DOI: 10.63550/ICEIP.2025.63.77.016

Cybersecurity in Digital Education: Strategies for Protecting Student Data

Phuc Hau Nguyen[1][a], Shakhgiraev Ismail Uvaisovich[2][b], Bashiyeva Anzhela Khamidovna[3][c]
[1]*PhD., Lecturer, Faculty of Information Technology, Electric Power University, 235 Hoang Quoc Viet, Ha Noi city, Viet Nam*
[2]*Ph.D. in Economics, Associate Professor of the Department of Economics and Economic Security of Industries and Enterprises, Federal State Budgetary Educational Institution of Higher Education "Chechen State University named after A.A. Kadyrov", Grozny, Russian Federation*
[3]*Senior Lecturer Federal State Budgetary Educational Institution of Higher Education North Caucasian State Academy, Cherkessk, Russian Federation*
phuchauptit@gmail.com; haunp@epu.edu.vn, skorpio7878@mail.ru, bash-angel@mail.ru

Keywords: cybersecurity, digital education, data protection, learners, threats, cybercrime, information security.

Abstract: The article is devoted to issues of cybersecurity in digital education, with a particular focus on data protection strategies for learners. It discusses threats related to cybercrime and internal risks, such as unauthorized access and negligence by educational institution staff. The importance of developing knowledge and skills in cybersecurity among students, teachers, and staff is emphasized, as well as the need to integrate information protection principles into curricula. The author analyzes existing threats, such as phishing, cyberattacks, and data breaches, and explores methods for their prevention, including the use of cryptographic technologies, software updates, and multi-factor authentication. In the context of the COVID-19 pandemic, when many educational institutions transitioned to remote learning, the issue of protecting informational resources became particularly relevant. The article also highlights the importance of developing a comprehensive cybersecurity strategy, focusing on compliance with legal and technical standards, as well as creating effective systems for protecting personal data of students and teachers.

1 INTRODUCTION

Ensuring the protection of information and the confidentiality of students' data is a highly responsible and multifaceted task for educational institutions worldwide. Cybersecurity incidents in educational institutions can be caused by both external acts of cybercrime and internal threats related to unauthorized access or negligence by staff and other participants in the educational process.

Cybersecurity in the educational context is the process of developing knowledge and skills among users — students, teachers, educators, and faculty — regarding the existing threats they may face when interacting with various digital platforms such as social networks, messengers, online games, email, and instant messaging systems. In this regard, the primary responsibility of educational institutions, both secondary and higher, is the systematic dissemination of information about the risks associated with activities in the digital space, the elements that can undermine the quality of the educational process, as well as the integration of cybersecurity principles into the structure of curricula and documentation used by the teaching staff.

The study of current scientific works and publications, which provide a detailed analysis of key aspects of this issue, serves as the basis for the author's argumentation; identifying previously unresolved elements within the context of the overall problem.

V.I. Aleskerov and V.V. Baranov conduct an in-depth analysis of the threats posed by extremism in

[a] https://orcid.org/0009-0002-6080-2622
[b] https://orcid.org/0000-0002-6644-9519
[c] https://orcid.org/0009-0006-4693-9760

the digital space and its impact on modern society. In their work, they systematize and examine various strategic approaches used globally to counteract extremist activity in both real and virtual dimensions. After thoroughly evaluating existing methods and their effectiveness, the authors conclude that combating extremism on a global scale requires a comprehensive and multi-level approach, encompassing both legal and technical measures at various levels of society.

Considering the rapid progress of global information infrastructure, an increasing proportion of young people are exposed to the harmful influence of destructive elements within the online community, manifesting in forms of cyber extremism. This issue affects not only students of higher educational institutions but also pupils in secondary educational establishments. This topic was addressed in the research work of A. Bayteryakova titled "Prevention of Cyber Extremism in the School Education System."

