QUBAHAN ACADEMIC JOURNAL
VOL. 5, NO. 1, March 2025
https://doi.org/10.48161/qaj.v5n1a1500

The Influence of National Information Security Policies on Advancing Higher Education

Viktor Paliukh [1*], Iryna Kovtun [2], Tetiana Pidlisna [3], Tatyana Tatarnikova [4], and Stanislav Poroka [5]

[1] Department of State Security Problems of the Training and Research and Production Center, National University of Civil Protection of Ukraine, Kharkiv 61023, Ukraine;
[2] Department of Public Administration and Administration, Khmelnytskyi University of Management and Law named after Leonid Yuzkov, Khmelnytskyi 29000, Ukraine;
[3] Department of Public Management and Administration, Faculty of Public Administration, Leonid Yuzkov Khmelnytskyi University of Management and Law, Khmelnytskyi 29000, Ukraine;
[4] Center of Forensic and Special Expertises of the Ukrainian Scientific and Research Institute of Special Equipment and Forensic Expertise of the Security Service of Ukraine, Kharkiv 61023, Ukraine;
[5] Department of Public Administration and Law, Institute of Management and Population Security, National University of Civil Protection of Ukraine, Kharkiv 61023, Ukraine.

* **Corresponding author:** paluxviktor88@gmail.com.

ABSTRACT: In the context of digitalization, the growing role of information security in higher education requires a comprehensive approach that will ensure high-quality regulatory and legal regulation, the development of cyber hygiene, the protection of intellectual property, and effective information risk management. The article aims to analyses and evaluate current challenges and opportunities for improving state information security policy measures in higher education. In addition to the general scientific methods of theoretical substantiation, in particular synthesis, systematization and generalization, this study analyzed the regulatory framework and statistical data characterizing the current state of information security of higher education institutions. In addition, a correlation analysis was carried out between the number of students and information security indicators of higher education institutions in Ukraine. The analysis's results show that concentrating fewer students in the system can contribute to better protection of digital services through a focus on quality. This confirms the analysis's initial assumption of a positive correlation with the Protection of digital services ($B = -0.43$ at $p = -0.099$; $M = 0.715$ at $p = 0.549$). High p-values in the correlation analysis indicate the possibility of random relationships, which requires further verification using larger samples and additional methods. Recommendations for improving information security in higher education include the introduction of unified cybersecurity standards for educational institutions, the development of specialized legislation to protect scientific data and confidential information, the promotion of research and education initiatives in the field of information security through state funding, the creation of focal points for data exchange between universities and government agencies, and active participation in international projects within the framework of European integration.

Keywords: information security, legal regulation, data protection, cyber defense, higher education institutions.

I. INTRODUCTION

In today's context of the rapid growth of the digitalization of society and the actualization of cyber threats, the state policy of information security in higher education is gaining strategic importance. The information security of higher education institutions (HEIs) is becoming a key element in ensuring the sustainability of the educational process, protection of intellectual resources and data privacy in the period

of aggravation of hybrid threats. The effectiveness of such a policy depends on an integrated approach to information security regulation that ensures the integration of legislative, technical and organizational solutions [1]. However, the existing problems of ensuring the quality of information security for the development of higher education by public authorities vary considerably depending on regional characteristics, the level of technological readiness of higher education institutions and the effectiveness of regulatory and legal support for information security in the country or geographical region [2]. In particular, in Ukraine, the war is currently causing a decrease in funding for higher education to implement the latest data protection technologies [3], which complicates the interaction and regulation of educational institutions in cybersecurity by public authorities. Therefore, the key hypotheses of the study can be defined as follows:

1. H1: Reducing the number of students in higher education institutions contributes to better protection of digital services by focusing on quality assurance.
2. H2: A decrease in the number of students in higher education institutions affects the level of funding for technological and human resources support for information systems security.

Thus, the purpose of the article is to study the components of the state information security policy in the field of higher education in Ukraine and to assess the effectiveness of this policy in the context of the ongoing cyber war. The article aims to develop directions for improving the system of information resources protection in higher education institutions, taking into account the challenges of digitalization and current cybersecurity threats to Ukrainian higher education institutions. Thus, the main objectives of the study are:

1. To determine the effectiveness of regulatory and legal regulation of information security in higher education institutions;
2. To identify the key components of the state information security policy in the field of higher education in Ukraine;
3. To develop recommendations for improving the state information security policy in higher education, considering the current risks of cyber warfare.

The study is a unique contribution to the scientific discourse on the effectiveness of the state policy of information security for the development of higher education, given its focus on improving public policy and solving key problems in the field of information security in the Ukrainian higher education system. This study addresses a gap in the development and integration of state information security policies for higher education institutions in Ukraine, given the impact of war, limited funding, and declining student enrolment on the effectiveness of such policies.

