Published Date: - 01-05-2025
Page No: - 384-386

THE NEED TO DEVELOP INFORMATION SECURITY COMPETENCIES AMONG FUTURE INFORMATICS TEACHERS IN HIGHER EDUCATION INSTITUTIONS OF UZBEKISTAN

Abdullaev Ilkhom Khujayorovich
Teacher at the Department of Informatics, Uzbekistan-Finland Pedagogical Institute, Uzbekistan

INTRODUCTION

In the 21st century, alongside the rapid development of information technologies and the integration of digitalization processes into all sectors and industries, cyber threats have also become increasingly complex. Each year, the number and complexity of cyber threats continue to rise, significantly increasing the demand for qualified specialists in the field of information security [1].

In the context of the digitalization of the education system in the Republic of Uzbekistan, the development of information security competencies among future informatics teachers is emerging as a pressing issue. Today, given the widespread use of digital technologies in educational institutions, it is crucial for teachers to possess sufficient knowledge and skills in information security to ensure the protection of both students and institutional information systems [2].

MAIN BODY

1. Theoretical Foundations of Information Security Competencies

Information security competency refers to the combination of knowledge, skills, and abilities required for a person to operate safely in a digital environment, protect information resources, and defend against cyber threats [3]. These competencies include the following components:

- Knowledge component: Theoretical knowledge about the basics of information security, types of cyber threats, and methods of protection;
- Practical component: Skills to use security tools, identify and mitigate threats;
- Personal component: A sense of ethical and legal responsibility in the field of information security.

2. Current Situation Analysis. Research conducted to assess the level of information security competencies among informatics students in higher education institutions in Uzbekistan reveals serious shortcomings in this area. More than 60% of students lack sufficient information about major cyber threats, and 45% are unable to properly use modern protection tools [4].

Moreover, the amount of instructional time allocated to information security topics in curricula is insufficient. Currently, only about 8–12% of the total academic load in informatics bachelor's programs is devoted to information security subjects, which is significantly lower than international standards (15–20%) [5].

3. Ways to Develop Competencies. To effectively develop information security competencies in future informatics teachers, the following measures are necessary:

3.1. Improving the Curriculum
- Increasing the number of hours allocated to information security subjects
- Expanding the share of practical training
- Studying modern cyber threats and protection methods

3.2. Implementing Innovative Teaching Technologies
- Utilizing virtual labs and simulators
- Using simulation games and scenario-based learning
- Offering information security courses via distance learning platforms

3.3. Enhancing Practical Experience and Internships
- Collaborating with IT companies and information security centers
- Creating opportunities for students to work on real projects
- Organizing mentorship programs with qualified specialists

4. International Experience and Adaptation to Uzbekistan's Context

In developed countries, special attention is given to information security competencies in the training of informatics teachers. For instance, in the USA, teachers are trained according to the NICE (National Initiative for Cybersecurity Education) standard, which outlines 33 core competencies [6].

In adapting such experiences to Uzbekistan, it is essential to consider the specific characteristics of the national education system, available resources, and infrastructure. Additionally, alignment with government policies and the goals of the "Digital Uzbekistan 2030" strategy must be ensured.

CONCLUSION

Research findings demonstrate that the development of information security competencies among future informatics teachers in Uzbekistan's higher education institutions is a legitimate necessity and should be pursued in the following key areas:

1. Improving instructional support: Reviewing and updating information security curricula in line with modern requirements;
2. Enhancing staff qualifications: Continuously updating teachers' knowledge and skills in the field of information security;
3. Strengthening the material and technical base: Creating laboratories equipped with modern information security tools and software;
4. Fostering practical cooperation: Establishing long-term partnerships with IT enterprises and information security centers.

The implementation of these measures will help meet the demand for highly qualified personnel in the field of information security in Uzbekistan and strengthen the country’s digital safety. Furthermore, it will contribute significantly to improving the quality of education by preparing informatics teachers who meet modern standards.

Recommendations for the Future: It is advisable to continue research in this area, develop pilot projects, and assess their effectiveness.

REFERENCES

1. Rajabov, A.N. (2023). Cyber Threats and Modern Information Security. Tashkent: "O‘qituvchi" Publishing House, p. 234.

2. Karimov, S.M., Abdullayeva, N.K. (2022). Issues of Information Security in Digital Education. Tashkent: "Fan" Publishing House, p. 189.
3. Usmanov, B.R. (2023). Methodology for Developing Information Security Competencies. Samarkand: SamSU Publishing House, p. 167.
4. Normatov, I.S., Qosimova, D.A. (2022). "Current State of Information Security Education in Higher Education Institutions", Journal of Educational Technologies, No. 3, pp. 45–52.
5. Mirzayev, F.T. (2023). Professional Training of Informatics Teachers. Bukhara: "Bukhara" Publishing House, p. 298.
6. Saidov, A.U., Tashmatov, R.B. (2022). "International Experience and Information Security in Uzbekistan's Education System", Information Security and Digital Technologies, No. 2, pp. 78–85.