Legal Challenges and Perspectives of Cybersecurity in the System of State Governance of Educational Institutions in Ukraine

Herasym Dei[1,*], Dmytro Shvets[2], Nataliia Lytvyn[3], Olena Sytnichenko[4] and Olena Kobus[5]

[1]*Department of Public Administration and Project Management, University of Educational Management, Ukraine*
[2]*Rector of Odessa State University of Internal Affairs, Ukraine*
[3]*Doctor of legal sciences, Professor, Ukraine*
[4]*Department of Legal Support of Business Security of the State University of Trade and Economics, Ukraine*
[5]*Educational and Scientific Institute Information Security National Academy of the Security Service of Ukraine, Ukraine*
E-mail: herasym_dei@edu.cn.ua; dmytro_shvets@sci-univ.com; nataliia_lytvyn@edu-knu.com; olena_sytnichenko@pltch-sci.com; kobus_olena@ukr.net
[*]*Corresponding Author*

Received 25 October 2023; Accepted 13 May 2024

Abstract

The aim of this research is to provide a detailed analysis of the basics of cybersecurity, define the essence of cybersecurity and its characteristics in the system of state governance of educational institutions, determine the prospects for such provision, and take into account all possible legal challenges facing such provision. The study used a number of general and special methods of scientific knowledge, such as the method of systematic analysis

Journal of Cyber Security and Mobility, Vol. 13_5, 963–982.
doi: 10.13052/jcsm2245-1439.1357

and synthesis, the dialectical method, the normative method and the method of studying legal documents. In general, the author identifies the peculiarities of cybersecurity, analyses in detail the current state of cybersecurity in the system of public administration of educational institutions and provides examples of large-scale hacker attacks on universities, the conclusions from which are important for improving the protection of the educational system; outlines the main legal challenges that arise in the course of ensuring cybersecurity of educational institutions and which must be overcome in order to effectively identify and neutralise potential threats; highlights the prospects that arise in this light and which are likely to bring the desired result within the framework of Ukraine's future European integration.

Keywords: Cybersecurity, education, educational institutions, state administration, information space.

1 Introduction

The 21st century cannot be described without the digital world and the information space, which are gaining momentum and improving every day. At the same time, various spheres of society are improving, simplifying important processes and saving a lot of time and resources. Along with such high-speed processes and a significant expansion of opportunities, there are significant security threats to those who use them. First and foremost, of course, we are talking about the protection of personal data and the improvement of potential systems for its protection and maintenance. At the same time, ensuring cybersecurity and information security in general is perhaps the most important task due to the rapid globalisation and informatisation of civil society, the growing number of threats in the Internet space, and the increasing intensity of cyberattacks (Mozhaiv et al., 2019). Moreover, we cannot ignore the ingenuity of cybercriminals, as a few years ago, cyberattacks were limited to government agencies, the defence sector and banking institutions, but now cyberattacks on educational institutions and the system of public administration of educational institutions in general have become relevant. Therefore, it is not surprising that scholars and legislators from various countries, including Ukraine, are paying considerable attention to the study of cybersecurity, the challenges it faces and the future prospects for its provision.

On its way to European integration, Ukraine has to implement a number of transformations, amendments to legislation and many reforms to ensure

a better future for its people. The issue of cybersecurity is no exception, especially during the period of active hostilities, when there is a cyber front alongside the real combat front. The main cyber threat to Ukraine is Russia, which on the eve of February 2022 carried out a series of cyberattacks on government agencies, defence structures and local governments (Ukrinform, 2022a; Ukrinform, 2022b; Ukrinform, 2022c). At the same time, other areas remain under threat, such as the education sector, which is also often subject to cyberattacks. For example, in July 2023, the Unified State Electronic Database on Education (USEDE), through which applicants apply for admission, was cyberattacked by Russia. Access to the database has been restored, but this is not the last attempt by Russia to obtain the data of ordinary Ukrainians to use it for its criminal purposes in the future (Ukrinform, 2023).

Therefore, it is not surprising that there is a broad interest and need to ensure cybersecurity at all levels. That is why, in the framework of our study, it will be expedient to define and provide a detailed description of the concept of "cybersecurity". There is no single vision of the phenomenon of cyberspace in the scientific literature, but each scholar, in a detailed analysis of the features visible in cyberspace, forms his or her own unique vision of this phenomenon and characterises it in his or her own way, without moving away from its foundations. Therefore, it is logical that the scale of modern transformations in the information sphere raises theoretical and practical problems that require a detailed description of the concept of cybersecurity and making it more systematic and powerful.

