УДК 004.056.5: 37 (477)(045)

Лунгол Ольга Миколаївна, кандидат педагогічних наук, доцент, доцент кафедри оперативно-розшукової діяльності та інформаційної безпеки Донецького державного університету внутрішніх справ, м. Кропивницький, вул. Велика Перспективна 1, e-mail: olyalungol@gmail.com, https://orcid.org/0000-0001-8128-0072

ДОСЛІДЖЕННЯ СУЧАСНИХ КІБЕРЗАГРОЗ В ОСВІТНЬОМУ СЕРЕДОВИЩІ

Анотація. Внаслідок активного розвитку цифрового простору сучасне освітнє середовище все більше залежить від цифрових технологій та онлайн-платформ, впровадження яких відкриває нові види кіберзагроз для закладів освіти. Заклади освіти, здобувачі освіти та персонал уразливі до різноманітних кіберзагроз, які можуть поставити під загрозу безпеку даних, конфіденційність і порушити процес навчання. У статті показано найпоширеніші кіберзагрози в освітньому середовищі: фішинг, атаки програм-вимагачів, порушення конфіденційності даних, атаки на відмову в обслуговуванні (DDoS), які спрямовані на перевантаження онлайн-систем, мереж або веб-сайтів трафіком, інсайдерські загрози, коли особи в освітньому закладі зловживають їхні права доступу, методи соціальної інженерії тощо. У статті також проаналізовано особливості кібератак на заклади освіти в умовах воєнного стану, оскільки воєнний стан в Україні призвів до тривожного зростання кількості кібератак, націлених також на освітнє середовище. Щоб подолати сучасні кібернебезпеки, навчальні заклади повинні приділяти першочергову увагу заходам кібербезпеки. У статті зазначається, що важливим фактором у захисті освітнього простору від кіберзагроз є навчання викладачів, здобувачів освіти і співробітників передовим практикам безпеки даних, гігієни паролів та безпечної поведінки в Інтернеті. Важливим є впровадження надійної безпеки мережі, постійне оновлення програмного забезпечення та систем, а також налаштування протоколів для реагування на інциденти безпеки. Тісна співпраця з фахівцями з кібербезпеки, обмін найкращими практиками та інформування про нові загрози залишаються важливими факторами для підтримки безпечного освітнього середовища. Отже, предсталене у статті дослідження є актуальним і важливими для закладів освіти, оскільки допомагає їм підготуватися до зростаючих кіберзагроз і забезпечує безпеку даних та конфіденційність інформації, що є критичними для успішного навчання та функціонування у цифровому світі.

Ключові слова: заклади освіти, кіберзагрози, персональні дані, фішингові атаки, кібербулінг, атаки програм-вимагачів, захист даних.

Lunhol Olha, PhD in Pedagogical Sciences, Docent, Associate Professor of the Department of Operational-search Activities and Information Security of Donetsk

State University of Internal Affairs, Kropyvnytskyi, Velyka Perspektyvna 1, e-mail: olyalungol@gmail.com, https://orcid.org/0000-0001-8128-0072

RESEARCH OF MODERN CYBER THREATS IN THE EDUCATIONAL ENVIRONMENT

Abstract. As a result of the active development of the digital space, the modern educational environment is increasingly dependent on digital technologies and online platforms, which have opened up new types of cyber threats. Educational institutions, students and staff are vulnerable to various cyber threats that can compromise data security, privacy and disrupt the learning process. The article shows the most common cyber threats in the educational environment: phishing, ransomware attacks, data privacy violations, denial of service (DDoS) attacks aimed at overloading online systems, networks or websites with traffic flow, insider threats when individuals in educational institution abuse their access rights, social engineering methods, etc. The article also analyzes the peculiarities of cyberattacks on educational institutions in times of war, as the state of war in Ukraine has led to a troubling increase in cyberattacks targeting the educational environment as well. To overcome modern cyber threats, educational institutions should prioritize cybersecurity measures. The article notes that an important factor in securing the educational space from cyber threats is the training of teachers, students and staff in best practices for data security, password hygiene and safe behavior on the Internet. It is essential to implement reliable network security, regularly update software and systems, and configure protocols for responding to security incidents. Close collaboration with cybersecurity experts, the exchange of best practices, and staying informed about new threats remain important factors in maintaining a secure educational environment. So, the research presented in the article is relevant and important for educational institutions as it helps them prepare for the growing cyber threats and ensures the security of data and confidentiality of information, which are critical for successful learning and functioning in the digital world.

