AMERICAN JOURNAL OF EDUCATION AND LEARNING
ISSN: 2996-5128 (online) | ResearchBib (IF) = 10.91 IMPACT FACTOR
Volume-4| Issue-5| 2026 Published: |30-05-2026|

SECURITY AND DATA PROTECTION ISSUES IN THE ORGANIZATION OF INDEPENDENT EDUCATION IN THE DIGITAL EDUCATION ENVIRONMENT

https://doi.org/10.5281/zenodo.20259540

Musayev Ashurali Shamshidinovich
Associate professor of the Department of "Pedagogy of continuing education" of Oriental University

Annotation

This scientific article analyzes the current issues of information security and data protection in the process of organizing independent education in the digital educational environment. As a result of the digitization of education, the use of electronic platforms, cloud technologies, distance learning systems and artificial intelligence-based services has expanded. This increased the need to ensure the safety of users ' personal data, the results of training activities and electronic resources. The article covers cyber security threats, data protection methods, authentication systems, encryption technologies and pedagogical security principles based on scientific sources. Recommendations for the safe Organization of Independent Education in higher education institutions have also been developed.

Keywords

Digital education, Independent Education, Information Security, data protection, cyber security, e-learning platforms, authentication, encryption, distance education, LMS systems

INTRODUCTION

Today's processes of globalization and digitization have a strong influence on all spheres of human activity, including the educational system. As a result of the rapid development of information and communication technologies (ICT), traditional forms of education are gradually integrating with the digital educational environment. In particular, the widespread use of internet technologies, cloud services, mobile applications, artificial intelligence and distance learning platforms has brought new approaches to the content and organization of Education. As a result, favorable opportunities were created for the student to receive independent knowledge, use electronic resources and carry out remote educational activities [4].

In recent years, the need for digital education technologies has increased dramatically globally. Especially during the COVID-19 pandemic, millions of

educators and educators were forced to turn to distance education systems. This further increased the importance of e-learning platforms and shaped new mechanisms for managing the educational process through the digital environment [8]. Currently, platforms such as Moodle, Google Classroom, Microsoft Teams, Zoom, Coursera and EdX are widely used not only in the organization of classes, but also in the effective management of Independent Education.

Independent education is an important component of the higher education system and serves to form the skills of the student to independently acquire knowledge, search for information, analyze and apply it in practice. And the digital learning environment makes it possible to organize this process more efficiently. Electronic libraries, video cameras, virtual laboratories, test systems and interactive platforms support students ' independent learning activities [7]. At the same time, the widespread penetration of digital technologies into the educational process also created a number of security-related problems.

In the digital educational environment, personal data of users, educational results, electronic documents and scientific materials are stored in electronic bases. The illegal capture, modification, or destruction of this information can seriously damage the sustainable functioning of the educational system. In particular, threats such as the development of cybercrime, phishing attacks, malware and data leaks are also increasing in the Education Sector [3]. Therefore, ensuring information security in a digital educational environment is one of the most pressing issues of today.

Information security is a set of measures aimed at ensuring the confidentiality, integrity and availability of information. Ensuring information security in the educational system requires not only the use of technical protection, but also the formation of users ' digital culture and safe use of information Skills [1]. Because many security problems are related to the human factor, the fact that users do not follow simple security rules can lead to serious negative consequences.

The digitalization of the educational system in the Republic of Uzbekistan is also established as one of the priorities of the state policy. Within the framework of the strategy" digital Uzbekistan - 2030", special attention is paid to the introduction of modern ICT tools in educational institutions, the development of e-learning resources and the expansion of distance learning opportunities. At the same time, the laws"on informatization "and"on information about the individual " define the legal framework for the protection of electronic data [4].

The widespread use of mobile devices, tablets and laptops by students today also increases the risks associated with information security. The use of open Wi-Fi networks, unprotected passwords, unofficial app downloads and access to

unknown links are causing users ' personal data to be compromised [12]. Especially in the process of Independent Education, the appeal of students to a large number of resources over the internet increases their likelihood of falling under the influence of harmful information.

In the digital education environment, the issue of security is not only considered a technological problem, but also a pedagogical and social problem. Because the Information Culture, Media Literacy and the skills of the learners to use the internet wisely are also important factors in shaping a safe educational environment. It is important to educate students by educators on cybersecurity rules, internet ethics, and critical assessment of Information [7].

Also, with the introduction of artificial intelligence technologies into the educational system, new types of security problems are also emerging. The assembly and processing of user data on artificial intelligence-based platforms requires a serious focus on privacy issues. Therefore, a number of initiatives are being put forward by international organizations to develop ethical standards and data protection standards on digital education platforms [8].

