 2021.

Websites :

1. (PDF) The Role Of Cybersecurity In Contemporary Technology: Evaluating The Effects Of Cyber-Attack On Progress In Modern Science .
2. (PDF) The Role Of Cybersecurity In Contemporary Technology: Evaluating The Effects Of Cyber-Attack On Progress In Modern Science Top 20 Biggest Cybersecurity Trends in 2025 .