

DOI: <https://doi.org/10.46502/issn.1856-7576/2025.19.02.3>

Cómo citar:


Zybin, S., Bondarchuk, O., Piroh, O., Suprun, O., & Kyshakevych, S. (2025). Cybersecurity on Ukrainian Higher Education: Threats and protection measures. *Revista Eduweb*, 19(2), 38-52. <https://doi.org/10.46502/issn.1856-7576/2025.19.02.3>

# Cybersecurity on Ukrainian Higher Education: Threats and protection measures

## Ciberseguridad en la Educación Superior Ucraniana: Amenazas y medidas de protección


**Serhii Zybin**

D.Sc. Professor, Department of Technical Information Protection, Faculty of Computer Science and Technology, National Aviation University, Ukraine.

 <https://orcid.org/0000-0002-2670-2823>  
[zysv@ukr.net](mailto:zysv@ukr.net)


**Oleg Bondarchuk**

M.Sc. DevOps Engineer, Stealthmail Ukraine LLC, Ukraine.

 <https://orcid.org/0009-0003-9626-1124>  
[iperaser@gmail.com](mailto:iperaser@gmail.com)


**Oleksandr Piroh**

PhD Department of Computer Engineering and Cyber Security, Faculty of Information and Computer Technologies, Zhytomyr Polytechnic State University, Ukraine.

 <https://orcid.org/0009-0001-6111-9676>  
[pirogov@ztu.edu.ua](mailto:pirogov@ztu.edu.ua)


**Olha Suprun**

PhD Associate Professor, Department of Theory and Technology of Programming, Faculty of Computer Science and Cybernetics, Taras Shevchenko National University of Kyiv, Ukraine.

 <https://orcid.org/0000-0002-1196-5655>  
[o.n.suprunso@gmail.com](mailto:o.n.suprunso@gmail.com)

**Svitlana Kyshakevych**

PhD Associate Professor, Department of Vocal and Choral, Choreographic and Fine Arts, Faculty of Primary Education and Arts, Ivan Franko State Pedagogical University of Drohobych, Ukraine.

 <https://orcid.org/0000-0003-4696-4764>  
[duvo\\_svit@ukr.net](mailto:duvo_svit@ukr.net)

Recibido: 01/04/25

Aceptado: 15/05/25

### Abstract

The purpose of the study is to analyse the impact of cybersecurity on higher education in Ukraine, identify key threats and formulate key recommendations for improving the security of educational institutions. For this purpose, a cross-sectional survey study has been chosen. A purposive sample has been used to include participants. 79 questionnaires have been received; five have been rejected, and three more have refused to consent to data processing. The study involved 71 people, including 15 administrative staff (IT departments, managers), 30 teachers, and 26 students. The primary tool in the study has been a cross-sectional questionnaire survey conducted in the same period for all participants from 11/20/2024 -



12/20/2024. The results indicate that the main cybersecurity threats in Ukrainian educational institutions are viruses and malware (39,4%), hacking of university platform accounts (26,8%), phishing attacks (14,1%), and personal data leakage (12,7%). The results also have showed that 49,3% of respondents are moderately aware of cybersecurity measures at the university, while 28,2% are poorly aware. The conclusions summarise that to ensure cybersecurity further, it is necessary to expand multi-level protection systems, control the use of the Internet, and conduct additional training for students and teachers in cybersecurity.

**Keywords:** Cyber hygiene, intellectual property protection, national strategy, technology, privacy policy.

## Resumen

El objetivo del estudio es analizar el impacto de la ciberseguridad en la educación superior en Ucrania, identificar las principales amenazas y formular recomendaciones clave para mejorar la seguridad de las instituciones educativas. Para ello, se optó por un estudio de encuesta transversal. Se utilizó una muestra intencionada para incluir a los participantes. En el estudio participaron 71 personas, entre ellas 15 miembros del personal administrativo (departamentos informáticos, directivos), 30 profesores y 26 estudiantes. La herramienta principal del estudio fue una encuesta transversal por cuestionario realizada en el mismo periodo para todos los participantes: del 20.11.2024 al 20.12.2024. Los resultados indican que las principales amenazas a la ciberseguridad en las instituciones educativas ucranianas son los virus y el malware (39,4%), el pirateo de cuentas de la plataforma universitaria (26,8%), los ataques de phishing (14,1%) y la filtración de datos personales (12,7%). Los resultados también mostraron que el 49,3% de los encuestados tiene un conocimiento moderado de las medidas de ciberseguridad en la universidad, mientras que el 28,2% tiene un conocimiento escaso. Las conclusiones concluyen que, para garantizar aún más la ciberseguridad, es necesario ampliar los sistemas de protección multinivel, controlar el uso de Internet y proporcionar formación adicional a estudiantes y profesores sobre los fundamentos de la ciberseguridad.