Key words: educational institutions, cyber threats, personal data, phishing attacks, cyberbullying, ransomware attacks, data protection.

Introduction. Modern cyber threats pose significant challenges in the educational environment. With the increasing reliance on technology for teaching, learning, and administrative tasks, educational institutions have become prime targets for cybercriminals seeking to exploit vulnerabilities and gain unauthorized access to sensitive data.

One of the prevalent cyber threats in the educational sector is phishing. Cybercriminals send deceptive emails, messages, or websites disguised as legitimate entities to trick students, faculty, or staff into revealing personal information, login credentials, or downloading malware-infected files. Phishing attacks can lead to identity theft, unauthorized access to systems, and compromise of sensitive data.

Ransomware attacks have also become a major concern in the educational sector. Malicious software encrypts valuable data and demands a ransom for its release. These attacks can cripple educational institutions, disrupt operations, and compromise the privacy of students and staff members.

Data breaches pose a significant risk to educational institutions, as they store a vast amount of personally identifiable information and academic records. Cybercriminals target these databases to obtain sensitive data for identity theft, financial fraud, or selling on the dark web. The consequences of a data breach can be severe, including reputational damage, financial losses, and legal implications.

The proliferation of connected devices in educational environments has introduced new vulnerabilities. Internet of Things (IoT) devices such as smartboards, surveillance cameras, and connected classroom tools may lack proper security measures, making them potential entry points for cyber attacks. Compromised IoT devices can be exploited to gain unauthorized access to networks or launch Distributed Denial of Service (DDoS) attacks.

To address these modern cyber threats, educational institutions must prioritize cybersecurity measures. This includes implementing robust network security, regularly updating software and systems, conducting security awareness training for students and staff, and establishing incident response protocols. Collaboration with cybersecurity experts, sharing best practices, and staying updated on emerging threats are crucial for maintaining a secure educational environment.

Educational institutions play a vital role in not only imparting knowledge but also protecting the privacy and security of their students and staff. By proactively addressing modern cyber threats, they can create a safe digital space for learning and ensure the integrity and confidentiality of their educational ecosystem.

Analysis of modern research and publications. The work of many domestic and foreign scientists is devoted to the problem of combating cyber threats. We analyzed the works of domestic and foreign scientists dedicated to the study of modern cyber threats in the educational environment, including in the conditions of martial law in Ukraine.

Thus, Uzoqov A. and Abdullaev A. (Uzoqov, 2022) note that the processes of informatization and the problems of cybersecurity in the educational environment are interrelated. The authors focus on the fact that with the development of information technologies and widespread digitalization, a trend of large-scale use of new communication technologies in the field of education, organization of the educational process, control of knowledge, etc. has emerged, which contributes, accordingly, to the growth of cyber threats for participants in the educational process.

Pinchuk O. and Prokopenko A. (Pinchuk, 2021) point out in their research the actual problem of using unreliable, unscientific information or disinformation from the Internet during the preparation and/or conducting of educational classes, the lack of protection of information from e-mails of students, the use of Internet resources from open sources and means of electronic communications.

Burov O., Butnik-Siversky O., Orliuk O. and Horska, K. (Burov, 2020) consider interaction of innovation, cybersecurity, and digital education environment. They point out that the issues of innovation in the digital learning environment

exacerbate the issues of cybersafety of the education process participants. Scientists are working on the development of a general model of cyber threats in the field of education and ways to avoid them.

Noran Sh. (Noran, 2021) focuses on cybersecurity specifically in the higher education sector as an area of scientific research and analysis, and draws attention to the exponential growth of cyber threats to colleges and universities around the world, especially in the wake of the COVID-19 pandemic.

