CLASSIFICATION AND MAIN TYPES OF CYBER THREATS TO THE EDUCATIONAL ENVIRONMENT

Verbovskyi Igor
Candidate of Pedagogic Sciences, Associate Professor
Head of Education Department
Associate Professor of the Department of Professional and Pedagogical, Special Education, Andragogy and Management
Zhytomyr Ivan Franko State University,
applicant for the second (master's) degree level of higher education in the specialty
125 Cybersecurity and Information Protection,
State University
«Zhytomyr Polytechnic», Ukraine

In the current context of digitalization of the educational process, the issue of cybersecurity is of particular importance for all levels of education. Educational institutions are actively introducing information and communication technologies, which, on the one hand, improves the quality and accessibility of education, and on the other hand, creates new vectors for cyber threats. The growing amount of personal data processed in educational institutions, as well as the use of various digital platforms, makes the educational environment an attractive target for cybercriminals. The lack of a proper culture of cyber hygiene, limited financial and human resources in educational institutions increase the risks of violating the confidentiality, integrity and availability of information. That is why the systematic classification and analysis of the main types

of cyber threats to the educational environment is an urgent task that requires scientific substantiation and practical implementation.

The issue of cyber threats in the educational environment of Ukraine is being actively studied by a number of domestic scholars who have made a significant contribution to the formation of theoretical and practical foundations of cybersecurity in educational institutions. In particular, Yu. Danyk and A. Zinchenko analyzed the formation of the cyber education system in Ukraine, emphasizing the need to introduce continuous cybersecurity training at all levels of education, which is a response to growing cyber threats in the education sector [2]. In her research, O. Evsyukova addresses the issue of standardizing the training of specialists in specialty «Cybersecurity», focusing on the importance of developing professional competencies to counter modern cyber threats in the digital society [3]. O. Kryvoruchko and I. Kostyk studied the issue of strategizing the information security of educational institutions, pointing out the need to adapt the best international practices to Ukrainian realities [4]. O. Trofymenko, N. Loginova, S. Manakov, and Ya. Dubovoi in their research classify the main cyber threats in the higher education sector, which allows institutions to clearly identify vulnerabilities and implement effective protection strategies [7]. Thus, there is a wide range of scientific works devoted to the classification and analysis of cyber threats to the educational environment, but the issues of systematization and adaptation of classifications to the current conditions of digitalization of education remain open.

Cyber threats to the educational environment are a multidimensional phenomenon that encompasses technical, organizational and social aspects. According to modern research, cyber threats in education can be classified according to various criteria, including the source of origin, method of implementation, object of attack, and consequences for the educational process. One of the most common classifications is the division of cyber threats into nine main classes: threats to IoT devices, threats due to human factors, identity theft, ransomware or malware, threats for financial gain, espionage, phishing, DDoS attacks, and threats to CMS (content management systems) [7].

Threats to IoT devices are becoming increasingly relevant due to the proliferation of smart classrooms, laboratories and campuses that use network-connected devices to automate and monitor the educational process. Insufficient security of such devices creates opportunities for unauthorized access, hacking, and their use in botnets to attack other infrastructure [5].

The human factor remains one of the key vectors of cyber threats. Insufficient awareness of employees and students of the basics of cyber hygiene, the use of weak passwords, and neglect of the rules of safe work with e-mail and suspicious files leads to successful phishing attacks, the spread of malware, and information leaks [5, 7].

Personal data theft is one of the most serious threats to educational institutions, as they process large amounts of information about students, teachers, parents, as well as financial and medical data [1, 5]. Attackers use the stolen data for further attacks,

blackmail, or sale on the black market. According to IBM, the average cost of a data breach in the education sector is one of the highest among all industries [6].

Ransomware and other malicious software are widely used to encrypt data of educational institutions for ransom. In recent years, there has been a significant increase in the number of attacks using ransomware, especially during periods of massive transition to distance learning [5, 6]. Losing access to educational resources, electronic journals and databases can lead to a halt in the educational process and significant financial losses.

Financially motivated attacks include not only ransom demands, but also fraud with electronic payments, falsification of scholarship or grant payments, and manipulation of financial documents of the institution [1, 6]. Espionage and unauthorized access to research, patent information and intellectual property pose an additional threat to universities and research institutions.