In his research, Kormych (2003) describes cybersecurity as the process of protecting legally defined rules that control information processes in the country and ensure the conditions for the development of society, the state and the citizen provided for by the Constitution of Ukraine. At the same time, a number of scholars, led by Lisovska (2019) provides her own definition of the concept of "cybersecurity" and indicate that it is a certain state of security of the state, society and individual, in which there is active information, intellectual, technical, socio-political development and during which no external information influences harm such development (Lisovska, 2019). In turn, Kaliuzhnyi (2002) notes that cybersecurity is a type of information legal relations that arise in the course of creating and protecting safe conditions for the life of society and each individual, as well as legal relations arising in connection with the creation, use and dissemination of information. Kharchenko, Lipkan, Loginov define the concept of "cybersecurity" as an integral component of the national security of every state, including the

process of managing potential threats, risks and dangers, as a result of which Ukraine's information sovereignty is ensured (Lisovska, 2019).

According to Article 1 of the Law of Ukraine "On the Basic Principles of Ensuring Cybersecurity of Ukraine" (Law of Ukraine No 2163-VIII. . . , 2017), cybersecurity is primarily a state of protection of the interests of a person and a citizen, society and the state as a whole when using the benefits of information space and cyberspace. This ensures the stable development of the information society and digital technologies, as well as timely prevention, response and detection, and subsequent neutralisation of potential cyber threats to the national security of Ukraine and its population (Law of Ukraine, № 2163-VIII.., 2022).

Thus, the following characteristic features of cybersecurity can be identified:

- Protection against external cyber threats – according to the PurpleSec 2021 report, 27% of all incidents and cyberattacks come from external sources. That's why security software should include tools to track threats from external sources (Seven Essential Features of Cyber Security One Should Know, 2023);
- Protecting against insider cyber threats – According to the 2020 Cybersecurity Insiders Threat Report, 68% of various organisations are threatened from within. In general, these are errors caused by employees or incorrect configuration (Seven Essential Features of Cyber Security One Should Know, 2023);
- Compliance with the established requirements for cybersecurity – means adherence to legal regulations, internal business guidelines and specifications;
- Availability of cloud-based security services that have the capabilities and appropriate tools to detect and eliminate potential threats. These services contain threat scanning endpoints for further security assurance and are the basis for improving scanning of complex targets;
- Preventing, detecting and responding to threats quickly.

In general, such variability in the interpretation of the concept of "cybersecurity" is explained by the rapid increase in the range of information space capabilities, its impact on social relations and, as a result, the emergence of new potential threats in cyberspace. This is what contributes to the constant updating of the knowledge base about this phenomenon, its more detailed study and adaptation of existing knowledge to current realities. One of these areas is the study of legal challenges and prospects for ensuring cybersecurity

in the system of public administration of educational institutions in Ukraine. That is why the purpose of this research is to provide a detailed analysis of the basics of cybersecurity, to define the essence of cybersecurity and its characteristics in the system of public administration of educational institutions, to determine the prospects for such provision, and to take into account all possible legal challenges facing such provision.

During the research, the current state of cybersecurity in the system of public administration of educational institutions is examined. Thus, due to the lack of funding, the complexity of the educational environment as a specific infrastructure is vulnerable to cybercriminals. In the course of the study, the regulatory framework is also investigated, which led to the conclusion that it is advisable to improve regulations of cyber defence of the educational space and their nomenclature features.

As a result, the legal problems faced by the cyber security of the educational sphere are outlined and the solutions are developed. Accordingly, the specific improvements for politicians and managers of educational institutions of Ukraine are suggested in order to enhance cybersecurity. These recommendations relate to legal changes, security policies, technical measures and training programs.

2 Methodological Framework

In the course of the scientific research, a number of general and special methods of scientific knowledge were used. These include the following methods, such as the method of systematic analysis, synthesis, dialectical method, normative method and method of studying legal documents, etc.

The leading method of research is the method of system analysis, with the help of which various sources of information regarding the features of cyber security in general and in the state education management system in particular have been developed and studied. At the same time, the characteristic features of cyber security that shape the vision of this phenomenon and contribute to its improvement were determined. As a result of the system analysis, certain provisions and conclusions were formed regarding the potential prospects of ensuring cyber security and protection of personal data in the educational sphere, as well as a list of legal challenges that arise in the course of security measures in the information space was determined. In particular, the measures that should be taken for a quick and effective response to cyber-attacks, and what tools should be used to neutralize potential threats, were analysed.