II. LITERATURE REVIEW

The issue of the spread of information security risks in higher education arises in the context of the general trend towards digitalization, which is accompanied by an increase in cyber threats, such as unauthorized access to educational platforms, leaks of personal data of students and other participants in the educational process, as well as technical attacks on the servers of educational institutions. In Ukraine, these risks are becoming more pronounced due to the outbreak of Russia's full-scale armed aggression, which is also accompanied by the spread of disinformation and propaganda and an increase in the number of cyberattacks as part of an ongoing cyberwar [4]. Even though certain types of cybercrime can be easily prosecuted due to the inherent adaptability of existing conventional laws, prompt legislative intervention is important in crisis or unusual situations [5]. Also, the scientific literature, in particular the works of Chang & Huang [6], Odebade and Benkhelifa [7], and Poliakova et al. [8], emphasizes the importance of the state as a coordinator of efforts of various sectors for the implementation of information security. Therefore, Horta [9] prioritises measures to consolidate the system given declining student numbers, reforming HEIs to cope with potentially reduced resources and automation, and restructuring the academic research system to ensure that the knowledge produced is more sustainable, shared and meaningful. Similar conclusions were reached by Jafari and Keykha [10], Shi and Yonezawa [11] and

Yang [12], who also highlight the impact of automation and the problem of declining student numbers as priority issues for the academic community. In this context, the advantage of Ukrainian higher education institutions is that they have a stable, hierarchical management system with all the necessary conditions for life and operate on the principles of centralized management [13]. However, the increased level of threat to information systems of higher education institutions requires the Ukrainian government to improve public policy to ensure enhanced protection of this area in cyber warfare. Bielai and Sporyshev [14] note the need to create and implement uniform standards for cyber defense, protect the intellectual property of scientists and researchers operating based on higher education institutions, and ensure the confidentiality of participants' data in the educational process. Similar ideas are also being promoted globally, with Weng and Wu [15] proposing establishing a global data privacy and security standard. Instead, according to Nahaichuk et al. [3], effective public policy involves funding infrastructure modernization and creating specialised centres for cybersecurity training. Similar proposals have also been put forward by Tkachuk [16] and Piatnychuk [17] to ensure national information security. In the Ukrainian context, the issue of integrating European Union standards in the field of data protection remains relevant, which requires the adaptation of existing regulations to the conditions of martial law and post-war reconstruction [18, 19, 20].

III. MATERIAL AND METHOD

1. APPLIED METHODS

1.1 Problem Statement

Ukraine was selected as a case study due to its distinct circumstances in the context of ongoing military aggression. The rise in cybersecurity threats has significantly impacted the stability of educational and information systems, necessitating prompt and tailored measures in the realm of national information security policy. The study analyses the state policy of information security in higher education in Ukraine. It aims to identify problematic aspects of regulatory and legal regulation, formulate an understanding of key threats, and develop directions for further improving the mechanisms for protecting educational institutions' information resources, taking into account current threats to information systems.

1.2 Data Collection

First, the research criteria are the number of bachelor's and master's students in Ukrainian higher education institutions. To collect the necessary data, the official reports of the State Statistics Service of Ukraine for 2010-2023 were processed. To collect data on other research criteria that characterise the state of information security of Ukrainian higher education institutions, the e-Governance Academy Foundation reports on data and components of the National Cyber Security Index for 2016-2023 were analysed.

2. RESEARCH METHODS

The synthesis of information from the literature was used to determine the components of the state policy of information security for the development of higher education in Ukraine. As part of the application of this method, a number of regulatory and legal documents were analysed, which are the basis of Ukraine's state policy in the field of information security of higher education institutions. The systematisation method was used to formulate key aspects and tasks within the main components of the state information security policy of Ukrainian higher education institutions. The method of generalisation was applied to develop recommendations for improving existing and forming new directions of the state information security policy. Correlation analysis is used to substantiate the interaction of demographic changes with the level of information security in the context of current priorities of higher education institutions. The criteria for the analysis are the statistical data collected from official sources on the distribution of the number of bachelor's and master's students in Ukrainian higher education institutions and indicators of information security of educational institutions. The Pearson's Correlations tool in the JASP statistical software obtained the correlation results.

2.1 Restrictions

High p-values in the correlation analysis indicate the possibility of random relationships, which requires further verification using larger samples and additional methods.

IV. RESEARCH RESULTS

3. COMPONENTS OF THE STATE POLICY OF INFORMATION SECURITY OF HIGHER EDUCATION DEVELOPMENT IN UKRAINE

The components of the state policy of information security in the field of higher education in Ukraine are based on a comprehensive legal and regulatory framework, including key legislative and strategic acts. The legislative framework is determined by the Laws of Ukraine "On National Security of Ukraine" No. 2469-VIII of 09.08.2024, "On Critical Infrastructure" No. 1882-IX of 21.09.2024, "On Personal Data Protection" No. 2297-VI of 27.04.2024, "On Protection of Information in Information and Telecommunication Systems" No. 80/94-VR of 28.06.2024, which provide a framework for the regulation of information security, including the definition of key concepts, mechanisms for protecting data and information systems, and requirements for critical infrastructure facilities, including higher education institutions and other educational institutions. Additionally, regulations of the Cabinet of Ministers of Ukraine play an important role, in particular, the resolutions "On Approval of the Regulation on Organisational and Technical Model of Cyber Defence" No. 1426-2021-p of 29.12.2021 and "Some Issues of Critical Information Infrastructure Objects" No. 1109-2020-p of 24.09.2024, which detail approaches to cybersecurity, including the procedure for protecting information in higher education institutions. Particular attention should be paid to the Cybersecurity Strategy of Ukraine for 2021-2025, which is also part of the country's overall information security policy. This strategy defines the directions of cyber defence development, including an educational component aimed at building competences and developing professional capacity in information security. In this context, it should be noted that the Law of Ukraine "On the Basic Principles of Ensuring Cybersecurity of Ukraine" No. 2163-VIII dated 28.06.2024 and the Resolution of the Cabinet of Ministers of Ukraine "On Approval of the General Requirements for Cybersecurity of Critical Infrastructure Objects" No. 518-2019-p dated 07.09.2022, which complement the regulatory framework by focusing on reforming management approaches that take into account cyber threats, in particular those related to the destabilisation of the public sector in the context of Russia's hybrid war against Ukrainian information systems.