Having analyzed the directions of domestic and foreign scientists (Uzogov, 2022; Pinchuk, 2021; Burov, 2020; Noran, 2021) and based on our own scientific research (Lunhol, 2022; Lunhol, 2023; Lysenko, 2023), we concluded that the digital space is rapidly and actively changing, transforming, expanding, which leads to the appearance of new and new cyber threats, including in the field of education. A special factor that negatively affects the digital educational environment in Ukraine is the state of war and the increase in the number of cyber attacks. Therefore, the aim of the article is to explore and analyze the various cyber threats that exist within educational institutions, to provide a comprehensive understanding of the current cyber threat landscape in the educational sector, focusing on the risks, vulnerabilities, and potential impacts these threats pose. Through research and analysis, the article aims to identify and categorize the different modern types of cyber threats that target educational institutions, such as data breaches, phishing attacks, ransomware, and compromised online platforms etc.

The relevance of the study is also confirmed by the works of Ankita Sharma (Assistant Professor CSE, Chandigarh University Punjab, India) who notes that scientists, students and universities around the world are constantly under cyber attacks. Ankita sharma confirms this also with large-scale educational surveys (Sharma, 2022).

To achieve the aim of the article used the complex of theoretical and empirical research methods. In the course of the research author analyzed pedagogical and professional literature in the field of digital technologies and cybersecurity (comparison and juxtaposition of different scientific views on the problem of cyber threats in the educational environment); empirical – observation, survey to determine the level of cyber attacks on educational institutions of Ukraine. The peculiarities of cyberattacks on educational institutions under martial law are analyzed.

Main material. In the modern digital era, educational institutions face numerous cyber threats that can significantly impact their operations, sensitive data, and the overall learning environment. These cyber threats pose serious risks to the confidentiality, integrity, and availability of educational systems, as well as the personal information of students, faculty, and staff. Understanding and addressing these threats are crucial to maintaining a secure educational environment, especially in the context of hybrid warfare in Ukraine.

One of the prevalent cyber threats in the educational environment is data breaches. Educational institutions collect and store vast amounts of personal information from students, including names, addresses, contact details, academic records, and sometimes even financial information. This data is highly valuable and attractive to cybercriminals who seek to exploit it for malicious purposes. Theft of

personal data can occur through various means, such as data breaches, hacking incidents, or insider threats. Cybercriminals may target educational institutions to gain unauthorized access to their databases and steal sensitive information. They can exploit vulnerabilities in network infrastructure, weak security practices, or social engineering techniques to obtain personal data. The consequences of personal data theft can be severe for students and teachers. It can lead to identity theft, financial fraud, and even reputational damage. Stolen personal information can be used to commit fraudulent activities, open unauthorized accounts, or impersonate individuals, causing significant financial and emotional distress. Moreover, the theft of personal data erodes trust in educational institutions. Students and their families expect their personal information to be handled securely and with utmost confidentiality. When data breaches occur and personal information is compromised, it can damage the reputation of the institution and erode the confidence of students.

To prevent the theft of personal data, educational institutions should prioritize cybersecurity and implement robust security measures. This includes implementing secure data storage practices, encrypting sensitive information, regularly updating and patching systems, and conducting thorough risk assessments. It is crucial to educate staff and students (Lunhol, 2022; Lunhol, 2023; Lysenko, 2023) about cybersecurity best practices, such as strong password management, phishing awareness, and the importance of reporting suspicious activities. In addition, compliance with data protection regulations, such as the General Data Protection Regulation (GDPR, n.d.)., the Law of Ukraine On the Protection of Personal Data (On Protection of Personal Data, 2022) or other relevant local laws, is essential. Institutions should establish protocols for incident response and have a contingency plan in place to effectively handle data breaches and mitigate their impact.

By taking proactive measures to safeguard personal data, educational institutions can protect education seekers from the theft of their personal information. Maintaining strong cybersecurity practices not only helps prevent data breaches but also preserves the trust and confidence of students and their families in the educational institution's commitment to their privacy and security.

Phishing attacks are also a significant concern in the educational sector. Phishing attacks in the educational sector have become a significant concern in recent years. Phishing is a cyber attack technique where malicious actors attempt to deceive individuals into revealing sensitive information, such as login credentials, financial details, or personal data, by posing as a trustworthy entity.

Educational institutions are attractive targets for phishing attacks due to the large number of students, faculty, and staff who use online platforms and email systems for communication and accessing educational resources. Phishing attacks in the educational sector can have several objectives, including identity theft, financial fraud, unauthorized access to institutional systems, and data breaches.

