JOURNAL OF MULTIDISCIPLINARY SCIENCES AND INNOVATIONS
VOLUME 05, ISSUE 01
MOPNTHLY JOURNALS
ISSN NUMBER: 2751-4390
IMPACT FACTOR: 9,08

STAGES OF ORGANIZING DIGITAL TRAINING IN CYBERSECURITY

Asadbek Otabek ugli Ne'matov
Asia International University MM2-TAT-25
Master's student

Abstract: This article analyzes the main stages of organizing digital training in the field of cybersecurity and their significance in the educational process. The paper examines the role of digital training in developing practical skills in cybersecurity, the possibilities of providing education based on virtual environments, the advantages of digital training, and issues related to integrating such training into pedagogical processes. In addition, it emphasizes that the use of digital training in cybersecurity education increases the effectiveness of learning.

Keywords: Cybersecurity, cyber threats, digital training, training stages, virtual environment, information security.

Introduction

Along with the rapid development of digital technologies today, the number and complexity of cyber threats are also increasing. This situation creates a need to train highly qualified specialists in the field of cybersecurity. Digital training makes it possible to model real cyberattacks in virtual environments, identify security vulnerabilities, and take countermeasures against them. This allows students to be trained in conditions close to real professional activities. Along with traditional teaching methods, the formation of practical skills through digital training is becoming an important component of cybersecurity education. [6]

Literature Review

In recent years, the rapid development of digital technologies and the widespread use of information systems have turned cybersecurity into an urgent scientific and practical issue. In particular, digital training plays an important role in preparing cybersecurity specialists. Therefore, it is necessary to analyze scientific research and methodological approaches conducted in this area. Digital training is based on distance education, e-learning, and blended learning models. Studies conducted by Clark and Mayer have proven that the effectiveness of digital education is directly related to interactivity, visualization, and practical exercises. It has been shown that the use of virtual laboratories, simulations, and "cyber range" technologies in cybersecurity training significantly increases the effectiveness of the learning process.

Main Part

The Concept of Digital Training and Its Importance

Digital training is an educational process organized on the basis of modern information technologies, virtual laboratories, simulators, and online platforms. In the field of cybersecurity, digital training enables students to strengthen theoretical knowledge with practical experience. Such training helps develop the following skills:

- studying real cyber threats in a safe environment;
- ensuring network and system security;
- identifying and analyzing cyberattacks;
- making quick decisions in problematic situations. [1]

Stages of Organizing Digital Training in Cybersecurity

Identifying Goals and Needs

Before organizing the training, students' knowledge levels, professional needs, and expected outcomes are determined. At this stage, the goals, objectives, and competencies of the training are defined. [3]

Designing the Curriculum

At this stage, a curriculum that includes both theoretical and practical lessons is developed. The program may include the following topics:

- cyber threats and their types;
- information security;
- network and system security;
- fundamentals of cryptography;
- incident management. [5]

Selecting Digital Platforms and Tools

The effectiveness of the training depends on the selected digital platform. Virtual laboratories, simulators, and online training systems make it possible to model real attack and defense processes. [4]

Organizing Practical Training

At this stage, students perform practical tasks in a virtual environment related to detecting cyberattacks, analyzing security vulnerabilities, and taking countermeasures against them. This process develops independent thinking and problem-solving skills.

Assessment and Monitoring

During and after the training, students' knowledge and skills are assessed. Tests, practical tasks, and project work are used to compare students' competencies before and after the training.

Improvement and Integration

Based on the results obtained, the training program is continuously updated and integrated into the educational process. This helps improve the quality and effectiveness of education. [2]

Advantages of Digital Training

Digital training has the following advantages:

- flexibility and convenience;
- interactivity and closeness to real-life situations;
- the ability to gain experience in a safe environment;
- rapid and effective development of practical skills.

Analysis and Results

The conducted analysis shows that organizing digital training in cybersecurity requires a multi-stage and systematic approach. Based on existing scientific sources and international experience, the training organization process was evaluated within the following main stages: identifying goals and needs, designing the curriculum, selecting digital platforms and tools, organizing practical training, assessment and monitoring, and improvement and integration. According to the analysis results, the stage of identifying goals and needs is one of the most important factors determining training effectiveness. It was found that when students' initial knowledge levels and the likelihood of encountering real cybersecurity threats are not sufficiently considered at this stage, training outcomes tend to be low.

Conclusion

In conclusion, systematically and step-by-step organizing digital training in cybersecurity contributes to the development of strong theoretical knowledge and practical skills among students. Training conducted in virtual environments is becoming an integral part of the modern education system and provides opportunities to train competitive specialists in the field of information security.

References

1. Karimov A.A., Jo‘rayev M.M. Fundamentals of Information Security – Tashkent: “Fan va texnologiya”, 2021.
2. Qodirov A., Mamatov S. Information Technologies and Information Security – Tashkent: TDPU Publishing House, 2020.
3. O‘rolov A. Information Culture and Information Security – Tashkent: “Yangi asr avlodi”, 2019.
4. ISO/IEC 27001:2022 — Information Security Management Systems — Requirements. International Organization for Standardization.
5. Lebedev S.Y. Digital security – digital criminal law resource / S.Y. Lebedev // Criminology: Yesterday, Today, Tomorrow. 2019, No. 4, pp. 17–25.
6. Alidjonovna O. O. Fundamentals of Cybersecurity: Initial Knowledge for School Students // International Journal of Scientific Researchers. – 2025. – Vol. 11. – No. 1. – pp. 519–521.