DOI: https://doi.org/10.32353/acfs.10.2024.02
UDC 343.98 (477)

Serhii Lukashevych
PhD in Law, Associate Professor, Professor at the Law Department of National Aerospace University "Kharkiv Aviation Institute" NAU "KhAI", Kharkiv, Ukraine
ORCID: https://orcid.org/0000-0001-8386-6237
e-mail: s.lukashevych@khai.edu

Karina Palkova
PhD in Law, Associate Professor, Decan Faculty of Social Sciences
Riga Stradina University, Latvia
ORCID: https://orcid.org/0000-0002-6909-571X
e-mail:karina.palkova@rsu.lv

Cybersecurity of the Information Space of a Higher Education Institution

The article examines the impact of cybercrime on the work of higher education institutions and the ways to prevent and overcome cyberattacks. It is substantiated that the use of computer technology, along with its benefits, poses certain threats in terms of the complexity of data protection. It is found that today the global trends in countering cyber threats are inferior to the attackers, which leads to aggressive and successful cyber attacks by the latter. It is proved that attacks on learning networks have recently intensified significantly. Organisational measures to address cybersecurity issues are proposed. Based on the material studied, it is concluded that the effectiveness of countering cyber attacks and, as a result, the successful and stable functioning of higher education institutions in Ukraine depends on the level of preparedness, competence and responsibility of the participants.

Keywords: crime prevention, information security, cybersecurity, cybercrime, preventing cybercrime, higher education institutions, information space of a higher education institution.

Introduction. It should be recalled that the ongoing deepening of the socio-political, financial and economic crisis, the war caused by the aggression of the russian federation spontaneous migration of the population, extremely high unemployment and growing social insecurity have led to social tension and increased the criminogenic potential of society. Given these circumstances, improving existing and developing new crime prevention strategies and measures are in the focus of attention of representatives of all branches of government and academics[1]. In the face of growing threats in cyberspace and the spread of cybercrime, higher education institutions must pay increased attention to the cybersecurity of their information resources. Cybercriminals use social engineering techniques to collect data on the preferences, behaviour and habits of students and staff, which allows them to more easily penetrate internal university systems, manipulate users or fraudulently gain access to important data.

To counter these threats, universities have an increased responsibility to protect academic information, research and personal data of students and staff. This means regularly reviewing security policies and computer network architecture, as well as restricting open access that could create vul-

Funding

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Disclaimer

The funder had no role in the study design, data collection and analysis, decision to publish, or preparation of the manuscript.

Contributors

The authors contributed solely to the intellectual discussion underlying this paper, case-law exploration, writing and editing, and accept responsibility for the content and interpretation.

Declaration of Competing Interest

The authors declare that they have no conflict of interest.

[1] Лукашевич С., Філіпенко Н. Information Technologies in Law Enforcement, Security and Expert Activities. *Наука і техніка сьогодні*. 2023. №. 13 (27). URL: http://perspectives.pp.ua/index.php/nts/article/view/7560

nerabilities for external attacks. According to the researchers[2], an important aspect of security is also the training of students and university staff in the principles of cyber hygiene, which will help minimise fraud and data theft. In addition, universities should develop effective cybersecurity strategies, including two-factor authentication, data encryption, and systems for monitoring and responding to suspicious activity. This approach allows not only to strengthen cyber defences but also to adapt to new challenges in the field of cybersecurity, which is becoming critical in the modern world.

Literature Review. The factors influencing the cybersecurity of higher education institutions in Ukraine and the world have been the subject of research by domestic scholars. These are, for example, I. Bilous, I. Galona, O. Zakharova, M. Kyrychenko, O. Kohanovska, O. Lytvynov, S. Lukashevych, N. Muranova, O. Sikora, N. Filipenko, Z. Shatska, I. Shemelynets, and others.

Foreign researchers did not stay away from these problems. Among them are M. Carr, E. Kost, K. Palkova, A. Piazza, V. Rakstiņš, A. Sprūds, L. Juļa, N. Schwartz, A. Vasudevan and many others.

However, research into the problems of cybersecurity of the educational process requires significant further theoretical developments and their practical implementation. In the context of instability caused by military operations, the security of information systems and networks in higher education institutions is becoming a particularly pressing issue. The technical means of protection against cyberattacks that can threaten both student and faculty data, as well as research and administrative systems, need to be constantly improved and adapted to new challenges. Therefore, it is particularly important to ensure reliable protection of information from external threats, as the enemy may use cyberattacks as a tool to destabilise the education and science system.

In addition, it is necessary to develop mechanisms for adapting the educational process to changing conditions, in particular, given the transition to distance learning or the use of online resources, which also creates new challenges for cybersecurity. In a time of war, it is of great importance to train students and teachers in the safe use of information technology, as well as to create systems that ensure reliable monitoring and control of information flows.

Results and Discussion. With the growing threats in cyberspace, cybercriminals are using increasingly sophisticated social engineering techniques to gain access to personal data of university staff and students, including information about their online behaviour and interests. This is forcing universities to assume increased responsibility for the protection of academic digital data. To do this, they are forced to constantly strengthen their cybersecurity, ensure regular monitoring of computer networks and control access to information resources.