Phishing attacks can take various forms, such as deceptive emails, fake websites, or fraudulent login pages. Cybercriminals often craft convincing messages that appear to be from legitimate sources, such as the institution's administration, IT department, or popular online services. These messages often create a sense of

urgency or exploit current events to prompt recipients to take immediate action, such as clicking on a malicious link or providing their login credentials.

The consequences of falling victim to a phishing attack can be severe for individuals and educational institutions. Compromised accounts can lead to unauthorized access to sensitive data, including student and employee records, financial information, and intellectual property. Data breaches resulting from successful phishing attacks can have legal, financial, and reputational implications for educational institutions, as they are responsible for safeguarding the privacy and security of their stakeholders' information.

To combat phishing attacks in the educational sector, institutions should prioritize cybersecurity awareness and education. Regular training programs and campaigns can help students, faculty, and staff recognize the signs of phishing attempts, understand the risks associated with phishing, and learn best practices to protect themselves and the institution.

Implementing robust email filtering and anti-phishing technologies can also help detect and block phishing attempts before they reach recipients' inboxes. Multi-factor authentication (MFA) should be encouraged as an additional layer of security to protect accounts from unauthorized access.

Furthermore, fostering a culture of vigilance and encouraging individuals to report suspected phishing attempts can enable quick response and mitigation. Institutions should establish clear incident response protocols to address phishing incidents promptly, including investigating the source of the attack, notifying affected individuals, and implementing necessary security measures to prevent future attacks.

By raising awareness, implementing technological safeguards, and promoting a proactive cybersecurity mindset, educational institutions can mitigate the risk of phishing attacks and protect their students, faculty, and staff from falling victim to these malicious schemes.

Ransomware attacks in the educational environment have become a significant and growing threat in recent years. Ransomware is a type of malicious software that encrypts critical data and holds it hostage until a ransom is paid, typically in the form of cryptocurrency. Educational institutions are particularly vulnerable to these attacks due to their reliance on digital systems and the valuable data they possess.

When a ransomware attack occurs, the attacker gains unauthorized access to the institution's network or systems and encrypts important files and data, making them inaccessible to the institution. This can include student records, financial information, research data, and other critical resources. The attacker then demands a ransom payment in exchange for the decryption key needed to regain access to the encrypted data.

The consequences of a successful ransomware attack can be severe for educational institutions. It can disrupt regular operations, impact teaching and learning activities, and jeopardize the privacy and security of sensitive information. Institutions may face financial losses, reputational damage, and legal implications if they are unable to restore their systems and recover the encrypted data.

Preventing and mitigating ransomware attacks requires a multi-faceted approach. Educational institutions should prioritize cybersecurity measures to reduce

the risk of an attack. This includes implementing robust network security, regularly patching and updating software, utilizing firewalls and intrusion detection systems, and employing strong access controls and user authentication mechanisms.

Creating regular backups of critical data is also crucial. Backups should be stored securely and offline to prevent them from being compromised during an attack. In the event of a ransomware incident, institutions can restore their systems and data from backups, minimizing the impact of the attack.

Education and awareness are vital in combating ransomware threats. Institutions should educate staff, faculty, and students about the risks of ransomware, train them to recognize phishing emails and suspicious links, and emphasize the importance of safe online practices, such as avoiding downloading files from untrusted sources.

Additionally, having an incident response plan in place is crucial. This plan should outline the steps to be taken in the event of a ransomware attack, including isolating infected systems, notifying appropriate authorities, engaging cybersecurity experts for assistance, and communicating with affected individuals.

By implementing strong cybersecurity measures, raising awareness, and having robust incident response plans in place, educational institutions can better protect themselves against ransomware attacks. Proactive measures and preparedness are key to minimizing the impact of such attacks and ensuring the continuity of teaching, learning, and research activities in the educational environment.

The compromise of remote learning platforms and online classrooms has emerged as a significant cyber threat in the educational landscape. As educational institutions increasingly rely on digital platforms to facilitate remote learning, cybercriminals have identified these platforms as lucrative targets for their malicious activities.

When remote learning platforms and online classrooms are compromised, it can have detrimental effects on the educational process. Cybercriminals may exploit vulnerabilities in these systems to gain unauthorized access, disrupt classes, steal sensitive data, or engage in other malicious activities. The consequences can range from interruptions in teaching and learning to privacy breaches and data theft.