The comprehensive regulatory framework for ensuring the information security of Ukrainian higher education institutions forms the basis for implementing state policy aimed at protecting information resources and increasing the resilience of the education sector to cyber threats. The key components of the state policy of information security for developing higher education include infrastructure and cybersecurity, as shown in Figure 1.

However, some aspects still require the development of appropriate directions for improving the state information security policy, in particular, the need to integrate information security principles into the activities of higher education institutions. Despite the fact that information security in higher education institutions requires the introduction of unified standards for cyber defence, intellectual property protection and data confidentiality, national legislation, including the Law of Ukraine "On the Basic Principles of Ensuring Cybersecurity of Ukraine", does not contain specialised norms that would take into account the specifics of educational institutions. In a time of war, it is also important to consider the regional distribution, the level of digitalization of the educational process and the priority of cyberattacks by Russia on all the country's higher education institutions. Therefore, it is crucial to ensure multi-level protection of data management systems and improve protocols for protecting participants' personal data in the educational process by the Law of Ukraine "On Personal Data Protection" requirements. Encouraging science and education in information security is also a necessary step in implementing state information risk management in the fields of technological support, cyber hygiene of educational institutions, and data protection. Given

that out of 281 universities, academies, institutes, and 338 colleges, technical schools, and vocational schools with the status of higher education institutions, only 61 have educational and professional programmes in information technology, cybersecurity, and information protection, a possible solution is to increase financial support for the relevant specialities and promote the development of new fields of knowledge in this area.

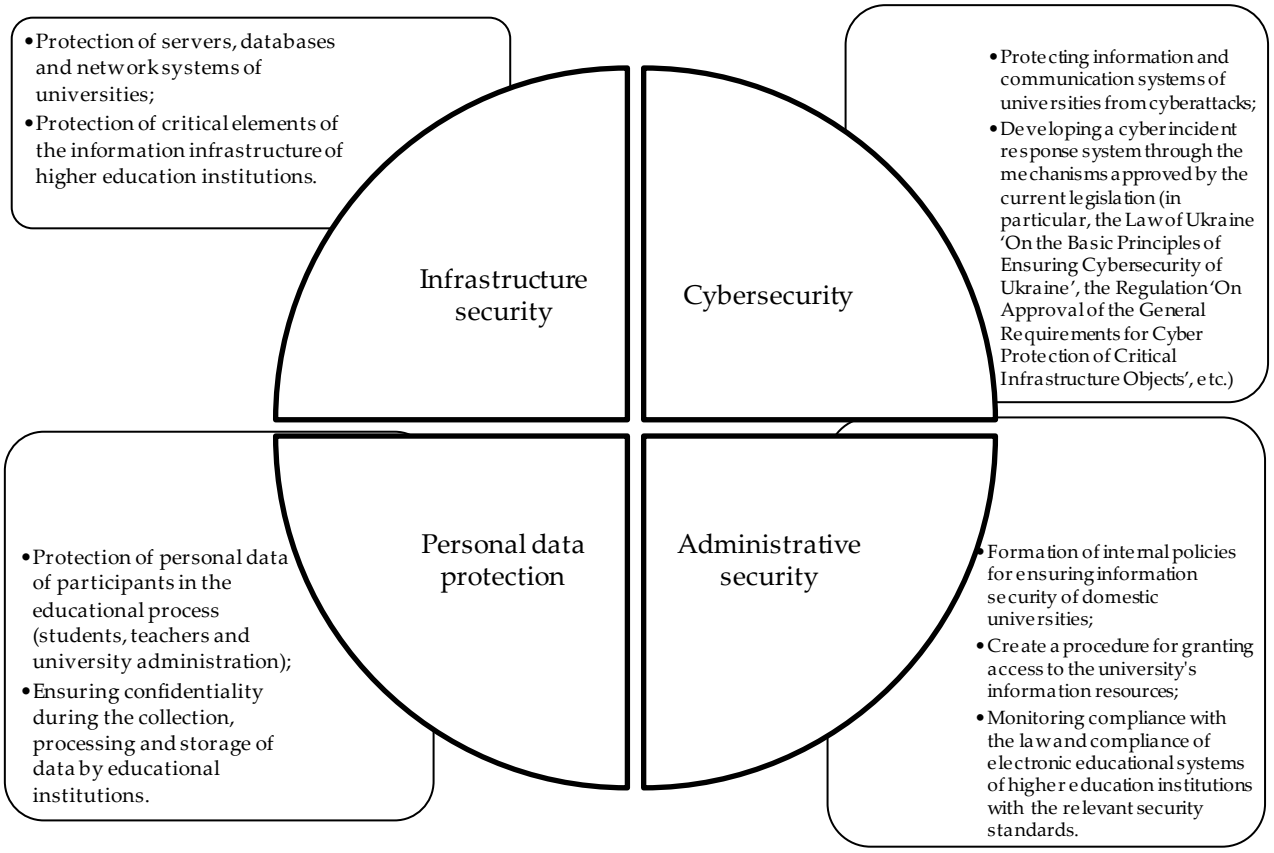

FIGURE 1. Components of the state policy of information security of higher education institutions.
Source: compiled by the author