At the same time, there are problems that accompany the introduction and use of information and communication technologies (hereinafter — ICT) in higher education institutions (hereinafter — HEIs), in particular: insufficient funding for the purchase of modern equipment and the introduction of ICT; lack of strategic vision on the part of the HEI management regarding the integration of ICT; low level of awareness among teachers and students about the possibilities and use of ICT in the educational process; lack of qualified specialists capable of ensuring the effective operation and cybersecurity of ICT in the institution

In line with the first three points, many HEIs have made efforts to address these issues. However, the fourth problem — the lack of cybersecurity specialists — is the most critical and relevant not only for individual institutions but also at the national level.

[2] Білявська Ю., Шестак Я. Кібербезпека та кібергігієна: нова ера цифрових технологій. *Товари і ринки*. 2022. № 3. С. 47–59.

С. Лукашевич,
К. Палкова

КІБЕРБЕЗПЕКА ІНФОРМАЦІЙНОГО ПРОСТОРУ ВИЩОГО НАВЧАЛЬНОГО ЗАКЛАДУ

У статті розглянуто вплив кіберзлочинності на роботу закладів вищої освіти та шляхи запобігання і подолання кібератак. Обґрунтовано, що використання комп'ютерних технологій, поряд з їх перевагами, несе певні загрози з точки зору складності захисту даних. З'ясовано, що сьогодні світові тенденції протидії кіберзагрозам поступаються зловмисникам, що призводить до агресивних та успішних кібератак з боку останніх. Доведено, що останнім часом значно активізувалися атаки на навчальні мережі. Запропоновано організаційні заходи для вирішення проблем кібербезпеки. На основі вивченого матеріалу зроблено висновок, що ефективність протидії кібератакам і, як наслідок, успішне та стабільне функціонування закладів вищої освіти в Україні залежить від рівня підготовленості, компетентності та відповідальності учасників.

Ключові слова: запобігання злочинності, інформаційна безпека, кібербезпека, кіберзлочинність, запобігання кіберзлочинам, заклади вищої освіти, інформаційний простір закладу вищої освіти.

S. Lukashevych,
K. Palkova

CYBERSICHERHEIT DES INFORMATIONSRAUMS EINER HOCHSCHULEINRICHTUNG

Der Artikel untersucht die Auswirkungen der Cyberkriminalität auf die Arbeit von Hochschuleinrichtungen und die Möglichkeiten zur Verhinderung und Bewältigung von Cyberangriffen. Es wird nachgewiesen, dass der Einsatz von Computertechnologie neben ihren Vorteilen auch gewisse Gefahren in Bezug auf die Komplexität des Datenschutzes mit sich bringt. Es wird festgestellt, dass die heutigen globalen Trends bei der Bekämpfung von Cyber-Bedrohungen den Angreifern unterlegen sind, was zu aggressiven und erfolgreichen Cyber-Angriffen durch letztere führt. Es ist erwiesen, dass die Angriffe auf Lernnetzwerke in letzter Zeit erheblich zugenommen haben. Es werden organisatorische Maßnahmen zur Bewältigung von Cybersicherheitsproblemen vorgeschlagen. Auf der Grundlage des untersuchten Materials wird der Schluss gezogen, dass die Wirksamkeit der Abwehr von Cyberangriffen und damit das erfolgreiche und stabile Funktionieren von Hochschuleinrichtungen in der Ukraine vom Grad der Vorbereitung, Kompetenz und Verantwortung der Beteiligten abhängt.

Schlüsselwörter: Verbrechensverhütung, Informationssicherheit, Cybersicherheit, Cyber kriminalität, Verhinderung von Cyberkriminalität, Hochschu leinrichtungen, Informationsraum einer Hochschuleinrichtung.

Research shows[3], that DDoS attacks are one of the most common cyberattacks on educational resources of educational institutions. They create difficulties with access to resources and disrupt the learning process. This confirms that cyber threats are a real and priority problem for modern society, including for the educational and scientific activities of higher education institutions. Cybersecurity is becoming especially relevant for universities, which train highly qualified personnel on a daily basis and play a systemic role in strengthening the defence capability of our country.

The modern introduction of information and communication technologies has become widespread and is a global trend that penetrates all spheres of life, especially interactive learning. Informatisation leads to an increasing dependence on ICTs in research and education, where information technologies are becoming important both as tools and factors in the functioning and development of education[4].

It should be noted that most higher education institutions have moved from a traditionally conservative educational and research process to modern information (educational and research) activities. The transition to the new format was accompanied by the creation of their own information space, which included the following main steps:

Updating and modernising ICT equipment — introducing modern hardware and software to support educational and research processes.

Development of the official website of the higher education institution and its structural units — providing access to information about the institution, its activities, educational programmes and other important resources.

Connecting the higher education institution to the Internet and creating an internal network — the network provides information exchange and communication between employees, students and structural units of the university.

Implementation of electronic document management — transition from paper to digital form of documents for ease of storage, processing and transfer.

Implementation of a distance learning system — the ability to conduct online training, which is especially relevant for the current military realities of Ukraine, when almost half of students and teachers may be in different regions of Ukraine, even abroad.

Development of e-learning resources — creation of materials and manuals in digital format available to students for self-study.