O.A. Stepanova, G.A. Didenko, and O.N. Shvartskope conduct an in-depth study on the issue of developing college students' readiness to resist involvement in cyber-extremist activities. According to their view, this group of learners is at an increased risk due to specific psychological traits and a high degree of engagement in the information space. The authors' work emphasizes the implementation of a procedural aspect in the methodology for developing the readiness of students in technical fields, within which various educational methods, organizational forms of the learning process, and teaching tools are integrated.

The relevance of the studied issue is determined by the universal adoption of modern information and communication technologies in the educational sphere and the increasing demands for the quality and security of internet content. In the context of the COVID-19 pandemic, as well as the widespread transition of educational institutions to distance learning, the issue of protecting information and educational resources from numerous cyber threats has gained particular importance. The integration of digital platforms into the learning process has created new challenges for ensuring information security, which, in turn, requires the development of effective measures to counter cyberattacks, compliance with legal regulations, and minimization of the risks of personal data breaches. Information security has become a key factor in maintaining the reputation of educational institutions and preserving the trust of students and faculty members.

2 METHODOLOGY

The objective of this study is to conduct a detailed analysis of the key cybersecurity threats that educational institutions may face, as well as to develop a comprehensive and highly effective cybersecurity strategy aimed at significantly reducing the likelihood of successful cyberattacks. The primary goal is to ensure reliable protection of the confidential data of participants in the educational process (students, faculty, and administrative staff), as well as to create resilient mechanisms to counter both external and internal threats arising in the digital environment.

To achieve this objective, regulatory, legal, and methodological principles for the secure storage of information in educational institutions were identified and thoroughly analyzed, with adherence to these principles eliminating the risks of exposure to cyberextremism. The primary research approach involved the synthesis of theoretical foundations with a descriptive analytical method, providing a comprehensive exploration of the aspects under consideration.

3 RESULTS

Computer systems, communication technologies, and their users form a unified entity known as cyberspace. Progressive advancements in information technology contribute to the expansion and integration of cyberspace, making it an integral part of modern human existence. Cyberspace represents a key element in the context of the educational ecosystem, covering both secondary and higher education levels.

The modern educational model is undergoing significant transformations, with a shift from the traditional education system to intellectual, hybrid, and fully digital learning formats. In this context, the integration of information and communication technologies (ICT) into educational processes becomes not only relevant but also a necessary step, which inevitably leads to cyberspace continuing to function as a fundamental component of educational infrastructure. However, along with the obvious benefits that cyberspace brings to learning and teaching, it is also associated with potential risks, caused by insufficient caution and incomplete control on the part of the learners.

Each student has easy access to internet resources through computers or mobile devices, which leads to a variety of sources of cybersecurity threats in higher

education institutions. Let's consider several such sources:

Downloading educational materials from suspicious websites, which may lead to the installation of malicious software capable of infiltrating the computer networks of educational institutions and exposing them to the risk of infection.

Threats associated with the use of corporate email, including phishing attacks aimed at gaining access to confidential information such as user credentials, usernames, and passwords, for further exploitation.

Personal devices that are not equipped with adequate protection, which can become a vector for compromising the wireless network of an educational institution, increasing its vulnerability to potential attacks.

Targeted cyberattacks on educational organizations, including Distributed Denial of Service (DDoS) attacks, which can paralyze the operation of online resources, disrupting their functioning either partially or completely.

Threats originating from malicious or careless insiders who may inadvertently or deliberately contribute to the leakage of information or security breaches.

Students may be exposed to content on the global network that is inappropriate for their age and psycho-emotional state, including pornography, scenes of violence, promotion of smoking, drug addiction, suicidal tendencies, and other forms of self-harm. Such resources become accessible through email, social platforms, and other online channels, where students may carelessly disclose personal information, significantly increasing the risks of negative consequences for their physical and mental well-being.