Another important solution to increase the effectiveness of implementing measures within the state information security policy framework in higher education institutions is to ensure clear interaction between government agencies, educational institutions, and the private sector. In this context, it is necessary to create special coordination centres based on higher education institutions to exchange information and experience between educational institutions, the Ministry of Digital Transformation of Ukraine and the State Service for Special Communications and Information Protection of Ukraine. Furthermore, implementing innovative solutions in HEI information systems requires the involvement of stakeholders, including the private sector, through public-private partnerships, which are regulated by the Law of Ukraine "On Public-Private Partnership". In the long term, it is also important to expand the integration of international experience by participating in European Union programmes (such as Horizon Europe) to expand information resource management practices in general and within the educational environment.

4. TRENDS IN INFORMATION SECURITY IN HIGHER EDUCATION

In the context of full-scale armed aggression, ensuring information security is particularly important for all state structures and sectors of the economy, particularly given the parallel escalation of Russia's cyber war

against Ukrainian information systems. Systematic acts of cyberterrorism are one of the key components of hybrid warfare, which is aimed primarily at destabilising key government areas. According to the government's computer emergency response team CERT-UA, 347 cyberattacks on government organisations, 276 on local authorities, and 175 on security and defence organisations were recorded in 2023. At the same time, educational institutions were the targets of 38 attacks, which indicates the specific interest of the aggressor country's special services in destabilising this sector, as such attacks disrupt the normal functioning of educational institutions, posing threats to participants in the educational process [21]. Moreover, according to the SCPS [22], 1105 cyber incidents were recorded and processed directly by security analysts, which is 62.5% higher than in 2022.

The study of information security trends in higher education primarily involves analysing changes in indicators such as response to cyber incidents, analysis of cyber threats to HEIs, professional development of teachers and student awareness of cybersecurity, protection of personal data of participants in the educational process and digital services used in educational institutions. International experience suggests that it is important to consider these trends in higher education. A study in the United States by Berry [33] shows that financial support is needed to overcome barriers to cybersecurity education, especially for college students who are often unaware of the risks they face online. In contrast, the Singaporean researchers Katuk et al. [34] noted the effectiveness of a program for college students focused on malware prevention strategies, which led to a marked improvement in students' knowledge and responsible online behaviour. Table 1 presents the data of the defined criteria that collectively characterise the current state and trends in the development of information security of Ukrainian higher education institutions in 2020-2023.

Table 1. Information security indicators of higher education institutions in Ukraine.

Information security indicators of higher education institutions	Period			
	2020	2021	2022	2023
Cyber incidents response	0.64	0.67	0.67	0.67
Cyber threat analysis and information	0.67	0.8	0.8	0.2
Education and professional development	0.6	0.89	0.89	0.89
E-identification and trust services	0.75	1	0.89	0.78
Protection of digital services	0.75	0.2	0.2	0.2
Protection of personal data	1	1	1	1

Source: NCSI [23]

According to the NCSI report (2024), Ukraine's cybersecurity system ranks 13th (80.83) in the global ranking, showing a significant improvement since 2020 (75.32). The high position in the global rankings is mainly due to the increase in the level of e-participation (in 2024, 1st place in the ranking), the development of electronic online services (in 2024, 5th place in the ranking) and digitalization in general (in 2024, 30th place in the ranking), which also has a positive impact on the state of modern education and the quality of the educational process in Ukraine [24].

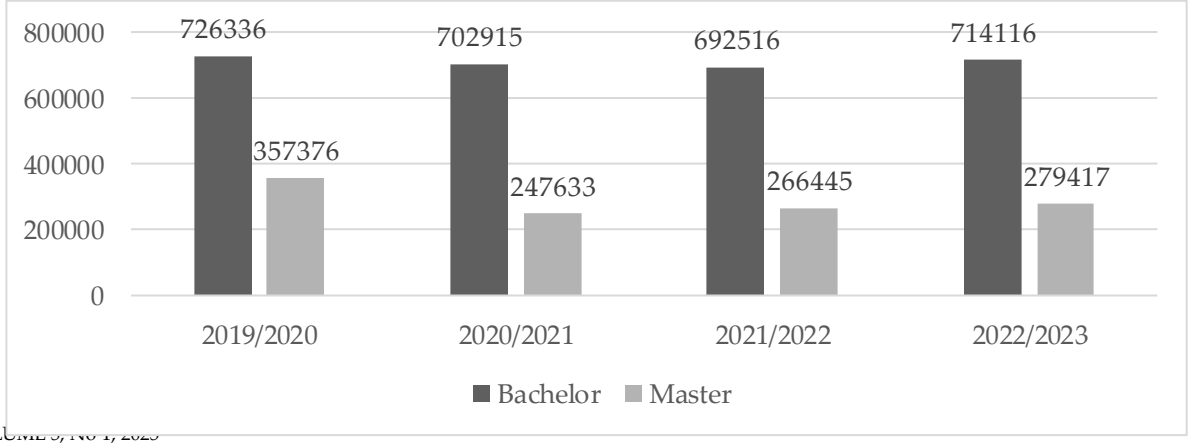

FIGURE 2. Distribution of the number of students in Ukrainian educational institutions. Source: Ukrstat [25]

Even though widespread digital transformation has dramatically facilitated the continuity and quality of the educational process in Ukrainian HEIs during the COVID-19 pandemic and the subsequent full-scale Russian invasion of Ukraine, the number of students has decreased significantly (Figure 2), in particular, in the 2020-2021 academic year, the number of bachelor's and master's students decreased by 3.24% and 30.71%, respectively, and further moderate declines or relative increases are observed.