[3] Див. докладніше: Татомир І. (2020) Кібербезпека університетів як спосіб протидії фішинговому шахрайству. *Економічний дискурс.* 2020. Випуск 1. С. 59-67. DOI: https://doi.org/10.36742/2410-0919-2020-1-7.; Vitālijs Rakstiņš, Karina Palkova, Lidija Juļa and Natalia Filipenko (2024) Improving cybersecurity measures in academic institutions to reduce the risk of foreign influence. Socrates. Rīga Stradiņš University Faculty of Law *Electronic Scientific Journal of Law.* Volume 2024 (2024): Issue 1-29 (September 2024). P. 75-79. URL: https://doi.org/10.25143/socr.29.2024.2.75-79; Савченко В., Маклюк О. (2024). Кібербезпека як фактор ефективності функціонування закладів вищої освіти. *Економіка та суспільство,* (60). URL: https://doi.org/10.32782/2524-0072/2024-60-24; Лісовська Ю. Кібербезпека: ризики та заходи : навч. посіб. Київ : Кондор, 2019. 272 с. та ін.

[4] Кібербезпека в інформаційному суспільстві: Інформаційно-аналітичний дайджест / відп. ред. О.Довгань; упоряд. О.Довгань, Л.Литвинова, С.Дорогих; Державна наукова установа «Інститут інформації, безпеки і права НАПрН України»; Національна бібліотека України ім. В.І.Вернадського. К., 2023. №7 (липень). 270 с.

Creation of an electronic library — providing students and faculty with access to e-books, scientific articles and other information resources.

Implementation of a system of electronic journals for publishing scientific results — providing a convenient tool for scientific activity and publication of scientific research.

Using a video conferencing system opens up the possibility of conducting lectures, seminars and meetings remotely, which is of particular importance for higher education institutions in times of war. Thanks to such technologies, educational processes can continue without physical presence in classrooms, which is a critical measure for the safety of both students and teachers, as it avoids the risk of injury in areas of possible danger. It also helps to maintain the stability of educational processes, minimising interruptions in learning and maintaining the quality of educational programmes even in difficult circumstances.

The introduction of a video surveillance system on the territory of a higher education institution is an important step to ensure control and improve security. Such a system allows you to quickly monitor the situation, record potentially dangerous events, control access to classrooms and prevent unauthorised entry. In addition, video surveillance helps to ensure law and order on the territory of the institution, reducing the risk of crime and improving emergency response. This is especially true in the current context of armed aggression, when the safety of students and staff of an educational institution requires additional attention[5].

Automation of financial and economic activities — the use of automated systems for financial management.

Automation of business activities is an increase in efficiency through the automation of administrative processes.

Automation of HR activities is a transition to an electronic system for keeping records of employees, including management of all aspects of HR processes. This solution provides a centralised record of personnel data, simplifies the procedure for recruiting and onboarding employees, monitoring their performance and maintaining electronic personal files. Automation also facilitates the prompt exchange of information between different departments of the institution and facilitates compliance with regulatory requirements for HR reporting. The use of an electronic HR system allows you to manage HR processes more efficiently, automate routine tasks, improve data accuracy and ensure the security of personal information. This approach not only reduces the amount of paperwork, but also significantly increases the efficiency of HR management, allowing managers to quickly obtain up-to-date data on employees.

Installation of an access control system — ensuring security on the territory of a higher education institution and restricting access to certain areas.

Informatisation in higher education institutions, on the one hand,

[5] Nataliia Filipenko, Hanna Spitsyna, Olena Agapova, Karina Palkova (2024) The Concept of Comprehensive Security for Higher Educational Institutions: Ukrainian and European Experience: Integrated Computer Technologies in Mechanical Engineering — 2023 Synergetic Engineering. Synergetic Engineering. Presents the proceedings of the ICTM´23 Conference held in Kharkov, Ukraine. URL https://doi.org/10.1007/978-3-031-60549-9_23.

S. Lukashevych,
K. Palkova

CYBERSÉCURITÉ DE L'ESPACE INFORMATIONNEL D'UN ÉTABLISSEMENT D'ENSEIGNEMENT SUPÉRIEUR

Résumé. L'article examine l'impact de la cybercriminalité sur le travail des établissements d'enseignement supérieur et les moyens de prévenir et de surmonter les cyberattaques. Il est prouvé que l'utilisation de la technologie informatique, malgré ses avantages, pose certaines menaces en termes de complexité de la protection des données. Il s'avère qu'aujourd'hui, les tendances mondiales en matière de lutte contre les cybermenaces sont inférieures aux attaquants, ce qui conduit à des cyberattaques agressives et réussies de la part de ces derniers. Il est prouvé que les attaques contre les réseaux d'apprentissage se sont récemment intensifiées de manière significative. Des mesures organisationnelles visant à résoudre les problèmes de cybersécurité sont proposées. Sur la base du matériel étudié, il est conclu que l'efficacité de la lutte contre les cyberattaques et, par conséquent, le fonctionnement stable et réussi des établissements d'enseignement supérieur en Ukraine dépendent du niveau de préparation, de compétence et de responsabilité des participants.

