JOURNAL OF MULTIDISCIPLINARY SCIENCES AND INNOVATIONS

VOLUME 5, ISSUE 03
MONTHLY JOURNALS

ISSN NUMBER: 2751-4390
IMPACT FACTOR: 9,08

FORMATION OF INFORMATION SECURITY COMPETENCIES IN STUDENTS

Ergashev Baxriddin Nomoz ugli,
Hamrayeva Komila Hamidjon kizi
Jizzakh State Pedagogical University,
Department of Information Technologies and Systems,
E-mail: baha-ergashev@mail.ru

Abstract: In the modern digital society, the issue of information security has become one of the most important aspects of education and professional training. The rapid development of information technologies and the increasing amount of digital data require students to possess sufficient knowledge and competencies in the field of information security. This article discusses the importance of forming information security competencies among students, the main directions of their development, and effective pedagogical approaches for teaching information security in higher education institutions. The study highlights the role of digital literacy, awareness of cyber threats, and responsible use of information technologies in ensuring information security. In addition, the article analyzes educational methods and strategies that can help improve students' competence in protecting information resources. The results show that integrating information security education into academic programs contributes to the development of responsible and competent specialists capable of ensuring the safe use of information technologies in various fields.

Keywords: information security, student competence, cybersecurity education, digital literacy, information protection, cyber threats, higher education, information technology.

Introduction

The rapid development of information and communication technologies has significantly transformed modern society. Today, digital technologies are used in almost all spheres of life, including education, economics, government, and social communication. However, along with these advantages, the widespread use of information technologies has also led to new challenges related to information security.

Information security refers to the protection of information resources from unauthorized access, misuse, disclosure, disruption, modification, or destruction. Students, as active users of digital technologies, often face various cyber threats such as phishing, malware, identity theft, and data leakage. Therefore, it is essential to develop information security competencies among students in order to ensure safe and responsible use of digital technologies.

Higher education institutions play a key role in preparing students to deal with information security challenges. Developing students' competencies in this area requires not only theoretical knowledge but also practical skills and awareness of potential risks.

The Concept of Information Security Competence

Information security competence can be defined as a combination of knowledge, skills, attitudes, and behaviors that enable individuals to effectively protect information and digital systems from various threats. It includes understanding security principles, recognizing potential risks, and applying appropriate protective measures.

The formation of such competencies among students is particularly important because they frequently use digital tools for learning, communication, and research activities. Without adequate knowledge of information security, students may unintentionally expose themselves and others to cyber risks.

Key components of information security competence include:

- **Knowledge of information security principles**
- **Understanding cyber threats and vulnerabilities**
- **Ability to use secure digital tools**
- **Responsible digital behavior**
- **Skills in protecting personal and organizational data**

These components form the basis for developing a secure digital culture among students.

Methods of Developing Information Security Competencies

The formation of information security competencies among students requires the implementation of effective educational strategies. Several pedagogical methods can be used in higher education institutions to achieve this goal.

Integration into the Curriculum. Information security topics should be integrated into academic programs related to information technologies, computer science, and other disciplines. This integration allows students to gain systematic knowledge about cybersecurity and data protection.

Practical Training. Practical exercises and laboratory work help students understand real-world security threats and develop skills in detecting and preventing cyber attacks. Simulated scenarios and case studies can be used to enhance practical learning.

Digital Literacy Development. Developing digital literacy is an important aspect of information security education. Students should learn how to safely use online platforms, protect personal data, and recognize suspicious online activities.

Awareness Programs. Educational seminars, workshops, and awareness campaigns can significantly improve students' understanding of cybersecurity issues. Such activities help promote responsible behavior in the digital environment.

Use of Modern Educational Technologies. The use of e-learning platforms, interactive simulations, and virtual laboratories can enhance students' engagement and improve the effectiveness of cybersecurity education.

Challenges in Developing Information Security Competencies

Despite the importance of information security education, several challenges remain. One of the main problems is the lack of sufficient attention to cybersecurity topics in educational curricula. In many cases, information security is taught only as a specialized subject rather than as a fundamental component of digital education.

Another challenge is the rapid evolution of cyber threats. New forms of cyber attacks appear constantly, making it difficult for educational institutions to keep their programs up to date.

Additionally, students often underestimate the importance of information security and may not fully understand the risks associated with careless online behavior.

Addressing these challenges requires continuous improvement of educational programs and active collaboration between educators, researchers, and cybersecurity professionals.

Conclusion

The formation of information security competencies among students is an essential component of modern education. As digital technologies continue to develop, the risks associated with cyber threats also increase. Therefore, it is important for higher education institutions to provide students with the necessary knowledge and skills to ensure safe and responsible use of information technologies.

Effective integration of information security topics into educational programs, combined with practical training and awareness initiatives, can significantly enhance students' competence in this area. By developing strong information security competencies, universities can contribute to the preparation of qualified specialists capable of addressing cybersecurity challenges in the digital age.

References

1. Whitman, M., & Mattord, H. (2018). *Principles of Information Security*. Cengage Learning.
2. Stallings, W. (2017). *Effective Cybersecurity: A Guide to Using Best Practices and Standards*. Addison-Wesley.
3. Bishop, M. (2019). *Computer Security: Art and Science*. Addison-Wesley.
4. Anderson, R. (2020). *Security Engineering: A Guide to Building Dependable Distributed Systems*. Wiley.
5. Von Solms, R., & Van Niekerk, J. (2013). Information security culture. *Computers & Security*, 38.
6. UNESCO. (2021). *Digital Literacy and Safety Skills Framework*.
7. NIST. (2020). *Cybersecurity Framework*. National Institute of Standards and Technology.
8. Kaspersky Lab. (2022). *Cybersecurity Education and Awareness Report*.
9. ISO/IEC 27001. (2018). *Information Security Management Systems – Requirements*.
10. OECD. (2021). *Digital Security Risk Management in Education*.