The synthesis method was also used to form a unified vision of cyber security. On the basis of data on cyberattacks on educational institutions of foreign countries, conclusions were drawn regarding problematic points and the main points of further improvement of the legislation.

The research was also conducted using the dialectical method of scientific knowledge. With its help, the problematic issues of ensuring the cyber security of educational institutions were identified and investigated, and manifestations of the negative impact of the information space on human rights, privacy and confidentiality during active cyberattacks were revealed. The content of the challenges faced by society, the state, and an individual in connection with the provision of cyber protection, and the ways to solve them, were revealed using the dialectical method.

The normative method became key in the analysis and definition of the concept of "cyber security" and its characteristics. The method of studying regulatory and legal documents contributed to the generalization of information about the features of cyber security during the educational process. The legal method allowed to assert the inconsistency of the current legislation with the development of digital technologies, the lack of clearly established norms and standards of cybersecurity, the improper level of confidentiality and protection of personal data, establishing responsibility for cybercrime, the need for specialized units and specialists in ensuring cybersecurity at the level of public administration. Having analysed regulations of cyber security, the main legal problems and challenges arising of cybersecurity in the educational sphere are determined. The method of statistical analysis made it possible to analyse the quantitative indicator of external and internal threats in cyber space in education over the past 3 years.

Directly, concepts, components of ensuring cyber security, its peculiarities and problematic aspects of its provision in the assessment process are considered in the scientific works of domestic and foreign researchers, namely: Kormych, Lisovska, Kalyuzhny, Bykov, Burov, Dementievska, Peterson, Kharchenko, Lipkan, Loginov, etc.

On the basis of the obtained results, conclusions are formulated on the state of cybersecurity in the system of public administration of education. Consequently, specific recommendations are suggested to solve legal problems and improve the situation. The methodology facilitates analysing legal challenges and prospects of cybersecurity in the system of public administration of educational institutions of Ukraine and to develop recommendations for further actions.

3 Results and Discussions

3.1 Current State of Cybersecurity in the System of Public Administration of Educational Institutions

Today, digital technologies have become an integral part of educational processes. They are manifested in the creation and use of various online learning applications, cloud storage, the use of student assessment systems and other educational technologies (Volik et al., 2019). These are not just tools for learning, but in the context of the coronavirus pandemic and military operations, they have become the basis for ensuring stable learning and teaching processes.

According to the United Nations, the pandemic has forced 190 countries to look for alternatives to conventional education, as the usual learning process has been disrupted (United Nations, 2020). Along with the new realities came new problems, as digital technologies and processes are a tasty piece for those who want to make money. That is why the issue of serious protection and security of both the educational process, materials, and personal data of students and teachers has arisen. Along with these problems, there are related ones, such as unequal access to digital technologies, constant interruptions, lack of proper training among teachers and students, etc. (Wei and Hindman, 2011).

In Ukraine, these problems are quite relevant, although they are gradually being addressed. However, artificial intelligence has also contributed to cyber defence and cyber threats, bringing digital technologies to a much higher level (Bongiovanni, 2019). Undoubtedly, every sphere of society deals with the information space and the latest technologies, but the education sector in Ukraine remains in a rather dangerous situation. Especially given the constant cyberattacks by the Russian Federation. That is why the issue of cybersecurity in the education sector is quite important for all its parties: teachers, students and even their parents.

Globally, the issue of cybersecurity in the public administration of educational institutions is also an important one. In May 2023, according to Malwarebytes, 30 attacks on the education sector worldwide occurred, which is the highest number since early 2022. This trend that has also become increasingly evident over the past twelve months. Between June 2022 and May 2023, Malwarebytes identified a total of 190 ransomware attacks on educational institutions. Between the first and second half of this period, the number of attacks increased by 84 % (Figure 1).

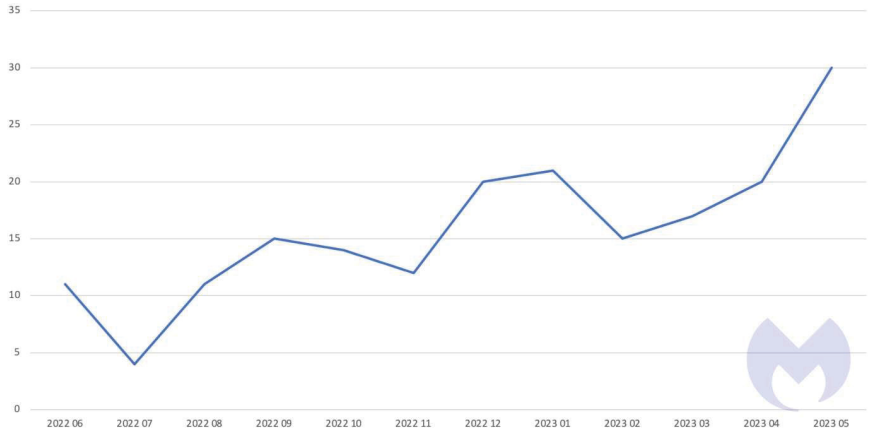


Figure 1 Ransomware attacks on education in June 2022 – May 2023.