Mots clés : prévention du crime, sécurité de l'information, cybersécurité, cybercriminalité, prévention de la cybercriminalité, établissements d'enseignement supérieur, espace d'information d'un établissement d'enseignement supérieur.

S. Lukashevych,
K. Palkova

CYBERBEZPIECZEŃSTWO PRZESTRZENI INFORMACYJNEJ INSTYTUCJI SZKOLNICTWA WYŻSZEGO

Artykuł analizuje wpływ cyberprzestępczości na pracę instytucji szkolnictwa wyższego oraz sposoby zapobiegania i przezwyciężania cyberataków. Uzasadniono, że wykorzystanie technologii komputerowej, wraz z jej korzyściami, stwarza pewne zagrożenia pod względem złożoności ochrony danych. Stwierdzono, że obecnie globalne trendy w przeciwdziałaniu cyberzagrożeniom są gorsze od atakujących, co prowadzi do agresywnych i skutecznych cyberataków. Udowodniono, że ataki na sieci uczące się ostatnio znacznie się nasiliły. Zaproponowano środki organizacyjne mające na celu rozwiązanie kwestii cyberbezpieczeństwa. Na podstawie przeanalizowanego materiału stwierdzono, że skuteczność przeciwdziałania cyberatakom, a w rezultacie pomyślne i stabilne funkcjonowanie instytucji szkolnictwa wyższego w Ukrainie zależy od poziomu gotowości, kompetencji i odpowiedzialności uczestników.

Słowa kluczowe: zapobieganie przestępczości, bezpieczeństwo informacji, cyberbezpieczeństwo, cyberprzestępczość, zapobieganie cyberprzestępczości, instytucje szkolnictwa wyższego, przestrzeń informacyjna instytucji szkolnictwa wyższego.

improves the quality and efficiency of educational and research activities, but on the other hand, creates a multi-level information system that becomes critical for their reliable operation and cybersecurity.

For this reason, the term «information space of a higher education institution» refers to an integrated digital environment consisting of various information and communication technologies (ICTs) and enabling integrated interaction between teachers, students and administration. It serves as a platform for the joint exchange of knowledge, learning materials and communication, providing a variety of educational processes and resources.

Cybersecurity in this context means a set of measures aimed at protecting the information space from unauthorised access, malicious interference and data integrity violations. This implies achieving a high level of confidentiality of information, maintaining its integrity and accessibility for participants in the educational process, which is a guarantee of the stability of all components of educational activities and effective interaction in the academic community.

The criticality of the information space of a higher education institution is due to the fact that it accumulates a large amount of confidential information, in particular: personal data (information about students, staff and changes in staff); official data (directives, orders, instructions and other documents with restricted access); financial information (reports and resources); legal information (court cases, investigations); educational and scientific materials (intellectual property, patents, research, training programmes, electronic journals, training courses and resources), etc.

As a result, the information space of a higher education institution is a potential target for various types of cyber threats, and a successful attack can lead to the following consequences: technical damage (damage to equipment, blocking access to resources, destruction of intellectual property); material losses (financial costs of restoration, cybersecurity audit); reputational risks (loss of trust of partners and students, loss of credibility); moral losses (blackmail, psychological stress of employees and students, especially in the event of a data leak), etc.

Based on this, ensuring cybersecurity of a higher education institution becomes an important task that includes:

1. Analysing the factors that affect the cybersecurity of a higher education institution.

2. Development and implementation of a cybersecurity model for a higher education institution.

3. Evaluation of the effectiveness of this model of cyber defence of a higher education institution.

4. Preparing recommendations to improve the effectiveness of the cybersecurity model.

Given the purpose of the article, we will focus on the first task — analysing the factors that affect the cybersecurity of a higher education institution. The cybersecurity of an educational institution is closely integrated with the cyber defence system, which is a set of interdependent measures aimed at comprehensive protection of information resources from numerous threats. Such threats can be both external and internal, affecting information systems in different ways — from positive strengthening to negative reduction of their resilience.

A set of cyber defence measures includes technological, administrative and organisational methods that together form a resilient security system that can quickly adapt to new cyber threats. Internal factors, such as human factors, access management policies, and compliance with security standards, can significantly strengthen cyber defences, while weak internal infrastructure or lack of user awareness can weaken them. External factors, such as new types of cyber threats and updates to data protection legislation, also require constant monitoring and rapid response to reduce their negative impact on an educational institution.

Internal and external factors of influence.

Internal factors, which can be directly influenced by the institution, depend on the actions of the institution's management and employees. They can have a positive impact on the level of cybersecurity, but also have the potential to reduce its level due to erroneous or negligent actions.

External factors are not directly controlled by the higher education institution and are caused by external conditions, but their impact can be mitigated by improving internal security measures.

The impact of these factors necessitates constant monitoring of the state of cybersecurity of the institution. The state of cybersecurity depends on how effectively the cybersecurity model is developed and implemented, which should take into account the results of the analysis of the impact of both groups of factors.

The analysis of these factors helps to make informed management decisions aimed at ensuring effective interaction of the university with the external information space in both the short and long term. Continuous monitoring and forecasting allow the university management to develop effective strategies to respond to possible threats.

The main external factors affecting the cybersecurity of a higher education institution:

Emergency situations — can lead to physical damage to the information infrastructure.