Given the stable downward trend in the number of students in Ukrainian higher education institutions, it is reasonable to assume that such dynamics can directly and indirectly impact the state of information security in higher education in Ukraine. Changes in the number and structure of students affect the cost structure and the need to attract resources available to ensure university information security. Therefore, a decrease in their number may lead to budget optimisation, affecting the quality of technological and human support for information system security. With limited resources, higher education institutions can refocus their efforts on meeting students' basic needs, reducing attention to secondary aspects of security. The results of the correlation analysis substantiated the interaction of demographic changes with the level of information security in the context of current priorities of higher education institutions. The results of the correlation analysis between the number of students and information security indicators of higher educational institutions in Ukraine are presented in Table 2.

Table 2. Correlation analysis between the number of students and information security indicators of higher education institutions in Ukraine.

Correlation			
Pearson's Correlations			
Variable		**Bachelor**	**Master**
Cyber incidents response (I1)	Pearson's r	-0.795	-0.963
	p-value	0.898	0.981
Cyber threat analysis and information (I2)	Pearson's r	-0.430	-0.099
	p-value	0.715	0.549
Education and professional development (I3)	Pearson's r	-0.795	-0.963
	p-value	0.898	0.981
E-identification and trust services (I4)	Pearson's r	-0.737	-0.804
	p-value	0.868	0.902
Protection of digital services (I5)	Pearson's r	0.795	0.963
	p-value	0.102	0.019

Source: compiled by the author

The reduction in student population caused by the war reduces the overall burden on the information infrastructure of universities, which is reflected in the negative correlation between the number of undergraduate and graduate students and I1 (B = -0.795; M = -0.963). However, the lower concentration of students in the system may contribute to better protection of digital services through a focus on quality, which confirms the initial assumption of the analysis by the presence of a positive correlation with I5 (B = 0.795; M = 0.963). The decline in student numbers may lead to a decreased strain on universities' information systems, allowing for more focused investments in cybersecurity. However, this effect is complex and depends on the institution's ability to allocate resources effectively amidst demographic shifts. Thus, the decline in the number of students has an ambivalent impact on the information security of HEIs, confirming the need to develop adaptive information security strategies that consider demographic challenges and the growing dependence of education on digital technologies.

Given the declining number of students, the overall burden on the information infrastructure, and the challenges associated with ensuring cybersecurity in higher education, there is a need for additional research, notably on changes in the education index in Ukraine. The rates of change in the education index are shown in Figure 3; however, due to the lack of current data for 2023, they were forecasted using the "FORECAST.ETS" function of the Excel analysis package. Factors that have a potential impact on the Education Index include the level of access to quality education, including regional barriers, gender and other inequalities in the education system; the current economic situation of the country, including sufficient capital investment in educational infrastructure, adequate teacher training, and student resources. The rate of change of the Education Index in Ukraine indicates the uneven impact of external and internal factors on the development of the education system. Despite the increase in the Education Index in 2021 due to the increased digitalization of the Ukrainian education system as a result of the COVID-19 pandemic, which contributed to the introduction of modern technologies in the educational process due to the outbreak of a full-scale invasion in 2022-2023, regional inequalities in access to quality education increased, funding for educational infrastructure decreased, and additional challenges to cybersecurity and adaptation of the educational process to new conditions emerged.

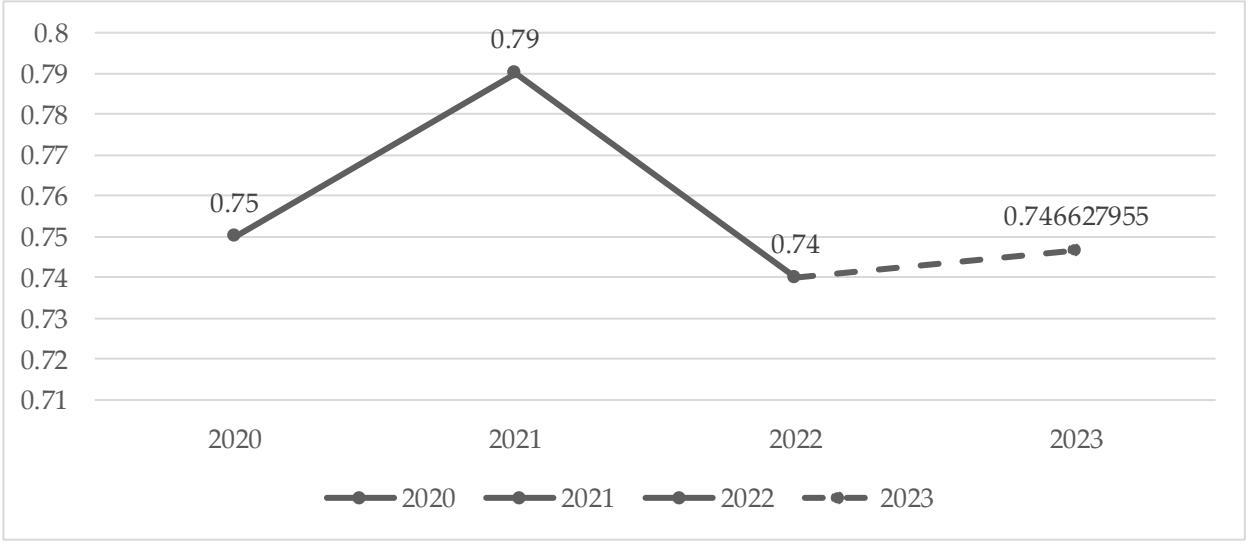

FIGURE 3. The rate of change of the education index in Ukraine.
Source: World Population Review [26]
Note: data calculated by the author are in italics