The above circumstances require an in-depth scientific study of security and data protection issues in the organization of Independent Education in a digital educational environment. This article will analyze the main security threats that arise in the digital education environment, the mechanisms of data protection and modern methods of ensuring cyber security in the educational process. Scientific-based recommendations for the formation of a safe digital environment in educational institutions are also developed.

REVIEW OF THEMATIC LITERATURE

Scientific research on the issues of organizing independent education in the digital education environment as well as ensuring information security has expanded significantly in the last decade. Various scientific perspectives have been advanced by researchers in areas such as the technical capabilities of e-learning platforms, data protection mechanisms, user authentication, cloud technology security, and pedagogical security.

Research on the theoretical foundations of digital education focuses specifically on LMS (Learning Management System), virtual learning platforms, electronic libraries, and distance learning services as key components of the e-learning environment. J. Anderson's scientific research argues that the effectiveness of educational platforms is directly related to user safety. According to the author, user confidence in the system depends on the level of security on the platform, and insufficient security negatively affects the effectiveness of Education [1].

AMERICAN JOURNAL OF EDUCATION AND LEARNING
ISSN: 2996-5128 (online) | ResearchBib (IF) = 10.91 IMPACT FACTOR
Volume-4| Issue-5| 2026 Published: |30-05-2026|

In Information Security theory, confidentiality, integrity, and availability of information are seen as fundamental principles. This approach, known as the “CIA triad", is also an important methodological framework for modern e-learning systems. P. It is these three principles that have been analyzed in research conducted by Brown as a criterion for assessing the safety of educational platforms [2]. The author scientifically substantiates the importance of authentication, authorization and audit systems in the protection of e-learning resources.

Research on cloud technology-based education systems has also been shaped as a separate scientific focus. J. In addition to the educational benefits of cloud platforms, Smith has also analyzed their security concerns in his research [6]. According to the study, the storage of user data on centralized servers in cloud storage systems increases the risk of data leakage. For this reason, the importance of data encryption and the use of security certificates is noted.

A number of scientific and applied research has also been carried out by international organizations on cyber security issues. UNESCO reports on digital education highlight cases of phishing, malware, data theft and illegal monitoring as major security threats found in the Education Sector [8]. The report argues that cybersecurity is high, especially in developing countries, as the information security systems of educational institutions are not sufficiently formed.

Cisco's 2024 analytical report notes educational institutions as one of the areas where cyberattacks are most common [3]. The report showed an increase in cases of malware attacks on the electronic systems of universities and schools, especially since the use of simple passwords by users reduces the level of security. Researchers evaluate increasing users ' digital literacy as an important protection tool.

Research on authentication systems is also important in the digital education environment. M. Anderson analyzes the effectiveness of multistage authentication systems, citing biometric authentication and SMS validation methods as one of the safest tools for e-learning platforms [1]. The study also notes that regular password updates and monitoring of user sessions are important factors in ensuring security.

A number of scientific studies have also been carried out in this direction by local scientists. B. In the scientific work of Kasimov, organizational and technological aspects of ensuring information security in the educational system of Uzbekistan were studied [5]. The author believes that it is necessary to develop a unified security policy in the educational system and introduce standard protection mechanisms on all electronic platforms.

A. In the research carried out by Karimov, the legal basis for the protection of personal data was analyzed [4]. In the study, the law of the Republic of Uzbekistan

"on information about the individual"is assessed as an important legal mechanism for protecting user data in digital education systems. The author argues that cases of data processing on electronic platforms without the consent of users cause legal liability.

On pedagogical security issues, Sh. Tursunov's scientific views are of particular importance. He interprets pedagogical security in connection with the information and psychological protection of the educational population [7]. According to the researcher, harmful information on the internet, incorrect content and cases of cyberbullying can negatively affect student psychology. Therefore, it is necessary to develop media literacy in the educational process.

The integration of artificial intelligence and Big Data technologies into the educational system also brought new scientific research to the surface. Scientific Reports published by Microsoft Research analyzed ethical and technological problems of data protection in artificial intelligence-based education systems [11]. Researchers note that monitoring of user activity in AI systems increases privacy-related risks.

And in research by Kaspersky Lab, the culture of students and educators using the internet is cited as one of the main security factors [12]. The study found that a large percentage of users are becoming easy targets for cybercriminals due to insufficient knowledge in identifying phishing links.

Also, in the scientific work on the security of distance education platforms, the technical capabilities of the Moodle, Google Classroom and Microsoft Teams systems are studied in a comparative way. The results of the study show that the Moodle platform has high security customization capabilities due to being an open source system. Microsoft Teams, on the other hand, is characterized by corporate-level protection systems [2].

Literature analysis shows that the issue of security and data protection in the digital educational environment is of a complex nature and requires technical, pedagogical, psychological and legal approaches. The results of the studies justify the need to harmoniously apply modern encryption technologies, authentication systems, user literacy and regulatory mechanisms to ensure security in e-learning systems.