**Palabras clave:** Protección de la propiedad intelectual, tecnología, política de privacidad, ciber higiene, estrategia nacional.

## Introduction

Digital technologies play an essential role in higher education and contribute to the development of the educational process, research and university administration. However, despite the numerous opportunities identified in scientific studies (accessibility of education, speed, convenience of obtaining educational information), the digitalisation of education also creates new challenges (Korhonen et al., 2021).

The field of cybersecurity is particularly affected. The growth of cyber threats, including hacker attacks, data breaches, phishing attacks, and malware, threatens the confidentiality of student and teacher data, the stability of educational platforms, and trust in the digital learning environment. In addition, Ukraine, which is currently in a state of hybrid war, faces significant risks in cyberspace, which is especially relevant for higher education and science.

Scientific works indicate that attacks on educational institutions lead to disruptions in the educational process and compromise research and academic integrity violations (Melenti et al., 2024; Nehrey et al., 2022). Therefore, this scientific problem is particularly relevant in the modern scientific space and requires careful analysis. In this regard, there is a need to analyse the main cyber threats and develop effective measures to protect the information space of Ukrainian universities.

The main research problem is the growing vulnerability of Ukrainian higher education to cyber threats due to insufficient security of digital platforms, lack of a comprehensive cyber defence strategy, and limited awareness of safe online behaviour among participants in the educational process. In addition, the lack of



effective mechanisms for responding to cyberattacks can lead to the leakage of confidential information, disruptions in the learning process, and undermine trust in the digital learning environment.

The focus of this paper is to provide a detailed analysis of the leading cyber threats affecting higher education in Ukraine and assess the effectiveness of existing protection measures. This will be done through a comprehensive survey of all participants in the educational process: teachers, students, and administration. The paper will address such aspects as the vulnerability of educational platforms to attacks, the level of digital literacy of teachers and students, and the state policy of cyber defence in times of war.

Therefore, the purpose of this study is to assess the impact of cybersecurity on higher education in Ukraine, identify key threats, and formulate key recommendations for improving the security of educational institutions. Accordingly, the main research questions are as follows:

1. What are the most common cyber threats in higher education?
2. What is the level of educational process participants' awareness of ensuring an adequate digital space?
3. What recommendations can be offered to improve cybersecurity in higher education?

The main research hypotheses that need to be confirmed or refuted:

1. Modern higher education institutions implementing systemic cybersecurity measures (multi-level authentication and regular system updates) have a significantly lower cyber threat.
2. The higher the level of digital competence of faculty and students, the lower the risk of cyberattacks on university learning systems.

The structure of this article is formed as follows: a review of the literature, which presents an analysis of existing modern works, methodology, which explains the procedure of data collection and analysis, results, which present the impact of the main cyber threats on the development of the education system, discussions, which describe the key discussions of the results and their comparison with other works. The last section is conclusion, which briefly describes the main identified cyber threats and their impact on the development of education.

## Literature Review

### Theoretical foundations for the formation of cybersecurity in an educational institution

Modern scholars have described various aspects of the impact of cybersecurity on the organisation of the educational process. According to several modern studies, the use of digital technologies has sharply intensified in recent years and decades in almost all countries and has covered all areas of activity (AIDaajeh et al., 2022; Blažič, 2021).

Despite the identified numerous advantages (accessibility and efficiency) of obtaining information, the use of digital technologies also poses specific threats, in particular, the complexity of data protection for individuals, firms, authorities, and societies in general (Terepyshchy & Kostenko, 2022). Recent studies have shown that the development of an effective cybersecurity system in education should be based on systemic and interdisciplinary approaches that synthesise technical, organisational, and legal aspects (Horlynskyi & Horlynskyi, 2019; Lakhno et al., 2024; Zabasta et al., 2020).

Cybersecurity research points to the importance of formulating a cybersecurity strategy for an educational institution, which should include access policies, monitoring of network activity, and data backup (AIDaajeh et al., 2022). The works of some scientists point to the importance of using a concept called "Zero Trust Security". The latter implies constantly checking all users and technical devices in the learning environment (Haque et al., 2023).

At the same time, not all researchers support this idea. In particular, other works describe that international cybersecurity standards such as ISO/IEC 27001 are recognised and effective in protecting educational institutions. Zhyvko et al. (2020) describe the main legal conditions for ensuring effective regulation of cyberspace. On the other hand, some scholars point out the critical role of public policy in the cybersecurity system, in particular, educational institutions must comply with GDPR data security standards, which are fully recognised in the European Union (Zhyvko et al., 2020; Potii et al., 2015).

