BG Pulse Journal USA
ISSN:1947-2536 http://www.bgpulseusa.com/index.php/bg

METHODOLOGY FOR CREATING AN EDUCATIONAL SIMULATOR BASED ON DIGITAL TRAINING IN CYBERSECURITY

Asadbek Otabek ugli Ne'matov

MM2-TAT-25 Master's Student of Asia International University

Abstract

This article discusses the methodology for creating an educational simulator based on digital training in cybersecurity. In cybersecurity education, providing only theoretical information is not sufficient, because this field requires practical skills such as identifying risks, analyzing situations, selecting protective measures, and responding to incidents. Therefore, an educational simulator enables learners to practice in an environment that is close to real conditions, while remaining safe and manageable [6]. The article analyzes issues related to simulator design, scenario development, ensuring security, and evaluating learning outcomes.

Keywords: cybersecurity, digital training, educational simulator, virtual laboratory, practical skills, scenario-based learning, assessment.

Introduction

The rapid development of digital technologies is expanding the use of information systems and digital services. In the Republic of Uzbekistan, the development of digital technologies in public administration, education, the economy, and the social sphere has been defined as a priority through the "Digital Uzbekistan — 2030" Strategy [2]. As digital infrastructure expands, the need to protect information resources, develop safe digital behavior among users, and strengthen cybersecurity culture also increases.

The Law of the Republic of Uzbekistan "On Cybersecurity" defines issues related to the regulation of relations in the field of cybersecurity and the protection of information systems and resources from cyber threats [1]. This demonstrates the need to form not only theoretical knowledge but also practical skills in cybersecurity within the education system. The NICE Framework describes cybersecurity competencies in connection with tasks, knowledge, and skills [3]. Therefore, the use of digital training and simulation-based exercises in teaching cybersecurity is an effective methodological solution.

Methodological Essence of Digital Training and the Simulator

Digital training is a form of organizing the educational process through electronic resources, interactive tasks, virtual laboratories, tests, and analytical assessment tools. Digital training in cybersecurity introduces learners to potential cyber threats and teaches them to identify, assess, and respond to those threats. The educational simulator is the practical component of this training, where users apply theoretical knowledge through tasks that are close to real-life situations.

The simulator methodology is based on three approaches: competence-oriented training, scenario-based instruction, and reflective assessment. The competence-oriented approach takes into account not only what the learner "knows" but also what the learner "can do." The scenario-based approach organizes training through real-life risk situations, problems, and decision-making

contexts. The ENISA methodology also considers the planning, implementation, and evaluation of cybersecurity exercises as a single cycle [5].

From this point of view, an educational simulator is not a simple testing program. It is a didactic system that integrates theoretical content, a laboratory environment, practical tasks, automated assessment, teacher supervision, and analytical reports. Studies on cyber ranges and testbeds show that such environments are used for education, training, and research purposes and are distinguished by their scenarios, architecture, and assessment capabilities [10].

Methodological Stages of Creating an Educational Simulator

Creating an educational simulator based on digital cybersecurity training is a consistent methodological process that covers several interrelated areas. Each area serves to ensure the content, technical capability, security, and pedagogical effectiveness of the simulator.

At the initial stage, needs and objectives are identified. This process determines who the simulator is intended for, what the initial level of learners' knowledge is, and what competencies they should acquire. For example, password security, protection against phishing, and the protection of personal data are important for general users, while network monitoring, log analysis, and incident response modules are priorities for specialized training programs [3].

The next important area is the definition of learning outcomes. At the end of each module, it is clearly stated what knowledge and skills the learner should acquire. Outcomes such as "being able to identify the main features of a phishing message," "being able to apply the criteria for creating a strong password," and "being able to distinguish suspicious login attempts in system logs" also make the assessment process more precise.

After that, scenarios and practical tasks are designed. Each scenario includes a description of the situation, the user's role, the task to be performed, available resources, limitations, expected results, and assessment criteria. The ENISA methodology also emphasizes that exercise scenarios should be developed in connection with the objective, scope, participants' roles, and evaluation outcomes [5].

In the next stage, the technological architecture is developed. The simulator may consist of a user interface, a teacher dashboard, a practical laboratory environment, a task bank, an assessment module, a database, and analytical reports. In platforms such as CyTrONE, the automation of training content development and environment configuration is considered an important component of hands-on cybersecurity training [9].

One of the key structural stages is the introduction of security, isolation, and management mechanisms. The simulator must operate in an environment that is separated from external networks, has restricted user privileges, and can be restored after each training session. The NIST guide on cyber ranges notes that such environments help develop practical cyber skills in safe and lawful conditions [6].

