

Valentina Nadolska

Lesya Ukrainka Volyn National University

ORCID 0000-0002-9621-0074

Yuliia Melnychuk

Lutsk National Technical University

ORCID 0000-0002-9313-8716

Information security in higher education institutions of Ukraine: analysis of risks and management strategies

Introduction

In today's digital world, information security has become a critically important component of the functioning of higher education institutions. With the widespread integration of information and communication technologies into the educational process, administrative activities, and scientific research, the volume of processed and stored data is increasing – ranging from personal information of students and staff to intellectual property and research outputs. Accordingly, the level of threats that may harm both the institution's reputation and the security of its information infrastructure is also growing.

For Ukraine, the issue of information protection in the field of higher education has become particularly relevant in the context of hybrid warfare, cyberattacks on educational institutions, threats of unauthorized access to confidential data, and the active digitalization of all spheres of public life. At the same time, not all institutions are adequately prepared to detect and

counter such challenges, which necessitates a systematic approach to information security management.

The purpose of this article is to analyze the main information security risks in Ukrainian higher education institutions and to outline effective strategies for their management. The study is based on the analysis of existing practices, regulatory and legal documents, as well as international experience in the field of information security in education.

Literature Review

Recent studies focus on issues of cybersecurity, digital culture, and management practices in the field of higher education in Ukraine. For example, the research conducted by H.A. Deya covers the following:

- current challenges, including phishing, malware, and data breaches;
- methods of system analysis and threat classification;
- strategic measures related to cyber hygiene, competency development, technical infrastructure upgrades, and the development of incident response policies in educational institutions (Дей, 2025).

Ukrainian scholars V. Savchenko and O. Maklyuk analyze the impact of cybercrime on the functioning of higher education institutions. They emphasize the importance of staff training, responsibility, and the level of digital culture in ensuring stability within the educational process (Савченко, Маклюк, 2024).

Researchers also explore the development of cyber competencies and cyber culture. In particular, I. Kozubtsov, N. Zinchenko, A. Kotenko, and I. Averichev analyze the issues of information security in the digital educational and scientific environment of HEIs during wartime, as well as the need to foster a culture of cyber hygiene among students in the humanities (Козубцов, Зінченко, Котенко, Аверічев, 2024).

S. Lupinovich and I. Lapshyna study the impact of information warfare and information pressure on student motivation, proposing ways to develop information hygiene in the context of distance education (Лупінович, Лапшина, 2023).

Regional and national contexts of information security in higher education institutions are examined by I. Radomskyi, who focuses on blended learning during wartime, data confidentiality, secure digital environments, and methods of protecting personal data at the National Aviation University (Радомський, 2024). I. Bosak analyzes cyber threats at the national level and countermeasures that are also relevant to the education sector (Босак, 2025).

International experience and approaches to information security in HEIs are discussed in the study by Lukashevych & Palkova. The authors

describe the impact of cybercrime on Ukrainian HEIs and propose organizational, technical, and educational measures to enhance cyber resilience (Lukashchych, Palkova, 2024).

International research, including that published on arXiv, highlights the impact of virtual laboratories (V-Labs) on active learning and student engagement in distance cybersecurity education, as well as the integration of generative AI to foster critical thinking and evaluate security policies in education (Kebande, 2024).

Thus, information security in Ukrainian higher education is shaped at the intersection of technical, organizational, and educational factors. The most pressing issues include low levels of cyber hygiene among participants in the educational process, a shortage of qualified personnel, the absence of systematic policies, and insufficient technical capacity.

Regarding recommended measures for improving the information security system in Ukrainian HEIs, researchers highlight the following:

- the creation of integrated Information Security Management Systems (ISMS) based on ISO/IEC standards;
- regular cybersecurity training for staff and students;
- the development of a culture of digital and information literacy;
- the use of technological innovations (such as V-Labs and AI-based approaches) to enhance learning effectiveness.

Methodology

The study employs a comprehensive theoretical approach to analyzing the issue of information security in higher education institutions of Ukraine. The methodological foundation is based on content analysis of scientific publications, analytical reports, regulatory documents, and international standards in the field of information security.

More than 20 relevant sources by Ukrainian and international authors (2020–2024) were analyzed, covering topics such as cyber threats, risk management in educational environments, digital transformation, and the organization of information protection systems in HEIs. Particular attention was paid to publications in professional journals, ENISA reports, and the provisions of ISO/IEC 27001, ISO/IEC 27005, and NIST SP 800–53 standards.