When academic staff or students use their email accounts, bank accounts, or social media profiles, they often do not pay proper attention to information security issues, unaware of the risks associated with various methods that cybercriminals use to gain financial benefits. This lack of awareness leads to an underestimation of the reality of cyber threats and the ignoring of potential consequences of incidents such as identity theft or phishing attacks. Moreover, they often lack the necessary training to respond adequately to such incidents, which exacerbates the consequences for their digital well-being.

Awareness is the starting point in the process of minimizing incidents related to the theft of personal data and the emergence of information security threats. A significant portion of students and faculty members believe that having a unique password provides adequate protection for their accounts from potential cyber threats. However, unique passwords turn out to be an insufficient measure for ensuring the safety of confidential information. Modern hackers possess advanced knowledge in cryptography and highly effective technologies that allow them to decrypt passwords and extract valuable data.

The most detrimental consequences of any aggression against an educational institution are material losses, including fines for non-compliance with information security standards, as well as costs for recovery efforts following the incident.

The protection of the confidentiality of student and staff data is of critical importance not only for preventing financial losses but also for preserving the institution's reputation. Negative publicity can significantly reduce the attractiveness of an educational institution to potential applicants, as well as create barriers to cooperation with government agencies in the context of joint scientific and research initiatives.

Educational institutions need to mobilize significant resources to ensure highly effective protection of their users' personal data. Given the multitude of legislative acts and regulatory standards governing the education sector, meeting basic requirements can be an extremely labor-intensive and multitasking process. Nevertheless, this task can be optimized through the development of a comprehensive and highly effective information security strategy aimed at complying with all current legal and technical standards.

The initial phase in forming the aforementioned strategy will involve a comprehensive and in-depth risk assessment, including the identification of all valuable information resources processed and stored within the educational institution. At this stage, it is necessary to highlight the data that holds the greatest significance in terms of protection. Next, an analysis of potential cybersecurity threats, both external and internal, should be conducted, considering not only external attacks but also possible vulnerabilities within the organization. The final step in this process is a thorough diagnostic of the already implemented protection measures to identify and address existing weak points in the security system.

Ensuring the security of stored data is a priority task aimed at minimizing the likelihood of data leakage or damage. There are strictly regulated data protection principles that are essential for effectively countering cyber-extremism threats:

Systematic backup procedures. In the event that an attacker successfully executes an attack and extracts information, having up-to-date backup copies becomes an invaluable tool for cybersecurity

specialists. This will not only help identify compromised systems and applications but also restore data that has been damaged or lost as a result of the attack;

Periodic software updates, with a focus on protection tools, including antivirus solutions. Using outdated versions of software products carries significant risks, as these versions often contain known vulnerabilities actively exploited by cybercriminals for attacks;

Limiting access to sensitive information about students, faculty, and staff. Personal data of students and academic staff should only be accessible to authorized representatives of security and IT support services, adhering to strict regulations and a multi-level access control system;

Implementing cryptographic methods to protect confidential information from external threats, including hacker attacks and sabotage. Data encryption serves as the primary barrier against unauthorized access, providing reliable protection against information leaks and its potential use for criminal purposes;

Ensuring secure access to the institution's corporate networks through the use of multi-factor authentication (MFA), which significantly enhances the security of the authorization process and minimizes the risks of unauthorized intrusions, including cyberattacks and other forms of digital threats;

Appointing a responsible person for information security, who has the authority to manage the compliance with data protection standards, assess risks, conduct regular security audits, and monitor changes in regulatory requirements and respond to incidents. This is a key practice in higher education institutions to ensure a high level of protection for information resources.

4 DISCUSSION

Awareness of cybersecurity principles is a critically important element in protecting confidential data within the academic environment, encompassing both students and faculty in higher educational institutions. The personal and educational data of learners are at increased risk due to prolonged and intensive interactions with virtual spaces. This risk becomes especially evident in the context of educational processes organized through digital platforms or online courses. As students regularly use the internet for research, accessing academic materials, interacting with peers, and participating in virtual events, they become a vulnerable target for cybercriminals seeking to exploit their online activity.