### Opportunities and threats in the digital learning space

The works of scientists indicate that forming a digital learning space opens up many advantages related to the accessibility of learning and the speed of knowledge acquisition (Bohomaz et al., 2023; Bingham, 2024). Other scholars also point to such advantages as the introduction of new methods and forms of learning that promote greater student engagement and increase their level of motivation.

In addition, according to Khan et al. (2022), the digital learning environment opens up new opportunities for distance and blended learning. Scientists point out that platforms such as Moodle, Google Classroom, and Microsoft Teams facilitate interactive learning and effective collaboration between students and teachers (Korhonen et al., 2021).

Devadze & Gechbaia (2024) found that virtual reality can increase students' learning motivation. However, despite several advantages, some challenges have also been identified in scientific research. In particular, the authors point to the threat of cyberattacks on educational institutions.

Modern universities are becoming targets for hackers because they store confidential data of employees and students. In addition, several works point to the problem of phishing attacks (Ulven & Wangen, 2021). These authors summarised that students' and teachers' lack of security awareness makes them vulnerable to fraudulent schemes, including in the digital learning space.

It is also worth paying attention to hacking and data leakage, as shown in the research of Sullivan & Kamensky (2017). In particular, these researchers determined that the lack of two-factor authentication contributes to the compromise of learning platform accounts (Guchua & Zedelashvili, 2023; Kharlamova et al., 2022).

On the other hand, scientists have drawn attention to the global problem of artificial intelligence and deep fakes, which have begun to be actively used in education. However, the widespread use of generative AI technologies can lead to information manipulation and affect academic integrity.

### Key cybersecurity measures

According to modern works, ensuring Ukraine's cybersecurity is a state of protection for the interests of a person, society, and the state in cyberspace should be achieved through several legal, organisational, and informational measures. The latter should also be based on the effective organisation of professional training of cybersecurity management specialists.

Cheng & Wang (2022) state that to protect information from unwanted interference, cybersecurity measures are implemented, which should be understood as systemic actions of a technological, organisational, economic, and legal nature. These measures should be designed to be purposefully carried out to identify and destroy cyber threats (Galushchenko et al., 2024; Guo, 2023).

Most studies point to the need to introduce innovative approaches to cybersecurity in educational institutions. In particular, the works consider such a measure as cybersecurity policy development (Melenti et al., 2024; Bobro et al., 2024). According to Dei et al. (2024), forming internal security standards governing access to resources and data storage plays an important role. However, not all scholars agree with this statement.

There are arguments that these measures are not enough. Thus, other authors point out that technical security measures should be considered, and continuous monitoring should be conducted (Melenti et al., 2024; Nehrey et al., 2022). Some authors emphasise increasing digital literacy among students and teachers (Kuzminykh et al., 2021).

The study by Buriachok et al. (2023) describes the main aspects of introducing cybersecurity education, which is currently a relevant area. Zhao et al. (2021) also describe the main complex and key conditions for forming digital competence.

The analysed works mostly use a qualitative approach to data analysis. Also, in some works there is a rather broad overview aspect (Buriachok et al., 2023; Melenti et al., 2024). Accordingly, there is a lack of analysis of statistical and quantitative data. In some works, although there is quantitative data, the authors did not widely discuss the obtained results.

The main limitations of these studies are the increased attention to the qualitative overview type. In addition, the vast majority of works are of an overview nature. This requires additional research involving experimentation. Accordingly, the main gaps are as follows:

1. Too much attention to theoretical research.
2. There is a lack of empirical works.
3. Too many reviews.
4. Insufficient analysis of new threats that appear in modern cyberspace.

Therefore, given that there is currently no unanimous solution to define effective cybersecurity measures in scientific works, it is worth revisiting all these measures and identifying the most effective ones. This should be done by surveying all participants in the educational process. This study will fill this gap, identify the main cyber threats, and provide recommendations for their elimination.

## Methodology

### Research design

A cross-sectional survey study has been chosen for this research. This type of research allows for a survey among different categories of participants in the educational process: students, teachers, and administration. Therefore, it enables us to analyse the opinions of other people at the same time. This type has been chosen because of its advantages, including obtaining information from different people and the speed of its processing. The study has been conducted from 11/20/2024 to 12/20/2024. Location - higher education institutions of Ukraine.