Source: Malwarebytes.

Over the past few years, there have been a number of serious attacks on world-renowned universities, which have had a number of negative consequences, such as leaks of personal data of employees, teachers, students and former students of these universities. For example, in 2018, a large-scale hacker attack on Yale University was detected, which resulted in the leakage of personal information of almost 120,000 students, including social security numbers and residential addresses (Fuchs, 2018). In 2020, cyberattacks were also recorded at the University of Northumbria in the UK, which were aimed at disrupting the usual educational process and subsequently cancelling exams (BBC News, 2020).

Ransomware cyberattacks are quite serious, as was the case at the University of California in the United States in 2020. At that time, the university was subjected to a hacker attack, when access to data was blocked, and a ransom of $1.14 million was required to restore it and prevent its further dissemination (Tidy, 2020).

In addition, many countries around the world are currently engaged in active litigation after similar hacker attacks, and therefore the issue of cybersecurity for educational institutions is relevant not only for Ukraine. At the same time, Ukraine is taking into account the experience of foreign countries and adapting its cybersecurity legislation to the realities of today and existing cases.

We cannot say that the issue of cyber defence of educational institutions is a top priority in Ukraine compared to the banking and defence sectors,

healthcare and industry, as these areas shape the country's economy and national security. But we cannot deny the fact that the education sector is being neglected either. Especially now – when specialists and new employees will be building the post-war state and rebuilding the economy.

It should be noted that, according to the latest available data, in Ukraine, more than 50 universities train cybersecurity specialists. In general, following the example of the world's leading countries, they gain knowledge of the basics of programming, database and information security systems development, cyberattack counteraction and security policy, public key certificate maintenance, security system monitoring, etc. (Burlaka et al., 2019). It is also important to note that the last 5 years have been significant, as the perception of cybersecurity has changed, as have the approaches to ensuring it. Analysts note that most incidents in the online space are related to the human factor, hacking of gadgets and cloud storage. This problem is especially acute with the increasingly digital humanistic nature of education, the growing role of social media in human life in general and education in particular, and humanity's understanding of the need to move to lifelong learning (Burov, 2016).

Moreover, in recent years, especially in the period before the full-scale invasion, a number of international documents have been developed that have become guidelines for educational institutions in terms of cybersecurity. First of all, these include the Digital Competence Framework for Citizens 2.0-2.1. The Law of Ukraine "On Education" (Law of Ukraine, No. 2145-VIII…, 2017) defines information and communication as one of the main competences, while cybersecurity is a key component of this competence and reflects the general approaches formulated in the Digital Competence Framework for Citizens 2.0-2.1 (Law of Ukraine, No. 2145-VIII…, 2017).

Today, higher education is a very vulnerable sector in the field of cybersecurity, as educational institutions have a very complex digital footprint given the amount and variety of data they hold, the diversity of their online activities, and their aggregate computing power (Singar and Akhilesh, 2020). It is also worth noting that universities constantly consume and produce a large amount of information, which is contained in the relevant registers and databases containing faculty files and other personal information stored for various accesses for training, etc. It should also be noted that in the course of education, databases on students and their performance indicators are formed, which become the basis for analytical work and further improvement of the educational process. The latter is of considerable concern, as it raises the issue of student privacy (Peterson, 2016). Security is another important

issue, as huge volumes of diverse data are difficult to protect, which increases the vulnerability of universities and the education sector in general to cyber threats (Fouad, 2021).

Currently, the education system, the public sector and energy suppliers must strengthen their defences, especially multifactor authentication and threat detection solutions. The existing problems may be due to the low IT budget. Moreover, educational institutions are often tempted to offer their students access to a variety of services from home, which results in configuration errors occur that can be exploited by cybercriminals.