One of the primary concerns is the potential exposure of sensitive student and faculty information. Remote learning platforms often store personal data, such as names, email addresses, and sometimes even financial information. If these platforms are compromised, cybercriminals can gain access to this information, leading to identity theft, financial fraud, or other forms of misuse.

Another significant concern is the disruption of online classes. Cybercriminals may employ tactics such as Distributed Denial of Service (DDoS) attacks to overwhelm the platforms, rendering them inaccessible or causing significant delays and interruptions. This can negatively impact the learning experience, impede student engagement, and create frustration among both students and educators.

Furthermore, compromised remote learning platforms can enable unauthorized access to online classrooms, allowing individuals with malicious intent to infiltrate discussions, share inappropriate content, or engage in cyberbullying. This poses risks to the safety and well-being of students and can create a hostile learning environment.

To mitigate the compromise of remote learning platforms and online classrooms, educational institutions should prioritize cybersecurity measures. This includes implementing robust security protocols, regularly updating and patching systems, conducting vulnerability assessments, and employing strong access controls and authentication mechanisms.

Educational institutions should also educate students, faculty, and staff about the importance of safe online practices. This includes promoting the use of strong passwords, raising awareness about phishing attempts and social engineering tactics, and providing guidance on how to report suspicious activities.

Regular monitoring and auditing of remote learning platforms can help identify and respond to potential security breaches promptly. It is essential to have incident response plans in place to address any compromises effectively, including isolating affected systems, conducting forensic investigations, and notifying relevant authorities.

Collaboration with cybersecurity experts and leveraging their expertise can enhance the security posture of remote learning platforms. Institutions should also prioritize ongoing security training and professional development for IT staff responsible for managing and securing these platforms.

By adopting a comprehensive approach to cybersecurity, educational institutions can minimize the risk of compromise to remote learning platforms and online classrooms. Protecting the privacy, data, and educational experience of students and educators is crucial in ensuring a safe and secure remote learning environment.

A prevalent cyber threat in the educational environment is cyberbullying. Cyberbullying posing serious risks to the well-being and safety of students. It involves the use of digital technologies, such as social media, messaging apps, or online forums, to harass, intimidate, or humiliate others.

In the context of education, cyberbullying can occur among students, and sometimes even involve teachers or other staff members. It can take various forms, including sending threatening or derogatory messages, spreading rumors or false information, sharing private or embarrassing photos or videos without consent, or creating fake profiles to impersonate and defame others.

The consequences of cyberbullying can be severe and far-reaching. It can negatively impact a student's emotional and psychological well-being, leading to stress, anxiety, depression, and even suicidal thoughts. Victims of cyberbullying may experience social isolation, decreased academic performance, and reluctance to attend educational establishment or engage in educational activities.

Furthermore, cyberbullying creates a hostile and unhealthy learning environment. Students who are targeted may feel unsafe, anxious, or fearful, which can significantly hinder their ability to focus on their studies and participate in classroom activities. It also disrupts the overall dynamics of the educational community, undermining trust, respect, and collaboration among students and educators.

Preventing and addressing cyberbullying requires a multi-faceted approach involving various stakeholders. Educational institutions should establish clear

policies and guidelines regarding acceptable online behavior, explicitly condemning cyberbullying and outlining consequences for those who engage in such behavior. These policies should be communicated to students, parents, and staff members, emphasizing the commitment to maintaining a safe and inclusive learning environment.

Educational institutions should also prioritize education and awareness-raising initiatives. Students should be educated about the potential dangers of cyberbullying, the importance of empathy, respect, and responsible online behavior. It is crucial to foster a culture of digital citizenship that promotes kindness, tolerance, and constructive communication.

In addition, schools should encourage an open dialogue and provide channels for reporting incidents of cyberbullying. Students should feel comfortable speaking up and seeking help when they encounter or witness cyberbullying. Timely and appropriate interventions, including counseling, mediation, or disciplinary actions, should be implemented to support victims and hold perpetrators accountable.

Collaboration with parents, teachers, counselors, and other relevant professionals is essential in addressing cyberbullying effectively. By working together, educational institutions can create a safer digital learning environment that promotes positive interactions, empathy, and respect, fostering the overall well-being and academic success of students.