To identify the main types of risks, the method of logical-semantic generalization and threat classification was applied, based on case descriptions in scholarly sources. A comparative analysis was also conducted between approaches to information security in higher education in Ukraine and European Union countries, particularly in terms of regulatory frameworks, organizational structure of security systems, and levels of digital literacy.

The obtained results made it possible to formulate a generalized typology of risks and propose corresponding strategies for their management at the institutional level.

Findings: Risk Analysis

We examined various types of information security risks in Ukrainian higher education institutions (Нашинець-Наумова, Бурячок, Коршун, Жильцов, Складанний, Кузьменко, 2020). The main categories of risks include technical, organizational, human factor (sociotechnical threats), external cyber-attacks, systemic risks, and external instability.

Technical risks include outdated or untimely updated infrastructure, particularly electronic educational systems that rely on BYOD (Bring Your Own Device) connections, which expose institutions to phishing and malware threats. Additionally, the absence of network segmentation and defined security zones allows attacks to spread, even if they originate from a single point in the network. Examples of technical risks include vulnerable systems and weak BYOD policies, with possible consequences such as data leakage or destruction and DDoS attacks.

Organizational risks involve the lack of clearly defined cybersecurity policies and standards regulating access, incident response, auditing, and control. They also include insufficient funding, staff shortages, and fragmented IT governance – where individual faculties operate autonomously, making unified protection more difficult. Examples of such risks are the absence of policies and fragmented IT management, with likely consequences including uncoordinated responses and low security effectiveness.

Regarding sociotechnical threats (Каулька, Пономарьова, 2025), key issues include a low level of cyber hygiene—students and staff often rely on weak passwords, fail to recognize phishing messages, and frequently download unsafe content. Insider threats – both intentional and accidental – are also significant, as they originate from within the organization (e.g., students or employees), increasing overall risk. Examples include poor cyber hygiene and phishing, which can lead to consequences such as account compromise and personal data leaks.

External attacks are represented by large-scale incidents, such as Petya (NotPetya) in 2017, HermeticWiper, and DDoS attacks during 2022–2023, which demonstrated high levels of activity by cybercriminals and cyber forces targeting Ukraine's critical infrastructure. Educational institutions, including universities, can become targets of such attacks due to their reliance on IT services.

In wartime conditions, cyberattacks on governmental and educational services have intensified, driven by the aggressor's political motives—this reflects systemic risks. There is also increasing dependence on vendors/cloud providers (such as AWS), which introduces additional risks in the case of access loss or coordinated attacks (Lallie, Thompson, Titis, Stephens, 2023).

Information Security Threats under Martial Law in Ukraine

Under martial law conditions, information security risks for higher education institutions in Ukraine acquire a qualitatively new dimension. Educational institutions increasingly function as elements of the national information infrastructure, ensuring the continuity of education and research during wartime. Consequently, they face not only traditional cyber threats but also targeted attacks aimed at destabilizing public services and undermining trust in state institutions.

One of the most significant wartime threats is the intensification of targeted cyberattacks against educational information systems, including learning management systems, electronic document management platforms, and research databases. These attacks often pursue strategic objectives rather than purely financial gain and may be synchronized with broader cyber operations against national infrastructure.

The level of social engineering and phishing attacks has also increased significantly during wartime. Heightened psychological pressure, stress, and information overload make students and staff more susceptible to manipulation. Cybercriminals exploit war-related topics such as evacuation, humanitarian aid, or institutional emergency notifications to gain unauthorized access to user accounts and sensitive data, which amplifies socio-technical risks previously identified in educational environments (Каулька, Пономарьова, 2025).

Operational challenges caused by relocation of universities, power outages, and unstable internet connectivity further exacerbate information security risks. In such circumstances, institutions are often forced to rely on temporary or emergency technical solutions that may not fully comply with established cybersecurity standards, increasing the likelihood of incidents.

Finally, the human factor plays a critical role under wartime conditions. Chronic stress, fatigue, and emotional strain among academic and administrative staff increase the probability of human error and non-compliance with security procedures. As a result, information security risks during martial law become systemic in nature, requiring comprehensive and adaptive risk management approaches rather than isolated technical solutions.