3.2 Legal Challenges in Ensuring Cybersecurity in the System of Public Administration of Education

When analysing the legal challenges in cybersecurity in the system of public administration of education, it is obvious that there is some complexity due to the diversity of the processes of the information space itself. It is these points that should be taken into account when improving the legislative regulation of cybersecurity in educational institutions. The main legal challenges include:

1. The mismatch between current legislation and the state of development of digital technologies – the legislator must take into account the fact that digital technologies are developing almost every day, and outdated wording of the law does not allow educational institutions in Ukraine to adapt to new realities in cyberspace, and therefore become an easy target for attackers. The fact that it is impossible to respond quickly to significant changes causes vulnerability in the education management system itself (Dementievska, 2015).
2. Lack of clearly established norms and standards for cybersecurity – there is a general trend in Ukrainian legislation towards vague standards. In general, this leads to conflicts in legislation, disagreements and ambiguity in the interpretation of a single rule, and, as a result, a lack of understanding of one's basic rights and obligations. However, it should be noted that recent years have been significant for Ukrainian education in terms of cybersecurity, as the standards of European countries have begun to move into our space. On 6 August 2021, the President of Ukraine approved the decision of the National Security and Defence Council of Ukraine of 14 May 2021 "On the Cybersecurity Strategy of Ukraine", which defines the basic priorities of national interests in the field of cybersecurity, including in the educational sphere, existing and potential risks and threats, the purpose, tasks and goals of ensuring cybersecurity of Ukraine in order to create conditions for the safe

functioning of cyberspace, its use in the interests of the individual, society and the state.

3. Inadequate level of confidentiality and the right to privacy and personal data protection, which can lead to leakage of personal data (which is logical) and their improper processing during the implementation of actions necessary for the person (for example, registration for an exam, etc.). That is why government agencies and educational institutions should use all necessary tools and means to protect participants in the educational process from personal data leakage and privacy violations (Kahn, 2019).
4. Establishment of liability for cybercrime – currently, the Criminal Code of Ukraine establishes liability for a number of crimes committed in cyberspace. However, cybercrimes committed within the framework of public education administration will be much more difficult to investigate, given the even greater variety of hacker attacks, the so-called originality of the attackers themselves and, accordingly, the understanding of the circumstances of the case.
5. Ensuring cybersecurity at the level of public administration requires knowledgeable specialised units and specialists. This, in turn, requires significant financial investments and capital to ensure that responses to potential cyber threats are truly effective and bring results.

   The public administration system should develop a cybersecurity strategy that will identify common goals, priorities, risks and measures to ensure the security of information resources. This strategy should be known to all participants in the educational process and constantly updated in accordance with changes in cyber threats. Accordingly, it is necessary to develop a specific cybersecurity policy that will determine the rules, procedures and requirements for protecting information resources. This policy should include aspects such as access control, data protection, threat monitoring and detection, and incident response planning. It is important to regularly audit cybersecurity systems and check their compliance with standards and requirements. The cybersecurity policy may involve working with other government agencies, cybersecurity companies, and experts to share information, experience, and coordinate cyber defence activities in the education system.
6. Low awareness of specialists – there is no doubt that the number of professional specialists in this field has increased over the past few years, making our cyberspace more secure. However, the required level of protection has not yet been achieved. This is exactly what education should be aimed at in order to "protect yourself" (Kahn, 2019).

7. The political component – ensuring cybersecurity can be complicated by political turmoil and the vested interests of government agencies. A threat in this aspect is the process of coordination of innovations between different structures and bodies.
8. The problem of protecting intellectual property, namely copyrights to scientific research by faculty and students, innovations and the latest developments made in the course of education (Korolchuk et al., 2023).
   Based on the analysis of the above legal challenges, the government is able and obliged to implement relevant and appropriate standards and practices, while not neglecting the experience of foreign countries. This experience means establishing, at a minimum, basic standards and cybersecurity measures that are mandatory for educational institutions to follow. This should be done in a manner similar to sectoral regulation, as in the medical, banking, and other sectors. Based on these measures, practices to ensure cybersecurity functions will be introduced in the future.
9. Due to the fact that cybercrime is international in nature, it is important to cooperate with international partners to ensure cybersecurity, exchange information and experience in this area.
   Many educational institutions in Europe use two-factor or multi-factor authentication systems to access information systems (this is very popular in Swedish universities). This system helps avoid unauthorized access to data and provide an additional level of protection. In accordance with the General Data Protection Regulation (2018), educational institutions are obliged to ensure a high level of protection of the personal data of their students and staff. Many Dutch universities implement modern security technologies such as data encryption and intelligent threat monitoring systems. Universities in Germany have a strict cybersecurity policy, which includes regular security checks, audits and software updates. Universities in the UK are often involved in national cyber security and research programmes, contributing to the development of innovative protection methods. It is important to note that national norms and standards should be consistent with international standards, complement them, adapt to Ukrainian realities and develop within this spectrum.
10. At the same time, the government can allocate funds for the implementation of free instructions and tools for educational institutions to respond to the most common attacks and threats.