Development and production of hardware and software — affects the quality and reliability of the systems used for protection.

Cyber-attacks — create risks of data leakage and disruption of critical systems.

Recruitment or blackmail of personnel — increases the threat of internal information leaks.

Let's take a closer look at the external factors that affect university cybersecurity.

1. Emergency situations. Higher education institutions are located in a certain area that may be vulnerable to natural or man-made hazards, which often occur simultaneously, increasing the overall impact on the facility. One hazard can trigger a number of others, increasing the damage.

Natural hazards: Any activity or functioning of an HEI's facilities is carried out in interaction with the natural environment, such as air, water or soil. The information environment of a higher education institution also interacts with natural elements through its components, such as information and telecommunication systems, communication lines, satellite and Wi-Fi antennas. These components can

be exposed to natural hazards, including: geological hazards (earthquakes, landslides, collapses, sinkholes and abrasion); hydrological hazards (floods, floodwaters, flooding, avalanches, heavy rains).

Technogenic hazards: the higher education institution uses energy, combustible materials and other potentially hazardous substances that can cause accidents. The analysis shows that a fire or explosion can cause significant damage to both the infrastructure and the staff of the institution. It is important to prevent such hazards by eliminating the conditions for their occurrence and maintaining industrial safety at the proper level.

Military actions are gradually gaining the status of a specific external threat to higher education institutions, as they can significantly affect the safety and stability of the educational process, changing the usual course of educational and scientific life. According to experts[6], in addition to direct threats to the lives and health of students, teachers and university staff, war can lead to serious destruction of the infrastructure of educational institutions. This includes damage to or destruction of buildings, laboratories, classrooms, libraries and other equipment used for research and education purposes. The consequences of such destruction can be extremely complex, not only disrupting the normal educational process, but also hampering important research and educational initiatives that require access to specialised equipment and resources.

In addition, war can have catastrophic consequences for the organisation of curricula and programmes, leading to the suspension or significant changes in the schedules of classes, teaching and examinations. This is especially true for specialities that require practical training or work with modern technologies, where even a temporary interruption of the educational process can affect students' qualifications and their ability to work in high-tech fields.

Another important problem is the restrictions on research and innovation projects. Many Ukrainian universities actively cooperate with foreign partners, but the ongoing war may lead to a breakdown in such international ties, making it difficult to participate in global research initiatives, international conferences and exchange of experience. It may also affect research funding, as grant programmes may be reduced or frozen.

Changes in the socio-economic situation also pose additional challenges for universities. In particular, economic instability leads to a reduction in budget funding, difficulties in attracting investment for the development of new research areas, and problems in providing universities with the necessary material resources. In such circumstances, higher education institutions are forced to optimise their costs, which may affect the quality of educational services and research.

All these factors together increase the risks for the future of Ukrainian education and science, so it is important to develop strategies that minimise the effects of the hostilities while maintaining a high level of education and research development even in times of crisis[7].

[6] Жила Г. Вища освіта в умовах війни: виклики, проблеми, перспективи для студентів та науковців. *Молодь і ринок,* 2023. №2 (210). С. 141–145. DOI: https://doi.org/10.24919/2308-4634.2023.276118

[7] Nataliia Filipenko (2023) The security for higher educational institutions during military aggression of the Russian federation against Ukraine. *Проєктний та логістичний менеджмент: нові знання на базі двох методологій*. Том 7 : збірник наукових праць. Одеса: КУПРІЄНКО С.В., 2023. 198 с.: іл., табл. (Серія «Проєктний та логістичний менеджмент: нові знан-

2. Information and communication technologies (ICTs) have now become the basis for increasing efficiency in scientific, applied and educational tasks in Ukraine. ICT can be defined as a set of actions related to the processing, storage and interpretation of information, as a result of which it is modified to meet the needs of a particular entity[8]. In this form, the data enters the public information flow, provoking a certain (mostly foreseen and planned) reaction of the audience of influence. However, as scholars emphasise, such implementation has also led to a significant dependence on ICT, in particular hardware and software components, which are critical for the proper functioning of many educational and scientific processes.

ICT hardware provides the technical basis — motherboards, processors, graphics adapters, disc drives, etc. Software enables the efficient operation of these hardware resources, including operating systems and a large number of application software. These two components are inextricably linked and form a single system. However, most of the software and hardware used in Ukraine originates from abroad, due to a number of factors, chief among them limited resources for technology research and development. The lack of sufficient funding and infrastructure to develop in-house R&D makes it difficult to create competitive Ukrainian products. Despite the fact that Ukraine has numerous talented IT professionals, economic constraints and low levels of investment in research significantly reduce the opportunities for large-scale innovation. As of today, the lack of funding and insufficient government support for domestic software and hardware development result in a serious shortage of high-quality domestic products capable of meeting the country's domestic needs. At the same time, international corporations with strong financial capabilities, access to state-of-the-art technology and a highly skilled team of specialists can create and supply products that are significantly superior to domestic counterparts in terms of quality and functionality. This gives them a significant advantage in the global market, making it difficult for Ukrainian developers to compete. The research potential of domestic higher education institutions is particularly affected, as limited funding and lack of sufficient resources for research lead to a decline in the quality of research papers and a decrease in the competitiveness of Ukrainian universities in the international arena. Due to the shortage of funds, many higher education institutions are forced to cut back on research programmes, limit the number of research projects, and reduce their participation in international research initiatives. This also leads to a decrease in the number of young scientists who are unable to implement their ideas due to a lack of adequate funding. In addition, the infrastructure for research often does not meet modern requirements, which significantly limits the opportunities for innovation. Lacking access to the latest technologies and modern laboratories, Ukrainian scientists are forced to work in conditions that make it difficult to achieve significant scientific results. This also leads to the emigration of talented scientists looking for better conditions to develop their careers abroad, which further exacerbates the problem. In such cir-