Discussion: Information Security Risk Management Strategies in Ukrainian Higher Education Institutions

In response to numerous information security threats – arising from both external cyberattacks and internal vulnerabilities – Ukrainian higher education institutions apply a variety of risk management strategies. However, the maturity level and effectiveness of these strategies vary significantly depending on the type of institution and its technical, organizational, and human resources. Under wartime conditions, the importance of structured and resilient risk management approaches becomes particularly evident.

Organizational Strategies. Organizational strategies form the foundation of information security risk management in higher education institutions. They primarily involve the development of a regulatory framework, including information security policies, personal data protection regulations, and internal guidelines governing the use of IT systems. These documents define roles and responsibilities, establish rules for access control, incident response, and auditing, and create a legal and organizational basis for protecting information assets.

At leading Ukrainian universities, such as the National University of Kyiv-Mohyla Academy and Ivan Franko National University of Lviv, information security policies cover key aspects including risk identification, access management, data encryption, activity monitoring, and internal audits. However, in many regional institutions, such policies either remain absent or exist only formally, without effective implementation mechanisms.

Under martial law, organizational strategies acquire additional significance, as universities must operate in conditions of uncertainty, relocation, and limited resources. Clear internal regulations and well-defined decision-making procedures become critical for maintaining continuity of educational and administrative processes and for coordinating responses to security incidents.

Technical Strategies. Technical strategies focus on the implementation of technological measures aimed at preventing, detecting, and mitigating cyber threats. Ukrainian HEIs employ basic cybersecurity tools such as anti-virus software, firewalls, intrusion detection systems (IDS), VPN access, and network segmentation. Increasingly, institutions are transitioning to cloud-based platforms with integrated security mechanisms, including Google Workspace for Education and Microsoft 365.

At the same time, unequal access to modern IT solutions remains a serious challenge. Due to limited funding, some universities continue to rely on outdated hardware and software, which significantly increases their vulnerability to cyberattacks. In addition, the lack of systematic software

updates and continuous security monitoring reduces the effectiveness of technical protection measures.

In wartime conditions, technical strategies must also address risks related to power outages, unstable internet connectivity, and emergency transitions to remote or hybrid learning. The resilience of information systems and the availability of backup infrastructure become crucial factors in ensuring the stability and security of educational services.

Administrative Strategies. Administrative strategies encompass measures related to monitoring, auditing, training, and coordination of information security activities. Regular training and awareness-raising initiatives are essential, as the human factor remains one of the primary sources of risk. Phishing attacks, weak password practices, and improper handling of sensitive data are often the result of insufficient user awareness.

Some Ukrainian HEIs conduct cybersecurity training for staff and students, as illustrated by initiatives at Uzhhorod National University. However, such practices are not systematic at the national level, and most universities lack dedicated cybersecurity positions. Information security responsibilities are often combined with general IT maintenance tasks, limiting the effectiveness of risk management.

Administrative strategies also include backup and disaster recovery planning, as well as security audits and incident management. While some institutions use cloud-based backup solutions, many still lack comprehensive incident response plans. Security audits are typically conducted only in response to incidents or regulatory requirements, rather than as part of a proactive risk management strategy.

Under wartime conditions, administrative coordination and cooperation with national and international bodies – such as CERT-UA, the State Service of Special Communications, and EU digital education initiatives – become especially important. These partnerships provide access to expertise, training, and up-to-date security solutions, although participation remains limited to a relatively small number of institutions.

Overall, although Ukrainian higher education institutions are making efforts to implement comprehensive information security risk management strategies, their effectiveness remains inconsistent. The main restraining factors include institutional weaknesses in policy enforcement, a shortage of qualified cybersecurity personnel, limited funding for infrastructure modernization, and low levels of information security awareness among users.

To enhance information security in the higher education sector, both nationwide initiatives and the strengthening of internal security culture within each university are essential, particularly in the context of ongoing military and cyber threats.

Conclusion

As a result of the conducted study, it was established that information security in higher education institutions in Ukraine is a multidimensional issue that encompasses both technical and organizational aspects. The main risks associated with the activities of such institutions include the leakage of confidential information, cyberattacks, gaps in staff's digital literacy, poor access management practices, and an insufficient level of regulatory oversight.

Based on the analysis of scientific and analytical sources, it was found that an effective information risk management strategy should include the following components: development of information security policies, regular staff training, implementation of modern technical protection tools (in particular, intrusion detection systems, multi-factor authentication, and data backup), as well as fostering a cybersecurity culture at the organizational level.