It is also important to note that the full range of tools for securing cyberspace is not built only with legal gaps in mind. Technical, informational and psychological aspects are also taken into account. Only in cooperation can the desired result be achieved.

3.3 Prospects for Cybersecurity in the System of State Education Governance

The cyber security of the educational space faces various legal problems that complicate the protection of information resources and personal data. Many countries have a limited or outdated legal framework that does not take into account modern technologies and cybersecurity challenges. The lack of specialized laws or regulations in the field of cybersecurity can complicate the protection of educational institutions from cyber threats. Therefore, the issue of determining responsibility for cyberattacks in the educational space can be difficult. It is not always obvious who is responsible for violating data security or for a cyberattack. This can create problems in resolving legal issues and compensating for damages.

A special category is children and young people who use information technology in their studies. Thus, the legislation should implement special measures to protect children from online threats, including protecting their personal information and restricting access to harmful content. The development and implementation of effective legal mechanisms to regulate these issues is important for ensuring security in the educational space. Countries should constantly adapt their legislation to growing cyber threats and cooperate internationally to exchange best practices and coordinate cybersecurity measures.

Within the framework of the research, it is important to note that the prospects for ensuring cybersecurity in the education management system are determined taking into account the current state of development of digital technologies, recent trends and available indicators of potential cyberattacks and cyber threats. Summarizing the above, we can say that the effective ways of solving the legal challenges of cybersecurity in public administration of education are the following ones:

- Improving the existing regulatory framework for cybersecurity in educational institutions. This is manifested in the improvement of laws, bylaws, regulations, guidelines and standards, while being consistent

with the already adopted Cybersecurity Strategy of Ukraine and real potential threats.

- The adoption of special laws or regulations that will determine the rights and obligations of education managers on cybersecurity issues, as well as mechanisms for responding to cyberattacks and protecting personal data.
- The development of national cyber defence standards for educational institutions to ensure uniform, standardised cyber security practices.
- Active implementation of innovative digital technologies, which includes artificial intelligence and its derivative applications and tools to facilitate educational processes (Dementievska, 2015).
- Development of an individual cybersecurity mechanism for each type of educational institution, taking into account the specifics of that particular educational institution, its students or pupils and available resources
- Strengthening cooperation with private entrepreneurs and firms – this generally includes IT companies that already employ specialists who understand the practical details of cyber defence and can provide their opinions on the technical capacity of educational institutions to deal with real cyberattacks.
- The development of educational programs and conducting information campaigns on cybersecurity to raise the awareness of participants in the educational process regarding cyber security.
- Updating and improving systems for responding to potential threats – this point correlates with the previous one, as the recommendations of experienced professionals will lead to active improvement of systems for responding to and detecting potential threats, minimise the damage caused and prevent the possible spread of cyberattacks in the future.
- Increasing funding at the state level, as well as attracting potential investors, is a very important future step, as reliable cyber defence mechanisms require significant investments and constant software updates to reflect the latest improvements and changes in the digital world. In addition, the creativity of attackers also encourages the optimisation of tools to respond quickly to potential threats (Wei and Hindman, 2011). Thus, financing cybersecurity in the educational sphere and legal ways of financing it (state subsidies, grant support, voluntary donation from all comers and/or sponsors) should be enshrined in the legislation.
- Developing and upgrading the qualifications of specialists in this area, as the availability of a certain range of skills and knowledge, together with

the latest technologies, increases the chances of identifying potential threats.

- Cooperating with international partners and developing a uniformity in approaches and exchanging experience in cyber security.

These prospects can become a driving force on the way to ensuring cybersecurity in the system of public administration of education and, as a result, will have a positive impact on both the internal situation of educational institutions and the state of security of the state's cyberspace in general.

4 Conclusion

Based on the above, we can confidently conclude that ensuring cybersecurity in educational institutions is an important area on the path to European integration. As Ukraine has committed to a number of reforms and improvements to its legislation in line with EU standards, this directly relates to ensuring privacy and protection of personal data in the information space, both in the banking and defence sectors, as well as in the healthcare and education sectors.

It was noted that the main characteristics of cybersecurity are protection against external cyber threats, protection against internal cyber threats, compliance with the established requirements for cybersecurity means compliance with legal norms, internal business instructions and specifications, availability of cloud security services that have the capabilities and appropriate tools to identify and eliminate potential threats and prevent, quickly detect and respond to threats.