ня на базі двох методологій», Том 7). ISBN 978-617-7880-38-6. DOI: 10.30888/2616-8936.2023-07. Pp. 52-55.

[8] Биков В. Ю., Буров О. Ю., Дементієвська Н. П. Кібербезпека в цифровому навчальному середовищі. *Інформаційні технології і засоби навчання. 2019. Т. 70, № 2. С. 313-331. Режим доступу*: URL: http://nbuv.gov.ua/UJRN/ITZN_2019_70_2_25

cumstances, Ukrainian universities are increasingly focusing on retaining the existing scientific potential rather than developing it, which leads to a gradual lagging behind of the national science from the global trends.

The problem of the lack of domestic ICT hardware and software also poses a risk to cybersecurity. The foreign origin of hardware and software often causes additional difficulties with its maintenance and ensuring the security of data circulating in the internal systems of higher education institutions.

In view of the above, there is a need to identify the key aspects of the impact of foreign software on the cybersecurity of higher education institutions. The main factors can be summarised as follows:

First, shortcomings in the development and production of hardware and software. The inability to control all stages of production and testing of such equipment can lead to undesirable consequences during its operation, including full or partial failure. This potentially increases the risks to the functioning of the information infrastructure of higher education institutions.

Second, the lack of legal responsibility for ensuring cyber security during development and production. Since the responsibility for possible cyberattacks or failures is often borne by the user, not the developer or manufacturer, higher education institutions may have difficulty ensuring cyber security when using foreign software.

Thirdly, the hypothetical possibility of intentionally built-in vulnerabilities. Given the current trends in information confrontation between states, it can be assumed that foreign hardware and software solutions may potentially contain vulnerabilities that could be used to pursue the national interests of foreign states to the detriment of Ukraine's interests.

Fourthly, the difficulty of creating an integrated cyber defence system in higher education institutions based on foreign solutions. The lack of financial resources to implement an effective cyber defence system means that higher education institutions are forced to compromise between a high level of cyber security and the cost of relevant technologies.

Thus, foreign hardware and software creates additional risks for the cybersecurity of higher education institutions.

3. Cyberattacks. One of the main factors affecting the cybersecurity of higher education institutions is cyberattacks. Cyber threats should be understood as targeted actions that affect the components of the information environment using a variety of hardware and software, violating the confidentiality, integrity and availability of data. Cyberattacks can be both remote (when the attacker is outside the operational area of the facility) and local (with physical access to the facility).

According to experts[9], the main types of attacks include:

Malware: provides full access to the operating system, allows you to control user actions, delete or modify confidential data, etc.

Phishing: an attack aimed at exploiting the impulsiveness of the target, in particular through emails with malicious links or

[9] Трофименко О. Г. Кібербезпека освітнього сектора. Європейський вибір України, розвиток науки та національна безпека в реаліях масштабної військової агресії та глобальних викликів XXI століття (до 25-річчя Національного університету «Одеська юридична академія» та 175-річчя Одеської школи права) : у 2 т. : матеріали Міжнар. наук.-практ. конф. (м. Одеса, 17 червня 2022 р.) / за загальною редакцією С. В. Ківалова. Одеса : Видавничий дім «Гельветика», 2022. Т. 1. С. 698–700. Режим доступу: https://hdl.handle.net/11300/19765.

files, SMS attacks (smishing) or voice calls (vishing), which force the target to perform dangerous actions.[10]

SQL injection: the use of structured query (SQL) commands to access a server database, which can give access to sensitive data or allow the execution of malicious code.

XSS attack (cross-site scripting). This type of attack allows you to use the vulnerability of a website or server to conduct a cyber attack on a specific object. The attacker can integrate malicious code into a web page that is likely to be visited by the target. This enables the cybercriminal to obtain, for example, the victim's authorisation cookies, which allows them to bypass account security and gain unauthorised access to the system or information.

DoS attack (denial of service). This method of attack is based on overloading the target system when numerous bot devices connect to it simultaneously. This leads to the complete exhaustion of the server's RAM and CPU resources, causing users to lose access to the resource. Such attacks can paralyse a website or other information resource for a long time.

Zero-day attack. This type of threat exploits hardware and software flaws that developers or users are not yet aware of. This allows attackers to exploit these vulnerabilities for their own purposes before they are fixed. Such attacks may result in a breach of the confidentiality, integrity or availability of an information resource.