A multitude of experts have reached a consensus that both learners and educational staff do not receive sufficient training in cybersecurity. This underscores the necessity of integrating a systematic approach to ensuring information security and ethical standards within the virtual environment across all levels of the educational process. As information and communication technologies continually evolve, the corresponding increase in potential threats makes the implementation of training programs focused on protecting personal data and confidential information extremely relevant for both students and educators.

5 CONCLUSIONS

Innovative technologies of the second half of the 21st century actively initiate discussions on globalization processes and the digitalization of educational systems, which have increasingly attracted attention in recent years. The modern reality, including the field of education, is undergoing significant changes, acquiring new forms of vibrancy and informativeness, driven by the widespread adoption of information and communication technologies. In the context of globalization trends, the issue of information security in the virtual environment has become critically important, as cyber threats driven by the actions of online fraudsters pose an increasingly serious danger to humanity.

In the context of higher education, training students and faculty in the field of cybersecurity and information protection is not only a necessary measure for their personal safety but also a crucial element in ensuring the long-term sustainability of digital spaces. The evolution of technologies requires the prompt adaptation of educational programs, which must be synchronized with the current challenges of information security. Cybersecurity, as a discipline, is one of the most intellectually demanding and complex fields, requiring deep interdisciplinary training. Therefore, higher educational institutions must integrate both theoretical and practical components into the curriculum, aimed at preparing specialists who can ensure the protection of data and infrastructure in the rapidly evolving technological landscape.

In-depth research is required on aspects related to improving strategies for countering various threats, including the ideological expansion of cyber extremism. Special attention is needed to analyze the key mechanisms of information security in

educational institutions, such as filtering and monitoring, with a focus on managing incoming and outgoing data flows. It is important to develop unified methodological recommendations for the implementation of software solutions that ensure comprehensive information protection, taking into account the specifics of different technical configurations and infrastructures of educational institutions.

REFERENCES

Abramova, Y., 2017. Artificial Intelligence in Cybersecurity. *Director of the Information Service.* No. 10, p. 12.

Shimko, M.V., 2018. Information Collection Systems in the Context of Cybersecurity. *Young Scientist.* No. 18 (204), pp. 28-39.

Kulik, S., 2018. Deadlocks in Cybersecurity. *Jewish Security: Events, Assessments, Forecasts.* No. 48 (64), pp. 2-4.

Aleskerov, V.I., Baranov, V.V., 2021. International Experience in Counteracting Extremism on the Internet. *Academic Thought.* No. 2 (15), pp. 122-128.

Bayteryakova, A., 2016. Preventing Cyberextremism in the School Education System. *Theory and Practice of Modern Science.* No. 11 (17), pp. 57-61.

Stepanova, O.A., Didenko, G.A., Shvartskop, O.N., 2020. Methodological Aspects of Forming IT Students' Readiness in Pedagogical Colleges to Counteract Cyberextremist Activities. *Azimuth of Scientific Research: Pedagogy and Psychology*. Vol. 9, No. 3 (32), pp. 244-247.

Kuzmin, V.V., 2018. Cybersecurity Strategies of Countries and Digital Diplomacy. *Student Science and the 21st Century.* No. 16-1, pp. 205-207.

Buryak, V.V., 2018. Cybersecurity Issues in the Information Society. Legal Fact. No. 32, pp. 25-31.

Grishin, M.N., 2018. Cybersecurity. Means and Methods of Cryptographic Information Protection. Materials of the XIX Regional Scientific and Practical Conference "Youth of the 21st Century: A Step into the Future". pp. 175-176.

Goryainova, N.V., 2018. Cybersecurity in the Modern World. Collection of Materials of the VIII All-Russian Scientific and Technical Conference "Student Science for the Development of the Information Society". pp. 66-68.