The main legal challenges include the mismatch between the current legislation and the state of development of digital technologies; lack of clearly established norms and standards for cybersecurity; inadequate level of confidentiality and the right to privacy and personal data protection, which may lead to leakage of personal data (which is logical) and their improper processing during the implementation of actions necessary for the person (for example, registration for an exam, etc.); establishing liability for cybercrime; the need for knowledgeable specialised units and specialists in the course of ensuring cybersecurity at the level of state governance; low awareness of specialists; political component; the problem of protecting intellectual property, namely copyrights to scientific research of the teaching staff and students, innovations and the latest developments that were carried out during training.

Regarding the prospects for cybersecurity in the field of public administration of education, it is worth noting the following: improving the existing regulatory framework for ensuring cybersecurity in educational institutions; active implementation of innovative digital technologies; development of an individual cybersecurity mechanism for each type of educational institution, taking into account the specifics of that particular educational institution, its students or pupils and available resources; strengthening cooperation with private entrepreneurs and firms; updating and improving response systems.

A set of legal, technical, informational and psychological tools can ensure full cyber protection of the education sector and facilitate active response to potential risks and threats. A detailed analysis of this issue allowed us to achieve our goal and draw important conclusions for further research. These conclusions can serve as a theoretical basis for the work of other researchers and provide suggestions for improving legislation, standards and guidelines for the educational sector in terms of cyber defence.

Further research on legal challenges and prospects for cybersecurity in public administration of education lies in comparing legal approaches and practices on cybersecurity in the educational sphere of other countries. Moreover, it is promising to study specific cyber incidents that occurred in educational institutions in order to identify the causes and consequences. In addition, the development of educational materials on cybersecurity for staff and students of educational institutions can help in expanding knowledge about cyber threats in education.

References

BBC News. (2020). *Northumbria University Hit by Cyber Attack*. Retrieved from https://www.bbc.co.uk/news/uk-england-tyne-53989404.

Bongiovanni, I. (2019). The least secure places in the universe? A systematic literature review on information security management in higher education. *Computer Security*, *86*, 350–357.

Burlaka, V, Hong, J.S., and Shvets, D. (2019). The Role of Adverse Childhood Experiences and Corporal Punishment in Early Adulthood Depression and Substance Use among Ukrainian College Students. *Journal of Family Violence, 35*(3), 285–295. DOI: https://doi.org/10.1007/s10896-019-00110-x.

Burov, Î. Ju. (2016). Educational Networking: Human View to Cyber Defense. *Information Technologies and Learning Tools*, *52*, 144–156.

Bykov, V.Y., Burov, O.Y., and Dementievska, N.P. (2019). Cybersecurity in the digital learning environment. *Information Technologies and Learning Tools*, *70*(2), 15–22.

Dementievska, N. P. (2015). Formation of skills of critical evaluation of web resources and the problem of students' safety on the Internet. *Computer in School and Family, 7*, 46–51.

Fouad, N.Sh. (2021). Securing higher education against cyberthreats: from an institutional risk to a national policy challenge. *Journal of Cyber Policy, 6*(2), 137–154. DOI: 10.1080/23738871.2021.1973526.

Fuchs, H. (2018). Yale Faces Lawsuit for Data Breach. *Yale Daily News*. Retrieved from https://yaledailynews.com/blog/2018/08/31/yale-faces-lawsuit-for-data-breach/.

General Data Protection Regulation. (2018). Retrieved from https://gdpr-info.eu/.

Kahn, A. (2019). The 2019 Cybersecurity Threat Landscape. Retrieved from https://www.rmahq.org/the-2019-cybersecurity-threat-landscape/.

Kalyuzhnyi, R.A. (2002). *Information support of management activities in the conditions of informatisation: organisational and legal issues of theory and practice*. Kyiv: Academy of the State Tax Service of Ukraine.

Kormych, B.A. (2003). Organisational and legal principles of cybersecurity policy of Ukraine. Odesa: Legal Literature.

Korolchuk, O., Vasiuk, N., Klymkova, I., Shvets, D., and Piddubnyi, O. (2023). COVID-19 Vaccination under Conditions of War in Ukraine. Asian Bioethics Review. DOI: 10.1007/s41649-023-00248.

Law of Ukraine No 2163-VIII "On the Basic Principles of Cybersecurity in Ukraine". (2017). Retrieved from https://zakon.rada.gov.ua/laws/show/2163-19?lang=en#Text.

Law of Ukraine No. 2145-VIII "On Education". (2017). Retrieved from https://zakon.rada.gov.ua/laws/show/en/2145-19#Text.