4. Recruitment or blackmail of personnel. Recently, there has been a growing number of reports of foreign agents in Ukraine and other countries, which has caused widespread public discussion, in particular due to the detention of high-ranking officials suspected of collaborating with enemy forces or foreign agents (e.g. the aggressor country, the russian federation). Such incidents become the subject of high-profile media investigations and pose serious challenges to national security. Agent activity, especially when it is aimed at actively recruiting or blackmailing citizens who hold key positions in government or in strategic areas, can have far-reaching consequences.

The threat posed by such methods extends not only to government agencies, but also to other institutions, including higher education institutions, especially those that train highly qualified personnel in technical and scientific fields. Higher education institutions, as the basis for the development of the national intellectual elite, are important elements in shaping the independence and security of the state. They train not only specialists who are directly involved in technological and scientific innovation, but also those who are involved in the development and management of critical infrastructures that are the basis for the country's functioning. Therefore, protecting these institutions from the influence of foreign agents and ensuring their cybersecurity is becoming one of the priority tasks in the context of the national security threat.

Preventing the recruitment of employees involved in managing the information infrastructure of universities, as well as faculty, is an important step in countering this threat. These individuals may be the most vulnerable to manipulation or blackmail because of their importance in ensuring the functioning of the educational process and maintaining the information security of higher education institutions.

[10] Татомир І. (2020) Кібербезпека університетів як спосіб протидії фішинговому шахрайству. *Економічний дискурс*. 2020. Випуск 1. С. 59-67. DOI: https://doi.org/10.36742/2410-0919-2020-1-7.

Under pressure or promises of benefits, they may be forced to take actions that will jeopardise not only individual systems but the entire information security of the university. This may include unauthorised access to critical data, breaches of cybersecurity standards, or even the creation of channels for the transfer of confidential information to foreign forces. In such circumstances, it is necessary to develop holistic strategies that include not only technological protections (such as a system for monitoring and detecting network breaches), but also organisational measures aimed at strengthening internal security.

According to experts[11], these measures may include ongoing training for staff, the development of ethics and procedures for checking the integrity of employees, as well as the creation of patriotic, cultural and psychological support to identify and prevent attempts at manipulation. In addition, it is important to raise awareness among students and teachers about cyber threats and their potential consequences for the security of not only the institution but the country as a whole.

Only a comprehensive approach to ensuring the security of higher education institutions can not only protect them from external threats, but also ensure the stability and independence of the country in the current geopolitical situation.

Conclusions. An analysis of external factors that affect the cybersecurity of higher education institutions reveals their uncontrollable nature on the part of the institutions themselves. Such external threats include cyber attacks (DDoS, phishing, zero-day attacks), constantly changing legislative requirements, the emergence of new technologies and other factors that can endanger the information systems and personal data of educational institutions. This creates an urgent need to strengthen internal components that can withstand such external influences and ensure the resilience of the university's cyber defences.

Building a strong cybersecurity system in an HEI should be based on a combination of strong internal factors. These include cybersecurity infrastructure, regular staff training and development, clearly defined risk management procedures, threat awareness, and an adequate level of IT infrastructure security. Cyber security programmes should include software updates, regular security audits and incident monitoring policies. Implementation of such a strategy will significantly improve the overall level of cyber defence while ensuring rapid response to new threats.

In addition, continuous analysis of internal factors is an important element of building an effective security system in a higher education institution. This includes assessing the level of cyber threat awareness among all staff, analysing existing security policies and procedures, and developing measures to create a security culture at the institution. It is important that the management of the HEI provides regular training for staff, implements updated procedures for handling confidential information, and maintains up-to-date technological solutions to prevent threats.

A systematic approach to security, which takes into account both external and internal factors, allows higher education institutions to significantly improve data protection and ensure effective functioning in the face of rapidly changing cyber risks. This approach encompasses not only technical tools such as antivirus software, firewalls and intrusion detection systems, but also organisational strategies that include continuous assessment and adaptation to new threats. Consideration of internal factors such as staff awareness, information access policies, and communications security can minimise risks associated with the human factor, which is often the most vulnerable element in cybersecurity systems.

External factors, such as global cyber threats, hacker groups or the influence of foreign agents, require constant monitoring of international trends and adaptation of internal procedures to new challenges. In such an environment, it is important not only to respond to current threats but also to conduct a predictive assessment of potential risks in order to anticipate and prevent possible incidents.

With a comprehensive approach that combines technical, organisational and human resources measures, HEIs can not only strengthen their cyber defences but also ensure the continuity of the educational process, research and innovation, even in the face of changing and complex cyber threats.

[11] Vitālijs Rakstiņš, Karina Palkova, Lidija Juļa and Natalia Filipenko (2024) Improving cybersecurity measures in academic institutions to reduce the risk of foreign influence. Socrates. Rīga Stradiņš University Faculty of *Law Electronic Scientific Journal of Law*. Volume 2024 (2024): Issue 1-29 (September 2024). P. 75-79. URL: https://doi.org/10.25143/socr.29.2024.2.75-79

References

Nataliia Filipenko (2023) The security for higher educational institutions during military aggression of the Russian federation against Ukraine. Proiektnyi ta lohistychnyi menedzhment: novi znannia na bazi dvokh metodolohii. Tom 7 : zbirnyk naukovykh prats. — Odesa: Kupriienko S.V., 2023. 198 s.: il., tabl. — (Seriia «Proiektnyi ta lohistychnyi menedzhment: novi znannia na bazi dvokh metodolohii», Tom 7). ISBN 978-617-7880-38-6. DOI: 10.30888/2616-8936.2023-07. Rr. 52-55 [in Ukrainian].