Martial law in Ukraine has led to an alarming increase in cyberattacks targeting the educational environment also. These attacks pose significant risks to the security and integrity of educational institutions, their systems, and the sensitive data they hold. During martial law, educational institutions are more vulnerable to cyberattacks due to potential disruptions in the overall security infrastructure. With limited resources and increased focus on other areas of concern, to cybersecurity measures may not receive adequate attention, making educational institutions attractive targets for malicious actors. Phishing attacks, including spear-phishing, become more prevalent during martial law. Cybercriminals exploit the uncertain and stressful environment to trick individuals into revealing sensitive information or clicking on malicious links, leading to unauthorized access or data breaches. Some educational institutions experience targeted ransomware attacks aiming to encrypt data and demand a ransom for its release. DDoS attacks disrupt some online learning platforms, communication systems, and other critical infrastructure, that causing significant disruptions to educational activities.

Conclusion. To mitigate these modern cyber threats, educational institutions need to implement robust cybersecurity measures. This includes regular security awareness training for students, faculty, and staff, promoting strong password practices, implementing multi-factor authentication, keeping software and systems up to date with the latest security patches, and conducting regular security audits and risk assessments. Collaboration with cybersecurity experts and adopting advanced threat detection and response systems are also essential to detect and respond to cyber incidents effectively.

Educational institutions must prioritize cybersecurity as a fundamental aspect of their operations. By investing in robust cybersecurity measures, fostering a culture

of security awareness, and staying vigilant against evolving cyber threats, they can create a safer and more resilient educational environment for students, faculty, and staff. Countering cyberattacks is especially relevant for an educational environment in martial law.

References:

1. Burov, O., Butnik-Siversky, O., Orliuk, O., & Horska, K. (2020). Cybersecurity and innovative digital educational environment. *Information Technologies and Learning Tools*, 80(6), 414–430. https://doi.org/10.33407/itlt.v80i6.4159 [in English].
2. GDPR Summary. (n.d.). General Data Protection Regulation. Retrieved July 10, 2023, from http://surl.li/jcatq [in English].
3. Lunhol, O. (2023). Features of using information technologies in law enforcement. *Udoskonalennia profesiinoi kompetentnosti vykladacha yurydychnykh dystsyplin : Vseukr. nauk.-ped. pidvyshch. kvalif.* 82–84 [in English].
4. Lunhol, O.M. (2022). Cybersecurity of society in a hybrid war. *Zabezpechennia publichnoi bezpeky i poriadku v umovakh voiennoho stanu : Vseukr. nauk.-prakt. konf.* 238–240 [in English].
5. Lysenko, O.V., Lunhol, O.M., & Haborets, O.A. (2023) Law enforcement information and analytical support. *Current issues in modern science.* 3(9) 281–291 [in English].
6. Noran, Sh.F. (2021). Securing higher education against cyberthreats: from an institutional risk to a national policy challenge. *Journal of Cyber Policy*, 6:2, 137-154, https://doi.org/10.1080/23738871.2021.1973526 [in English].
7. On Protection of Personal Data. (2022). Law of Ukraine. Document 2297-VI. Verkhovna Rada of Ukraine. Official web-portal of the Parliament of Ukraine. Legislation of Ukraine. https://zakon.rada.gov.ua/laws/show/en/2297-17#Text [in English].
8. Pinchuk, O.P. & Prokopenko, A.A. (2021). Suchasni problemy kiberbezpeky u navchalnomu seredovyshchi zakladu viiskovoi osvity [Modern problems of cybersecurity in the educational environment of military education]. *Innovatsiini transformatsii v suchasnii osviti: vyklyky, realii, stratehii: zbirnyk materialiv III Vseukrainskoho vidkrytoho naukovo-praktychnoho onlain-forumu*. 73-75.
9. Sharma, A. (2022). Review on Major Cyber security Issues in Educational Sector. *International Journal of Computer Sciences and Engineering*. 9. https://doi.org/10.26438/ijcse/v9i12.2629 [in English].
10. Uzoqov, A.M., & Abdullaev, A.S. (2022). Informatization of education and cybersecurity issues in the educational environment. *Science and innovation*, 1 (B3), 758-762. https://doi.org/10.5281/zenodo.6798289 [in English].