In the context of war and the ongoing digital transformation of education in Ukraine, the issue of information protection is becoming increasingly critical. Therefore, it is essential to develop a national digital security strategy for the education sector that considers both global challenges and the specific context of Ukrainian higher education institutions.

Future research may focus on empirically testing the proposed strategies, as well as examining data protection practices in individual Ukrainian universities.

In the context of ongoing hybrid warfare and large-scale cyber confrontation, information security in higher education institutions should be viewed not only as an internal organizational challenge but also as an integral component of national security. Universities operate as critical nodes of knowledge production, human capital development, and digital infrastructure, which makes them potential targets in information and cyber warfare. Disruption of educational information systems may have long-term consequences for social stability, workforce development, and the resilience of the state. Therefore, the protection of the educational information environment requires policy-level attention, including the development of national cybersecurity strategies for the education sector, integration of higher education institutions into national incident response frameworks, and alignment with international security standards and best practices. Strengthening information security in higher education thus contributes not only to institutional resilience but also to the overall security and sustainability of society under conditions of prolonged military and cyber threats.

References

- Harjinder S. Lallie Thompson A., Titis E., Stephens P. (2023). Understanding Cyber Threats Against the Universities, Colleges, and Schools. *arXiv*. <https://doi.org/10.48550/arXiv.2307.07755>.
- Lukashevych S., Palkova K. (2024). Cybersecurity of the Information Space of a Higher Education Institution. *Archives of Criminology and Forensic Sciences*, 10(2), 60–71. <https://doi.org/10.32353/acfs.10.2024.02>.
- Victor R. KEBANDE. (2024). The Impact of Virtual Laboratories on Active Learning and Engagement in Cybersecurity Distance Education. *arXiv*. <https://doi.org/10.48550/arXiv.2404.04952>.
- Босак І. (2025). Інформаційна безпека України: загрози та методи протидії. *Київський економічний науковий журнал*, (9), 33–38. <https://doi.org/10.32782/2786-765X/2025-9-4>.
- Дей Г.А. (2025). Кібербезпека в українських закладах освіти: основні проблеми та шляхи розв'язання. *Таврійський науковий вісник. Серія: Публічне управління та адміністрування*, (2), 35–43. <https://doi.org/10.32782/tnv-pub.2025.2.5>.
- Каулька О., Пономарьова Л. (2025). Забезпечення кібербезпеки в освітніх установах: обізнаність, правила, стратегія. *Фахова передвища освіта*. Retrieved July 28, 2025, from <https://osvitafp.com.ua/2025/02/07/zabezpechennia-kiberbezpeky-v-osvithnikh-ustanovakh-obiznanist-pravyly-stratehiia/>.
- Козубцов І., Зінченко Н., Котенко А., Аверічев І. (2024). Проблеми забезпечення інформаційної безпеки суб'єктами освітньої діяльності в цифровому освітньо-науковому середовищі закладів освіти. *Смарт технології: промислова та цивільна інженерія*, 2(15), 56–65. <https://doi.org/10.32347/st.2024.2.1204>.
- Лупінович С.М., Лапшина, І.С. Формування навичок інформаційної безпеки у здобувачів вищої освіти в сучасних реаліях. *Науковий журнал Хортицької національної академії. Серія: Педагогіка. Соціальна робота*, 2 (9), 68–74.
- Нашинець-Наумова А.Ю., Бурячок В.Л., Коршун Н.В., Жильцов О.Б., Складанний П.М., Кузьменко Л.В. (2020). Технологія забезпечення інформаційної і кібербезпеки в закладах вищої освіти України. *Інформаційні технології і засоби навчання*, (3), 337–354. <https://doi.org/10.33407/itlt.v77i3.3424>.
- Радомський І.П. (2024). Інформаційна безпека та конфіденційність у змішаному навчанні в умовах війни. *Актуальні проблеми в системі освіти: загальноосвітній заклад середньої освіти – доуніверситетська підготовка – заклад вищої освіти*, 1(4), 394–404. <https://doi.org/10.18372/2786-5487.1.18755>.
- Савченко В., Маклюк О. (2024). Кібербезпека як фактор ефективності функціонування закладів вищої освіти. *Економіка та суспільство*, (60). <https://doi.org/10.32782/2524-0072/2024-60-24>.