Nataliia Filipenko, Hanna Spitsyna, Olena Agapova, Karina Palkova, (2024). The Concept of Comprehensive Security for Higher Educational Institutions: Ukrainian and European Experience: Integrated Computer Technologies in Mechanical Engineering — 2023 Synergetic Engineering. Synergetic Engineering. Presents the proceedings of the ICTM´23 Conference held in Kharkov, Ukraine. URL: https://doi.org/10.1007/978-3-031-60549-9_23 [in Ukrainian].

Vitālijs Rakstiņš, Karina Palkova, Lidija Juļa and Natalia Filipenko, (2024). Improving cybersecurity measures in academic institutions to reduce the risk of foreign influence. Socrates. *Rīga Stradiņš University Faculty of Law Electronic Scientific Journal of Law*. Volume 2024 (2024): Issue 1-29 (September 2024). R. 75-79. URL: https://doi.org/10.25143/socr.29.2024.2.75-79

Bykov, V. Yu., Burov, O. Yu., Dementiievska, N. P. (2019). Kiberbezpeka v tsyfrovomu navchalnomu seredovyshchi. *Informatsiini tekhnolohii i zasoby navchannia*. T. 70, № 2. S. 313-331. URL: http://nbuv.gov.ua/UJRN/ITZN_2019_70_2_25 [in Ukrainian].

Biliavska ,Yu., Shestak, Ya. (2022). Kiberbezpeka ta kiberhihiiena: nova era tsyfrovykh tekhnolohii. *Tovary i rynky*. № 3. S. 47–59 [in Ukrainian].

Zhyla, H. (2023). Vyshcha osvita v umovakh viiny: vyklyky, problemy, perspektyvy dlia studentiv ta naukovtsiv. *Molod i rynok,* №2 (210). S. 141–145. DOI: https://doi.org/10.24919/2308-4634.2023.276118 [in Ukrainian].

Kiberbezpeka v informatsiinomu suspilstvi: Informatsiino-analitychnyi daidzhest / vidp. red. O. Dovhan; uporiad. O. Dovhan, L. Lytvynova, S. Dorohykh; Derzhavna naukova ustanova «Instytut informatsii, bezpeky i prava NAPrN Ukrainy»; Natsionalna biblioteka Ukrainy im. V.I.Vernadskoho. Kyiv, 2023. №7 (lypen). 270 s.

Lisovska, Yu. (2019). Kiberbezpeka: ryzyky ta zakhody : navch. posib. Kyiv : Kondor, 272 s. [in Ukrainian].

Lukashevych S., Filipenko N. Information Technologies in Law Enforcement, Security and Expert Activities. *Nauka i tekhnika sohodni*. 2023. №. 13 (27). URL: http://perspectives.pp.ua/index.php/nts/article/view/7560 [in Ukrainian].

Savchenko, V., Makliuk, O. (2024). Kiberbezpeka yak faktor efektyvnosti funktsionuvannia zakladiv vyshchoi osvity. *Ekonomika ta suspilstvo*, (60). URL: https://doi.org/10.32782/2524-0072/2024-60-24 [in Ukrainian].

Tatomyr, I. (2020). Kiberbezpeka universytetiv yak sposib protydii fishynhovomu shakhraistvu. *Ekonomichnyi dyskurs*. 2020. Vypusk 1. S. 59-67. DOI: https://doi.org/10.36742/2410-0919-2020-1-7. [in Ukrainian].

Trofymenko, O. H. (2022). Kiberbezpeka osvitnoho sektora. Yevropeiskyi vybir Ukrainy, rozvytok nauky ta natsionalna bezpeka v realiiakh masshtabnoi viiskovoi ahresii ta hlobalnykh vyklykiv XXI stolittia (do 25-richchia Natsionalnoho universytetu «Odeska yurydychna akademiia» ta 175-richchia Odeskoi shkoly prava) : u 2 t. : materialy Mizhnar. nauk.-prakt. konf. (m. Odesa, 17 chervnia 2022 r.). Odesa : Vydavnychyi dim «Helvetyka», T. 1. S. 698–700. URL: https://hdl.handle.net/11300/19765. [in Ukrainian].

Filipenko, N. Ye., Lukashevych, S. Yu., Andreieva, O. O., Salaieva, K. A. (2023). Sotsialno-pravovi ta moralno-etychni problemy zastosuvannia shtuchnoho intelektu ta informatsiino-komunikatsiinykh tekhnolohii. *Visnyk Penitentsiarnoi asotsiatsii Ukrainy,* (4), 95-103. URL: https://visnykpau.com/index.php/journal/article/view/650/511 [in Ukrainian].

Received by Editorial Board: 29.09.2024

Suggested Citation:

Lukashevych, S., Palkova, K. (2024). Cybersecurity of the Information Space of a Higher Education Institution. *Archives of Criminology and Forensic Sciences*. 2 (10). 60-71. DOI: https://doi.org/10.32353/acfs.10.2024.02