METHODS OF ENSURING INFORMATION SECURITY IN THE VOCATIONAL EDUCATION PROCESS

Hamroyeva Madina Yunusovna
Senior Teacher of Specialized Subjects, Gijduvon District Technical School No. 4

Abstract. This article examines current issues in ensuring information security in vocational education institutions, methods of protecting electronic learning resources and information systems, protecting users' personal data, and ways of building a culture of cybersecurity. It also analyzes the information security threats that may arise in the vocational education process and proposes organizational, technical, and pedagogical solutions for preventing them.

Keywords: vocational education, information security, cybersecurity, digital education, personal data, e-learning platform, information technologies, data protection.

Introduction. Today, the use of digital technologies in the education system is expanding, and e-learning platforms, distance learning systems, electronic gradebooks, and digital learning resources are becoming an essential part of the educational process. In vocational education institutions in particular, the use of information systems for assessing students' knowledge, keeping attendance records, distributing learning materials, and organizing teaching activities is increasing efficiency. At the same time, the digitalization of education is giving rise to new problems related to information security. In particular, unauthorized disclosure of personal data, hacking of user accounts, malware, phishing attacks, and the loss of educational data may have a negative impact on the operations of educational institutions.

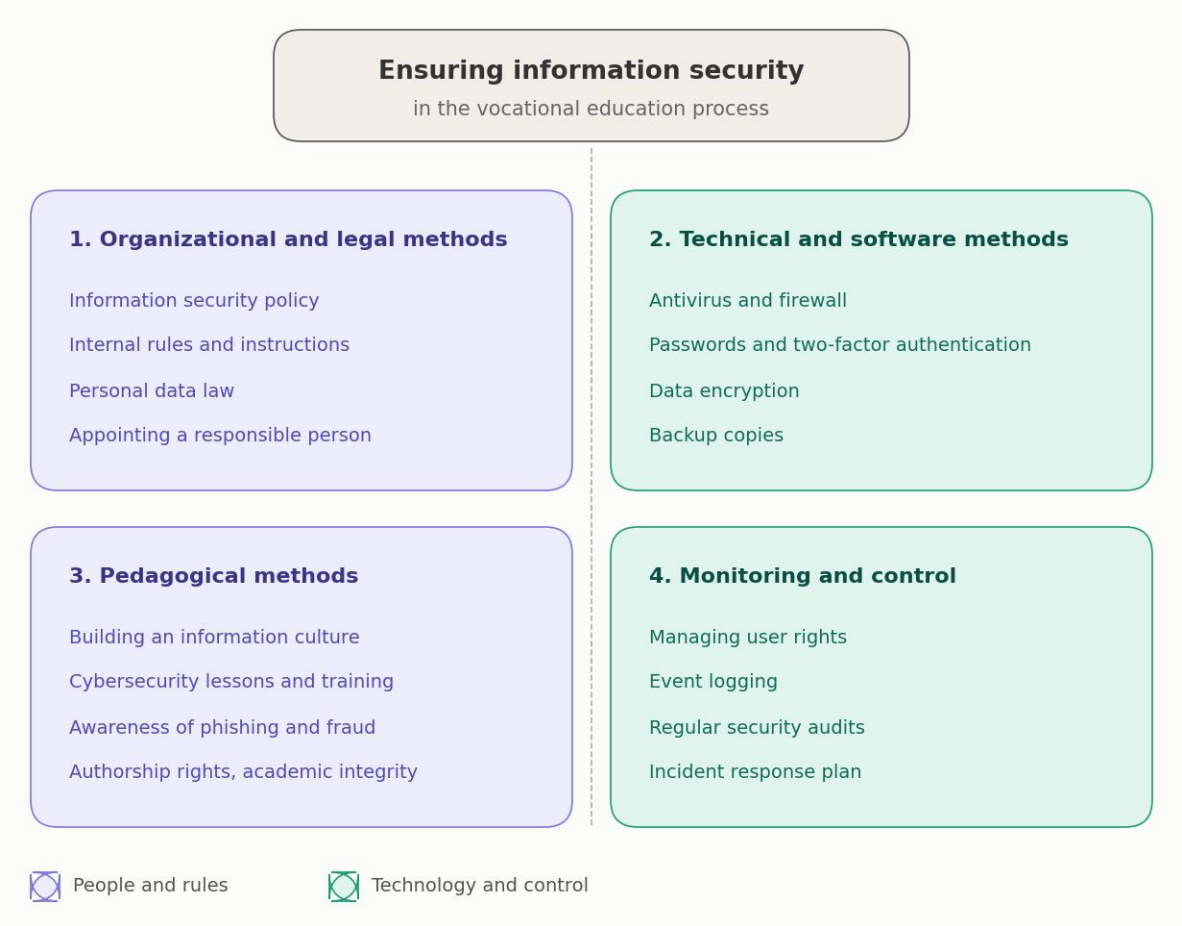
Aim and objectives of the research. The aim of the research is to identify effective methods of ensuring information security in vocational education institutions and to develop practical recommendations for protecting data in the digital learning environment.