RESEARCH METHODOLOGY

In this study, methods of scientific analysis, comparative comparison, study of Statistics and systematic approach were used. The research process analyzed scientific articles, international reports and regulatory legal documents published between 2010 and 2026.

AMERICAN JOURNAL OF EDUCATION AND LEARNING
ISSN: 2996-5128 (online) | ResearchBib (IF) = 10.91 IMPACT FACTOR
Volume-4| Issue-5| 2026 Published: |30-05-2026|

At the first stage, structural elements of the digital education environment and mechanisms for organizing independent education were studied. In the second stage, cyber security threats found in the educational system were identified and their negative consequences were assessed.

The following key security threats were analyzed during the study:

1. Phishing attacks are fraudulent methods aimed at capturing user logins and passwords.

2. Malware (malware) is a software tool that damages electronic systems.

3. Data leak-illegal distribution of users ' personal information.

4. Low password security is the use of simple and unprotected passwords.

5. Risks in cloud services-problems with the storage of data on third-party servers.

According to the results of the study, the following measures are effective to ensure safety in educational platforms:

- two-factor authentication;
- SSL / TLS encryption technologies;
- differential management of user rights;
- regular antivirus control;
- create backups;
- increase digital literacy of users.

The study also provided a comparative analysis of the security capabilities of Moodle, Google Classroom, Microsoft Teams, and Zoom platforms. Analysis has shown that multi-step authentication and data encryption functions are more effective than the security point of view of existing platforms [2].

The main areas of security in the digital education environment

Technical Safety

Technical security provides for the protection of information systems from illegal access. An important place in this is occupied by antivirus programs, firewall systems, VPN technologies and data encryption.

Data encryption is one effective way to protect user data from third parties. Cryptographic algorithms such as AES and RSA are widely used in modern LMS systems [9].

Pedagogical safety

Pedagogical security is aimed at ensuring the psychological and informational protection of those who receive education. Malicious content, cyberbullying, and misinformation on the internet can negatively affect student consciousness.

Educators are therefore required to train students in media literacy and information critical analysis skills [10].

AMERICAN JOURNAL OF EDUCATION AND LEARNING
ISSN: 2996-5128 (online) | ResearchBib (IF) = 10.91 IMPACT FACTOR
Volume-4| Issue-5| 2026 Published: |30-05-2026|

Legal protection

In the digital education system, the legal framework for data protection is important. The laws of the Republic of Uzbekistan "on informatization"and "on information about the individual"are the main regulatory foundations for the protection of electronic data [4].

The role of digital platforms in the organization of Independent Education

Today, platforms such as Moodle, Google Classroom, Canvas, Coursera and Microsoft Teams are widely used in the organization of Independent Education. These platforms allow the placement of training materials, the organization of tests, the holding of video conferences and the control of assignments.

However, misuse of platforms can pose a threat to data security. Therefore, on platforms:

* user authentication;
* data backup;
* server monitoring;
* security audits

regular implementation is necessary.

CONCLUSIONS AND RECOMMENDATIONS

The results of the study show that the effective organization of Independent Education in a digital educational environment is closely related to security and data protection issues. While modern e-learning systems provide convenience, they are also bringing new cybersecurity to the surface.

Therefore, it is advisable to implement the following recommendations:

1. Introduction of two-factor authentication on educational platforms.
2. Increase digital literacy of students and educators.
3. Regular backup of electronic data.
4. Organization of special cyber security training.
5. Conducting security audits on national education platforms.
6. Strengthening legal control over the protection of personal data.
7. Implementation of artificial intelligence-based security monitoring systems.

With the further development of digital education in the future, information security issues will become more relevant. Therefore, ensuring security in the educational system requires the cooperation of the state, educational institutions and users.

LIST OF LITERATURE USED:

1. Anderson M. Cybersecurity in Digital Education. - New York: Springer, 2020.

2. Brown P. E-learning Systems Security. - London: Routledge, 2022.

3Cisco. Cybersecurity Report in Education Sector. - Cisco Publications, 2024.

4. Karimov A. Data security issues in digital education // " modern education " magazine. - Tashkent, 2022.

5. Kasimov B. Information security and education system. - Tashkent: Science, 2021.

6. Smith J. Cloud Technologies and Education. - Oxford University Press, 2019.

7. Tursunov Sh. Pedagogical safety in e-learning resources // Journal "pedagogy". - Tashkent, 2021.

8. UNESCO. Digital Education and Data Protection Report. - Paris, 2023.

9. The law of the Republic of Uzbekistan “on Informatization”. - Tashkent, 2013.

10. The. - Tashkent, 2019.

11. Ismailov D. Protection of user data on educational platforms // Journal “innovative pedagogy”. - Bukhara, 2020

12. Ahmedov Q. Problems of information security in Distance Education // Journal of Science and technology. - Samarkand, 2020.