Another necessary part of the methodological process is the creation of an assessment and feedback system. This includes correct decision-making, task completion speed, number of errors,

accuracy of risk identification, quality of reporting, and progress in repeated attempts. At the final stage, the simulator is piloted with a small group and improved based on the feedback received.

Functional Model and Tasks of the Simulator

An effective educational simulator includes three main user roles: learner, teacher, and administrator. The learner studies theoretical materials, performs tasks, and reviews the results. The teacher manages groups, assigns tasks, and analyzes outcomes. The administrator is responsible for system security, user accounts, and technical settings. Research on cyber range design also considers the alignment of learning objectives, the technical environment, scenarios, and assessment mechanisms as an important factor [7].

It is advisable for the simulator to include a theoretical module, a virtual laboratory, a scenario bank, a testing and control module, automated assessment, and analytical reports. At the beginner level, tasks related to password security, phishing, social engineering, and personal data protection are assigned. At the intermediate level, exercises on network security, secure configuration, access rights, and log analysis are used. At the advanced level, tasks such as incident response, preservation of digital evidence, and preparation of security reports are performed [8].

For example, in the task “Identifying a phishing message,” the learner analyzes the sender’s email address, errors in the text, suspicious links, and attempts to request personal information. In the task “Log analysis,” unusual IP addresses, failed login attempts, and repeated requests in system logs are identified. The fact that the NIST CSF 2.0 document includes awareness and training within the “Protect” function indicates that user preparedness should be regarded as an important part of the protection process [4].

Assessment, Security, and Pedagogical Effectiveness

The effectiveness of an educational simulator should not be assessed only by a final score. The level of knowledge, quality of practical performance, speed, analytical thinking, quality of explanation, and progress dynamics should be considered together. Comparing pre-training and post-training results helps determine the pedagogical impact of the simulator. The CyTrONE study also shows that systematic organization of training content, environment configuration, and execution processes contributes to improving the effectiveness of exercises [9].

Security and ethical requirements are of particular importance in a cybersecurity simulator. All tasks must be performed only for educational purposes, in a limited virtual environment, and under teacher supervision. Real personal data, actual organizational infrastructure, or unauthorized networks must not be used. Studies on cyber ranges also interpret such platforms as environments that model real networks and systems while remaining safe and manageable [8].

From an ethical perspective, the simulator should guide learners not toward attacking, but toward understanding risks and developing protective measures. Tasks that include attack elements should also be used for the purpose of understanding threats, learning protection methods, and responding to incidents. This approach is closely linked to legal regulation in the field of cybersecurity and the requirements for protecting information resources [1].

Conclusion

Creating an educational simulator based on digital training in cybersecurity is an effective way to transform theoretical knowledge into practical skills in the educational process. Such simulators allow learners to practice in conditions close to real situations, analyze mistakes in a safe environment, and make independent decisions.

In developing a simulator, it is important to identify needs and objectives, define learning outcomes, design scenarios, develop the technological architecture, ensure security and isolation, introduce an assessment system, and improve the simulator through pilot testing. In the future, such simulators can be enhanced with adaptive assessment based on artificial intelligence, learning analytics, and team-based exercises.

References

1. Law of the Republic of Uzbekistan "On Cybersecurity." April 15, 2022, No. ZRU-764.
2. Decree of the President of the Republic of Uzbekistan "On Approval of the Digital Uzbekistan — 2030 Strategy and Measures for Its Effective Implementation." October 5, 2020, No. PF-6079.
3. Petersen R., Santos D., Wetzel K., Smith M., Witte G. Workforce Framework for Cybersecurity: NICE Framework. NIST Special Publication 800-181 Revision 1. 2020.
4. National Institute of Standards and Technology. The NIST Cybersecurity Framework 2.0. NIST CSWP 29. 2024.
5. ENISA. The ENISA Cybersecurity Exercise Methodology. European Union Agency for Cybersecurity. 2026.
6. National Institute of Standards and Technology. The Cyber Range: A Guide. NIST/NICE. 2023.
7. Katsantonis N., Manikas A. Cyber Range Design Framework for Cyber Security Education and Training. International Journal of Information Security. 2023.
8. Chouliaras N., Kittes G., Kantzavelou I., Maglaras L., Pantziou G., Ferrag M. Cyber Ranges and TestBeds for Education, Training, and Research. Applied Sciences. 2021.
9. Beuran R., Tang D., Pham C., Chinen K., Tan Y., Shinoda Y. Integrated Framework for Hands-on Cybersecurity Training: CyTrONE. Computers & Security. 2018. Vol. 78. P. 43–59.
10. Yamin M.M., Katt B., Gkioulos V. Cyber Ranges and Security Testbeds: Scenarios, Functions, Tools and Architecture. Computers & Security. 2020. Vol. 88. Article 101636.