An analysis of the relationship between changes in the education index and information security will allow us to determine whether a decrease in the education index affects the vulnerability of information systems of higher education institutions, assess the effectiveness of current security strategies and infrastructure, and assess their compliance with current challenges. The results of the correlation analysis were obtained using the "CORREL" function in the Excel statistical software. The variables in the correlation analysis, such as the number of students and the education index, were measured through standard indicators reflecting institutional data, such as student enrolment numbers and specific information security metrics like cyber incident response and digital service protection. The correlation analysis presented in Table 3 was carried out to identify the relationships between the education index and information security indicators of higher education institutions in Ukraine.

Table 3. Correlation analysis between the education index and information security indicators of higher education institutions in Ukraine.

	Correlation *Pearson's Correlations*	
Variable		**Education Index**
Cyber incidents response (I1)	Pearson's r	0.196254275
	p-value	< 0.05
Cyber threat analysis and information (I2)	Pearson's r	0.355986406
	p-value	< 0.05
Education and professional development (I3)	Pearson's r	0.196254275
	p-value	< 0.05
E-identification and trust services (I4)	Pearson's r	0.738232478
	p-value	< 0.05
Protection of digital services (I5)	Pearson's r	-0.196254275
	p-value	< 0.05

Source: compiled by the author

The high positive correlation between the education index and the introduction of electronic identification and trust services (r = 0.738) highlights the effectiveness of digital technologies in improving the quality of the educational environment and promoting security and trust in using electronic services. This confirms the central argument of the article about the importance of integrating the latest digital technologies into the educational process to ensure a greater level of security. At the same time, the negative correlation between the Education Index and the protection of digital services (r = -0.196) characterises the impact of the lack of development of digital educational infrastructure, which limits the ability to integrate comprehensive measures and leads to changes in the structure of cybersecurity in higher education institutions. Thus, a high level of education may not always correlate with effective protection of digital services, which is an important aspect for further research and improvement of digital infrastructure in education. The resulting correlation corroborates the central premise of the article, namely, that the advancement of technological advancements contributes to the protection of digital resources in educational establishments, while also highlighting the need to enhance infrastructure to ensure more effective safeguarding of digital assets.

V. DISCUSSION

Nashynets-Naumova [13] notes that modern HEIs have a clear strategy for developing information technology, standard requirements for information infrastructure, information security policy and approved regulations, but differ in their administrative core and different operating environments. Such differences are due to organisational, technical or economic reasons and require appropriate government regulation to implement uniform information security standards. It is worth noting that Bielai and Sporyshev [14] propose to create a single standard of protection against cyberattacks, which will also cover the protection of intellectual property and ensure the confidentiality of the data of participants in the educational process. This approach is relevant because our study also proposes a comprehensive approach to forming a nationwide system of protecting higher education institutions from cyberattacks. Our work also proposes the creation of special coordination centres based on higher education institutions to exchange information and experience between educational institutions, the Ministry of Digital Transformation and the State Service for Special Communications and Information Protection of Ukraine, as well as to implement measures to stimulate science and education in the field of information security, which echoes the findings of Nahaichuk et al. [3] and Piatnychuk [17]. Some authors, such as Koshovyi

[18], Kotsur et al. [19], and Nehodchenko [20], consider it expedient to continue the course of Ukraine's European integration, which also includes the adaptation of existing data protection regulations to the conditions of martial law and post-war reconstruction, as noted in our paper.

Existing research often analyses demographic change [9], national policy [28] and cybersecurity [29] in higher education separately, but does not sufficiently integrate these factors in the context of current crisis situations such as war and global digital transformation. Malik et al. [29] point out that the digitalization of higher education has resulted in increased vulnerability, as private information is a prime target for online assaults; as a result, institutions must implement robust cybersecurity protocols, including encryption and user education, to safeguard academic data networks. Hence, it is imperative to establish national cybersecurity policies to safeguard educational institutions from cyber threats, while also aligning with international norms to foster a culture of compliance [28]. Policies like India's National Education Policy (NEP) of 2020 aim to improve quality and accessibility in higher education through structural reforms and technology integration [30]. Similarly, the European Union has implemented frameworks like the General Data Protection Regulation (GDPR), which imposes strict data protection standards that directly affect educational institutions across member states [31], [32]. In Ukraine, the ongoing efforts of the government regarding digitization within the framework of the national education development strategy emphasize the need to strengthen cybersecurity in the education sector [33].