Phishing remains one of the most common methods of attacking educational institutions. Attackers send emails with fake links or attachments that mimic official messages from the administration or partners. According to Infosecurity Magazine, in 2023, 30 % of attacks on educational institutions were related to phishing [6].

DDoS attacks (distributed denial of service attacks) are aimed at disabling key educational services, such as e-journals, distance learning sites, or corporate email. As a result of such attacks, the educational process can be completely paralyzed for a long time, which negatively affects the quality of education and the reputation of the institution [1, 6].

Threats to CMS (content management systems) are associated with the use of outdated software versions, lack of regular updates, and incorrect security settings. This creates conditions for unauthorized access to the websites of educational institutions, posting malicious content or stealing confidential information [7].

Particular attention should be paid to insider threats that arise from the actions of employees or students who have access to critical systems. According to Arctic Wolf, more than 56% of internal incidents are related to human error, mishandling of data, or intentional actions [1].

It is worth noting that the introduction of modern information technologies in the educational process, including distance learning, cloud services, and mobile applications, significantly expands the surface of potential attacks. At the same time, limited funding, a lack of qualified IT professionals, and the absence of a systemic cybersecurity policy in many educational institutions make it difficult to implement effective protection measures.

To increase the level of cybersecurity in educational environments, researchers recommend implementing comprehensive strategies that include technical, organizational, and educational measures: regular software updates, multi-factor authentication, training staff and students in the basics of cyber hygiene, conducting security audits, backing up data, and developing incident response plans [5, 6]. It is also important to develop partnerships between educational institutions, government

agencies, and private companies to share experiences and implement best practices in cybersecurity.

The study found that the educational environment is one of the most vulnerable areas to modern cyber threats due to a combination of technological, organizational and social factors. The classification of the main types of cyber threats allows for a systematic approach to the development of effective protection strategies, taking into account the specifics of educational processes and resources. The most urgent threats are phishing, ransomware, DDoS attacks, personal data leaks, attacks on IoT devices and CMS, as well as threats related to the human factor. Given the dynamics of information technology development, educational institutions should implement comprehensive cybersecurity measures aimed at increasing the digital literacy of educational process participants, modernizing technical infrastructure, and developing partnerships to share experience in cybersecurity. Further research should be aimed at adapting international cybersecurity standards to the conditions of domestic education and developing innovative methods of countering the latest threats.

References

1. Arctic Wolf. (2024). 10 Cybercrimes Against Colleges and K-12 Schools, and How To Prevent Them. https://arcticwolf.com/resources/blog/cyber-attacks-against-schools-and-colleges/.
2. Danyk, Yu., & Zinchenko, A. (2018). Cyber education and its features. Military Education, (2), 67-84. https://doi.org/10.33099/2617-1783/2018-2/67-84
3. Evsyukova, O. (2021). Features of training of specialists in the field of cyber security: current challenges and prospects. Derzhavne upravlinnya: udoskonalennya ta rozvytok, 2. https://doi.org/10.32702/2307-2156-2021.2.2
4. Kryvoruchko, O., & Kostyk, I. (2020). Information security strategy. Cyberhygiene. Cubersecurity. State security: materials of scientific seminars. Kyiv National University of Trade and Economics, 12-13. https://knute.edu.ua/file/MjExMzA=/d8e24930571c0d91476be247343bb902.pdf
5. Microsoft Corporation. (2023). Cyber Signals issue 8: Education under siege. Microsoft Security Insider. https://www.microsoft.com/uk-ua/security/security-insider/intelligence-reports/cyber-signals-issue-8-education-under-siege.
6. Novikava, A. (2024). Cybersecurity in education: back to school, back to risks. NordLayer. https://nordlayer.com/blog/cybersecurity-challenges-in-education/.
7. Trofymenko, O., Loginova, N., Manakov, S. & Dubovoi, Ya. (2022). Cyberthreats in Higher Education. Electronic Professional Scientific Journal "Cybersecurity: Education, Science, Technique", 4 (16), 76-84. https://doi.org/10.28925/2663-4023.2022.16.7684