To achieve this aim, the following objectives were set:

- to identify the main information security threats in the vocational education process;
- to study methods of protecting electronic learning resources and information systems;
- to outline ways of developing users' knowledge and skills in digital security;
- to develop recommendations for improving organizational and technical protection measures.

Research methods. In preparing the article, the use of scientific literature analysis, comparison, a systematic approach, and generalization is envisaged. These methods make it possible to classify the main directions for organizing information security in vocational education institutions and to develop proposals for eliminating existing problems.

© 2026Scottish International Conference on Multidisciplinary Research and Innovation. All Rights Reserved.



Information security is a set of organizational, technical, and software measures aimed at ensuring the confidentiality, integrity, and availability of information. In vocational education institutions, these requirements are of great importance for protecting students' personal data, electronic grades, attendance records, teaching and methodological materials, and administrative documents.





The following risks may occur in educational institutions:

© 2026Scottish International Conference on Multidisciplinary Research and Innovation. All Rights Reserved.

Technical methods of ensuring information security – In vocational education institutions, technical protection tools serve to defend information systems against external and internal threats.

Using strong passwords – Passwords should be sufficiently long, hard to guess, and not used on other systems. Storing passwords in open documents or sending them through messengers is not recommended.

Antivirus and protection software – It is necessary to use reliable protection software on the computers of the educational institution, to update its databases regularly, and to scan for malicious files.

Network security – Access between the institution's internal network, administrative computers, and the devices used by students must be restricted in an appropriate manner. Firewalls and secure Wi-Fi settings reduce the risk of unauthorized connections.

Software updates – Installing security updates for operating systems, browsers, and educational platforms on time reduces the likelihood of known vulnerabilities being exploited.

Data backup. Backup copies of electronic gradebooks, educational documents, and other important data must be created regularly. Backups should be stored separately from the main system in a protected location, and the ability to restore them should be tested periodically.

Conclusion. Ensuring information security in the vocational education process is an integral condition of the modern digital learning environment. When using e-learning platforms and information systems, it is important to protect the personal data of students and educators, preserve the integrity of educational documents, and ensure the uninterrupted operation of information resources.

Based on the analysis, the following conclusions were reached:

1. Alongside technical protection tools, organizational and pedagogical measures must also be applied to ensure information security.
2. Strong authentication, restriction of access rights, software updates, and data backup are among the main protection measures.
3. Regularly raising educators' and students' knowledge of cybersecurity reduces the likelihood of security breaches.
4. Regular monitoring of the state of information security and developing an incident response plan help ensure the continuity of the institution's operations.

References

1. Law of the Republic of Uzbekistan "On Personal Data", No. ZRU-547, July 2, 2019.
2. International Organization for Standardization. ISO/IEC 27001:2022. Information security management systems - Requirements. Geneva: ISO, 2022.
3. International Organization for Standardization. ISO/IEC 27002:2022. Information security controls. Geneva: ISO, 2022.
4. National Institute of Standards and Technology. The NIST Cybersecurity Framework (CSF) 2.0. NIST CSWP 29, 2024.
5. National Institute of Standards and Technology. SP 800-63B. Digital Identity Guidelines: Authentication and Lifecycle Management. NIST.
6. Cybersecurity and Infrastructure Security Agency. Secure Our World: Cybersecurity Awareness Resources. CISA.

© 2026Scottish International Conference on Multidisciplinary Research and Innovation. All Rights Reserved.