Horta [9] notes that reducing the number of students can lead to budget optimisation, affecting the quality of technological and human resources support for information systems security. However, our study indicates that in times of war, the reorganisation of the state budget is primarily focused on the military aspect, so a reduction in the number of students does not have a significant impact on the quality of information system security support, in particular, the correlation of this factor with Cyber threat analysis and information ($B = 0.795$ at $p = 0.102$; $M = 0.963$ at $p = 0.019$) is not statistically significant. Although the estimates provide useful information about the relationship between demographic factors and information security, their ability to fully capture the complexity of these issues may be limited if they rely solely on quantitative indicators without considering the deeper contextual and qualitative factors that influence the security environment in higher education institutions. In future studies, the utilization of a broader array of indicators that encompass diverse aspects of information security, including technical, organizational, and regulatory aspects, may yield a more comprehensive comprehension of the challenges and opportunities in this domain. However, the negative correlation between Cyber incidents response and Education and professional development ($B = -0.795$ at $p = 0.898$; $M = -0.963$ at $p = 0.981$) echoes the findings of Adeyemo [27] regarding the possibility of refocusing attention on ensuring quality information security in a resource-limited environment by reducing student enrolment. Additionally, the conclusions of Alhadidi et al. [5] regarding the potential for more effective measures to protect digital services due to a reduced concentration of students are corroborated by the positive correlation with the Protection of digital services ($B = -0.43$ at $p = -0.099$; $M = 0.715$ at $p = 0.549$) found in our analysis.

VI. CONCLUSION

The current state and effectiveness of the state policy of information security for the development of higher education is characterised by imperfections in the regulatory framework for the specific needs of higher education institutions, such as the protection of research data, confidential information of participants in the educational process, and ensuring the smooth functioning of digital platforms during cyberattacks. In the post-pandemic period and the context of full-scale armed aggression, the lack of adequate protection of information systems makes it challenging to ensure the quality of education, and the number of cyberattacks by Russia is increasing significantly. An additional negative factor is a significant decrease in the number of students in all forms of education. The study found that the decline in the number of students in the post-pandemic and wartime periods did not directly contribute to the reallocation of resources in favour of improving information security, given the need to increase public defence spending. However, it has contributed to reducing the number of incidents unrelated to cyber

warfare and increased the effectiveness of protecting digital services by concentrating resources. Limited funding and demographic changes pose risks to providing technological support to higher education institutions, which reduces the ability to innovate their information and data protection systems.

Recommendations for improving the state information security policy include the introduction of unified standards for cyber defence, intellectual property protection and data confidentiality with a focus on developing specialised legislation to take into account the specifics of educational institutions; stimulating science and education in the area of information security, in particular through funding for relevant specialities; creating focal points for information exchange between educational institutions, government agencies and the private sector. The contribution of the study is that it confirms the link between reducing student concentration and improving the security of digital services, which allows for the implementation of more effective security measures in the educational environment and digital technologies. The results of the study can be useful for practitioners in improving security measures in the digital sphere, focusing on reducing student concentration. Policymakers, in turn, should support strategies that reduce risks to digital services and promote effective governance in this area.

Funding Statement

This research received no external funding.

Author Contributions

The author, Viktor Paliukh, was solely responsible for this manuscript's conceptualization, design, analysis, editing and writing. The author, Iryna Kovtun, was solely responsible for this manuscript's conception, design, data collection, analysis, editing and writing. The author, Tetiana Pidlisna, was solely responsible for this manuscript's conception, design, data collection, methodology, analysis, software, editing and writing. The author, Tatyana Tatarnikova, was solely responsible for this manuscript's design, formal analysis, data collection, analysis, editing and writing. The author, Stanislav Poroka, was solely responsible for this manuscript's conception, methodology, project management, supervision, editing and writing.

Conflict of Interest

The author declares no conflict of interest.

Data Availability Statement

Data are available from the author upon request.

Acknowledgements

The author would like to thank colleagues for their assistance in collecting the data that formed the basis of this research. Special thanks are also extended to the Qubahan Academic Journal for their help in preparing and refining this article.

REFERENCES

1. Ogborigbo, J. C., Sobowale, O. S., Amienwalen, E. I., Owoade, Y., Samson, A. T., Egerson, J., & Owoade, Y. (**2024**). Strategic integration of cyber security in business intelligence systems for data protection and competitive advantage. *World Journal of Advanced Research and Reviews, 23*(1), 81–96.
2. Admass, W. S., Munaye, Y. Y., & Diro, A. A. (**2024**). Cyber security: State of the art, challenges and future directions. *Cyber Security and Applications, 2*, 100031.
3. Nahaichuk, O. V., Kyrchata, I. M., & Holodiuk, H. I. (**2024**). Partnership between higher education institutions and government structures in the field of security: Assessing the impact on educational processes. *Pedagogical Academy: Scientific Notes, 9*, 1–25.
4. Chystokletov, L., & Obrembalskyi, S. (**2024**). Peculiarities of ensuring information security in the conditions of the Russian-Ukrainian war. *Academic Visions, 29*, 1–11.
5. Alhadidi, I., Nweiran, A., & Hilal, G. (**2024**). The influence of cybercrime and legal awareness on the behaviour of university of Jordan students. *Heliyon, 10*(12), e32371.