Lisovska, Y.P. (2019). *Cybersecurity: risks and measures*. Kyiv: Condor Publishing House.

Malwarebytes. (2024). Retrieved from https://www.malwarebytes.com/blog/threat-intelligence/2023/06/the-2023-state-of-ransomware-in-education-84-increase-in-known-attacks-over-6-month-period.

Mozhaiv, O., Kuchuk, H., and Shvets, D. (2019). Minimization of power losses by tractiontran-sportation vehicles at motion over a bearing surface that undergoes deformation. *Eastern-European Journal of Enterprise Technologies, 1*(1–97), 69–74. DOI: https://doi.org/10.15587/1729-4061.2019.156721.

Peterson, D. (2016). Edtech and Student Privacy: California Law as a Model. *Berkeley Technology Law Journal, 31*(2), 961–996.

Seven Essential Features of Cyber Security One Should Know. (2023). Retrieved from https://www.jaroeducation.com/blog/7-essential-features-of-cyber-security-one-should-know/.

Singar, A.V., and Akhilesh, K. B. (2020). Role of Cyber-Security in Higher Education. *Smart Technologies: Scope and Applications*, 249–264.

Tidy, J. (2020). How Hackers Extorted $1.14 m from University of California, San Francisco. *BBC News*. Retrieved from https://www.bbc.co.uk/news/technology-53214783.

Ukrinform. (2022a). Sites of Banks and Authorities have undergone a mass DDOS-attack. Retrieved from https://www.ukrinform.ua/rubric-technology/3410542-sajti-bankiv-ta-organiv-vladi-zaznali-masovoi-ddosataki.html.

Ukrinform. (2022b). Hackers are attacking the site of the Kyiv Regional State Administration. Retrieved from https://www.ukrinform.ua/rubric-technology/3411812-sajt-kiivskoi-oda-atakuut-hakeri.html.

Ukrinform. (2022c). Email addresses of the Ukrainian military are being attacked by hackers. Retrieved from https://www.ukrinform.ua/rubric-technology/3412829-emailadresi-ukrainskih-vijskovih-atakuut-hakeri.html.

Ukrinform. (2023). Hackers attack electronic database on education issues. Retrieved from https://www.ukrinform.ua/rubric-technology/3741316-hakeri-atakuvali-elektronnu-bazu-z-pitan-osviti.html.

United Nations. (2020). Policy Brief: Education During Covid-19 and Beyond. Retrieved from https://www.un.org/development/desa/dspd/wp-content/uploads/sites/22/2020/08/sg_policy_brief_covid-19_and_education_august_2020.pdf.

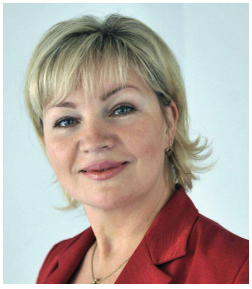
Volik, V., Lozhmets, Y. and Shvets, D. (2019). Electronic governance in Ukraine and Estonia current situation and prospective. *Journal of Legal, Ethical and Regulatory, 22*(Special Issue 2), 5–7.

Wei, L., and Hindman, D.B. (2011). Does the Digital Divide Matter More? Comparing the Effects of New Media and Old Media Use on the Education-Based Knowledge Gap. *Mass Communication and Society*, *14*(2), 216–235.

Biographies

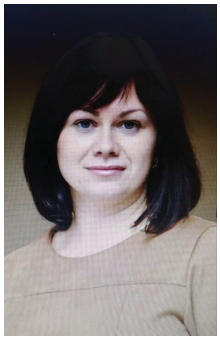
Herasym Dei – PhD student in Public Administration.

Dmytro Shvets – Scientific interests: Preparation of future officers of the Ministry of Internal Affairs of Ukraine for the protection and maintenance of public order in the process of professional training.

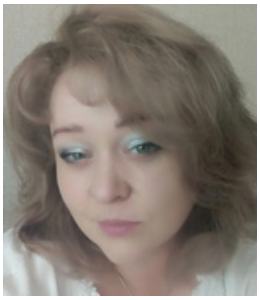


Nataliia Lytvyn – Scientific interests: administrative activity of state executive authorities and local self-government bodies; protection of the rights and

interests of individuals and legal entities in the field of public legal relations; information legal relations and information security; ensuring the realization of the rights and legitimate interests of medical workers, patients, and other persons and increasing the level of legality and law and order in the medical field.



Olena Sytnichenko – Scientific interests: research on legal support of information security; information law; administrative law and process.



Olena Kobus – Scientific interests: cybersecurity.