Author's Bionote

Valentyna Nadolska, PhD in Historical Sciences, Associate Professor at the Department of Museology, Monument Studies, and Information and Analytical Activities at Lesya Ukrainka Volyn National University (Ukraine). She teaches the courses “Information and Analytical Activity”, “Information Analytics”, and

“Information and Analytical Services” for bachelor’s and master’s degree students. Her research focuses on the development of information and analytical activity in Ukraine.

Selected publications

- Nadolska, V. (2024). Scientific centers for the study of information activity as a component of Ukraine’s scientific field. In *Topical issues of modern education and science in the context of European integration progress: Proceedings of the 10th International Scientific and Practical Conference (Lutsk, May 23–24, 2024)* (pp. 54–61). LIROL.
- Nadolska, VV. (2024). Analytical centers of Ukraine as actors in information relations. In *The humanitarian space of science: Experience and prospects: Proceedings of the 40th International Scientific and Practical Online Conference (Pereiaslav, March 4, 2024)*, 40, 132–134.
- Yuliia Melnychuk, PhD in Pedagogical Sciences, Associate Professor at the Department of Digital Educational Technologies at Lutsk National Technical University (Ukraine). She teaches the courses “Computer Security and Cryptography”, “Information Protection Technologies”, “Algorithmization and Programming”, and “Web Technologies and Web Design”. Her research focuses on educational information systems, their security, and protection.
- Selected publications:
- Melnychuk Y., Satsyk V., Grudetsky R., Kuzmych O., Bahniuk N., Hlynchuk L. (2020). Reduction of server load by means of CMS Drupal. In *2020 10th International Conference on Advanced Computer Information Technologies (ACIT)*. IEEE. <https://doi.org/10.1109/ACIT49673.2020.9208874>.
- Barabash O., Laptiev O., Sobchuk V., Salanda I., Melnychuk Y., Lishchyna V. (2021). Comprehensive methods of evaluation of distance learning system functioning. *International Journal of Computer Network and Information Security*, 13(3), 62–71. <https://doi.org/10.5815/ijcnis.2021.03.06>.
- Melnychuk Y., Mialkovska L., Herasymchuk H., Sushyk I., Martyniuk Y., Haponchuk O. (2023). Management models and methods in modern education: Information technologies, sustainability and development. *The Global Development of Innovative Technologies and Their Impact on the Education*, 16(se2). <https://brajets.com/index.php/brajets/article/view/1256>.
- Markina L., Palchevskiy B., Hrudetskyi R., Smoliankin O., Melnychuk Y., Khrystynets N. (2023). Optimization of ethanol production using state-space modeling and optimal control technology. In *2023 13th International Conference on Dependable Systems, Services and Technologies (DESSERT)* (pp. 1–7). IEEE. <https://doi.org/10.1109/DESSERT61349.2023.10416529>.
- Satsyk V., Reshetylo O., Markina L., Khrystynets N., Bahniuk N., Melnychuk Y. (2024). Modeling of improved solar energy installation for efficient power systems. In *2024 14th International Conference on Advanced Computer Information Technologies (ACIT)* (pp. 688–694). IEEE. <https://doi.org/10.1109/ACIT62333.2024.10712532>.

Abstract

The article explores the issue of information security in higher education institutions (HEIs) of Ukraine as one of the key challenges in the context of the digitalization of the educational process. The growing use of digital technologies, the shift toward remote and hybrid learning, as well as the increasing volume of personal data processing, significantly heighten the relevance of protecting the information space within the educational environment. The study provides a theoretical analysis of the current risks faced by Ukrainian HEIs. The main types of risks identified include: leakage of confidential information, phishing attacks, malicious software, cybercrime, insufficient user awareness, and a weak regulatory and organizational framework for IT security management. It is noted that these threats are exacerbated under martial law, as the risk of external interference in educational infrastructure increases. Based on the analysis of literature sources, the paper describes existing risk management strategies, including: organizational (development of security policies, staff training), technical (implementation of data protection systems, data backups), and administrative (monitoring, auditing, access control). The need to integrate information security into the digital development strategies of HEIs is substantiated. In the conclusions, the article offers recommendations for improving approaches to protecting the educational information environment, particularly through the enhancement of digital culture, development of clear regulations, and increased investment in security.

Key words: information security, higher education institutions, cyber threats, digital transformation, risk management, Ukraine.