6. Chang, K., & Huang, H. (**2023**). Exploring the management of multi-sectoral cybersecurity information-sharing networks. *Government Information Quarterly, 40*(4), 101870.
7. Odebade, A. T., & Benkhelifa, E. (**2023**). A comparative study of national cyber security strategies of ten nations. *arXiv preprint arXiv:2303.13938*.
8. Poliakova, Yu., Stepanov, A., & Dubil, T. (**2024**). Innovative approaches to the formation and implementation of intersectoral cooperation. *Economy and Society, 60*, 1–10.
9. Horta, H. (**2023**). Emerging and near future challenges of higher education in East Asia. *Asian Economic Policy Review, 18*(2), 171–191.
10. Jafari, F., & Keykha, A. (**2024**). Identifying the opportunities and challenges of artificial intelligence in higher education: A qualitative study. *Journal of Applied Research in Higher Education, 16*(4), 1228–1245.
11. Shi, L., & Yonezawa, A. (**2023**). The changing roles of university education in the age of innovation: Implications from China and Japan. In *Student and skilled labour mobility in the Asia Pacific region: Reflecting the emerging fourth industrial revolution* (pp. 23–48). Springer International Publishing.
12. Yang, J. (**2023**). The impact of Industry 4.0 on the world of work and the call for educational reform. In *The frontier of education reform and development in China: Articles from educational research* (pp. 285–298). Springer Nature Singapore.
13. Nashynets-Naumova, A. Yu. (**2020**). Legal provision of information security in higher educational institutions of Ukraine. In *Modern achievements of EU countries and Ukraine in the field of law* (pp. 376–388). Izdevniecība "Baltija Publishing".
14. Bielai, S., & Sporyshev, K. (**2024**). Influence of the state of the system of information and analytical support of the security forces of Ukraine on state security. *Scientific Innovations and Advanced Technologies, 2*(30), 29–37.
15. Weng, Y., & Wu, J. (**2024**). Fortifying the global data fortress: A multidimensional examination of cyber security indices and data protection measures across 193 nations. *International Journal of Frontiers in Engineering Technology, 6*(2), 13–28.
16. Tkachuk, T. Yu. (**2018**). Priority directions of state policy for ensuring information security at the current stage of state formation. *Scientific Bulletin of Kherson State University. Series: Legal Sciences, 4*(2), 32–35.
17. Piatnychuk, I. D. (**2024**). Regulatory and legal mechanisms of public management of information security protection processes in the field of electronic services. *Scientific Perspectives. Series: State Administration, 4*(46), 361–370.
18. Koshovyi, B.-P. O. (**2023**). Method of nationalisation of state socio-economic policy to achieve intellectual security of the nation. *Scientific Notes of Lviv University of Business and Law, 39*, 600–608.
19. Kotsur, V., Kotsur, L., & Hryha, O. (**2023**). Main directions of implementation of state information policy of Ukraine in the conditions of martial law: Challenges and tasks. *Public Administration: Concepts, Paradigm, Development, Improvement, 6*, 90–103.
20. Nehodchenko, V. (**2016**). Main directions of state information policy in Ukraine. *Information Law, 4*, 77–81.
21. Word and Deed. (**2024**). *The number of cyberattacks in Ukraine over the past year*. IA Word and Deed.
22. SCPS. (**2024**). *Vulnerability detection and response systems for cyber incidents and cyber attacks in 2023: Statistical report on the results of the work*. The State Cyber Protection Centre of Ukraine.
23. NCSI. (**2024**). *NCSI fulfilment percentage: Ukraine*. National Cyber Security Index.
24. United Nations. (**2024**). *UN e-government survey 2024*. UN E-Government Knowledgebase.
25. Ukrstat. (**2023**). *Higher and professional pre-higher education in Ukraine*. State Statistics Service of Ukraine.
26. World Population Review. (**2024**). *Education index by country 2024*. World Population Review.
27. Adeyemo, K. S. (**2023**). The status of digital innovation and data security in South African higher education. *South African Journal of Higher Education, 37*(2), 26–39.
28. Fowler, B. (**2024**). Cybersecurity leadership policy and compliance for institutions of higher education. *World Journal of Advanced Engineering Technology and Sciences, 12*(2), 553–563.
29. Malik, A. F., Soesanto, E., & Hamidah, N. (**2024**). Implementasi nilai-nilai kebangsaan berbasis UUD 1945 guna mendukung sistem cyber security dalam penggunaan sistem informasi akademik (SIA) di institusi perguruan tinggi. *MENAWAN: Jurnal Riset dan Publikasi Ilmu Ekonomi, 2*(3), 235–249.
30. Modi, T. B. (**2023**). The impact of the national education policy on higher education in India. *Research Review Journal of Social Science, 3*(2), 8–14.
31. Mohammad, A., & Vargas, S. (**2022**). Barriers affecting higher education institutions' adoption of blockchain technology: A qualitative study. *Informatics, 9*(3), 64.
32. Pryhodii, M. A. (**2024**). Legislative support for the digital transformation of vocational education. In *Innovative vocational education: Modernization of educational programs for training higher education applicants in the context of global and national challenges* (pp. 53–60).
33. Berry, H. S. (**2023**). Survey of the challenges and solutions in cybersecurity awareness among college students. In *2023 11th International Symposium on Digital Forensics and Security (ISDFS)* (pp. 1–6).
34. Katuk, N., Zaimy, N. A., Krishnan, S., Kunhiraman, R. K., Lee, H.-H., & Eleyan, D. (**2024**). Fostering cyber-resilience in higher education: A pilot evaluation of a malware awareness program for college students (pp. 154–167).