### Sample and participants

A purposive sample has been used for this study. The inclusion criteria have been based on the following aspects:

1. Teaching OR studying in a higher education institution (two years of teaching experience).
2. Information security professionals working in universities.
3. Experience in protecting educational information systems.
4. Understanding cybersecurity and how it is implemented in an educational institution.
5. Professional experience in cybersecurity, information technology or administration of educational processes.
6. Persons who regularly use digital platforms for learning, management or administration in the educational environment (Moodle, Google Classroom, Microsoft Teams, etc.).
7. Location: Representatives of Ukrainian higher education institutions (public and private) who work or



- have studied in Ukraine are eligible.
8. Voluntary consent to participate.

The exclusion criteria have been also preliminarily formed:

1. Persons with no experience in the field of cybersecurity.
2. Persons with no experience in modern educational digital technologies were excluded.
3. Representatives of companies working in cybersecurity but without experience cooperating with educational institutions.

Participants have been recruited by distributing the survey announcement via corporate emails. A total of 79 questionnaires have been received. However, not all participants met the pre-established criteria.

Therefore, five questionnaires have been rejected, and three more have refused to consent to data processing. Thus, 71 people have been included in the study. The study consists of the following categories:

1. Administration (IT departments, managers);
2. Teachers (especially those who work with digital platforms);
3. Students (users of educational systems).

Table 1 provides detailed information about all participants.

**Table 1.**  
*Data of the participants.*

Nº	Category	Number (N)	%	Average age	Gender (M/F)	Work experience (years)	Use of digital platforms
1	Administration	15	21,1%	38	10/5	10	+
2	Teachers	30	42,3%	45	19/11	15	+
3	Students (users of educational systems)	26	36,6%	21	12/14	-	+
	Total	71	100%	35	42/29	12	+

*Source: Author's development*

## Instruments and procedure

The main instrument in the study was a cross-sectional questionnaire survey. It has been conducted in the same period for all participants: from 11/20/2024 to 12/20/2024.

The survey has been designed to explore the main opportunities and threats to cybersecurity in modern digital space.

The survey also focused on the mechanisms implemented in educational institutions to ensure a secure digital space and protect the data of teachers and students.

The questionnaire also contained both closed and semi-open questions. This made it possible to determine the level of awareness of participants about cybersecurity measures and their experience of facing cyber threats. Respondents filled out the questionnaire online via Google Forms. This allowed us to collect and structure responses effectively.

The questionnaire has been distributed through official university channels, such as e-mail and internal

portals, as well as professional teachers' communities. Table 2 shows the main structure of the survey.

**Table 2.**  
*Structure of the questionnaire.*

Part of the questionnaire	Key questions
1. Data	1. Please indicate your role in the higher education institution: administration, faculty, student 2. Your age 3. Your gender 4. Please indicate your experience in education (for faculty and administration) 5. Do you use digital educational platforms in your work/study?
2. Experience with cyber threats	6. Did you face any cyber threats while studying or teaching? 7. How often did this happen?
3. Basic security measures	8. How aware are you of the cybersecurity measures at your university? (on a scale from 1 to 5) 9. What measures do you consider effective? 10. Does your university have an official cybersecurity policy? (Yes or No) 11. Have you received formal cybersecurity training? (Yes or No)
4. Assessment of the effectiveness of measures	12. How would you rate the effectiveness of cybersecurity measures in the educational institution where you work or study? (on a scale from 1 to 5) 13. How secure do you feel when using university digital resources? 14. What measures should be optimised in the field of cybersecurity in universities?

*Source: Author's development*

## Data analysis

After collecting responses, the data has been processed and analysed using quantitative and qualitative analysis methods. First, all responses have been exported from Google Forms to Excel for further processing. Microsoft Excel was chosen because of its accessibility and ease of data processing.

First, the data have been cleaned to remove invalid or incomplete answers. Then, discrete variables (in particular, categories of respondents, level of awareness, and performance assessments) have been coded for further processing. Descriptive statistics were used to analyse the main trends, and frequencies have been calculated for categorical variables (for example, the frequency of encountering cyber threats).

Open questions have been subjected to thematic analysis. In particular, similar central answers have been first grouped into categories (e.g., the main cyber threats and security measures proposed by participants), and key trends have been identified. The potential of Microsoft Excel was used to present the results, particularly the diagrams of the distribution of responses.

## Validation

The questionnaire was specifically designed to assess the impact of modern approaches to resolving intergenerational conflict in education. In order to ensure content validity, the questionnaire was validated by a panel of three experts in educational psychology and conflict resolution. Their feedback led to changes in the wording and structure of the questions for better clarity and relevance.

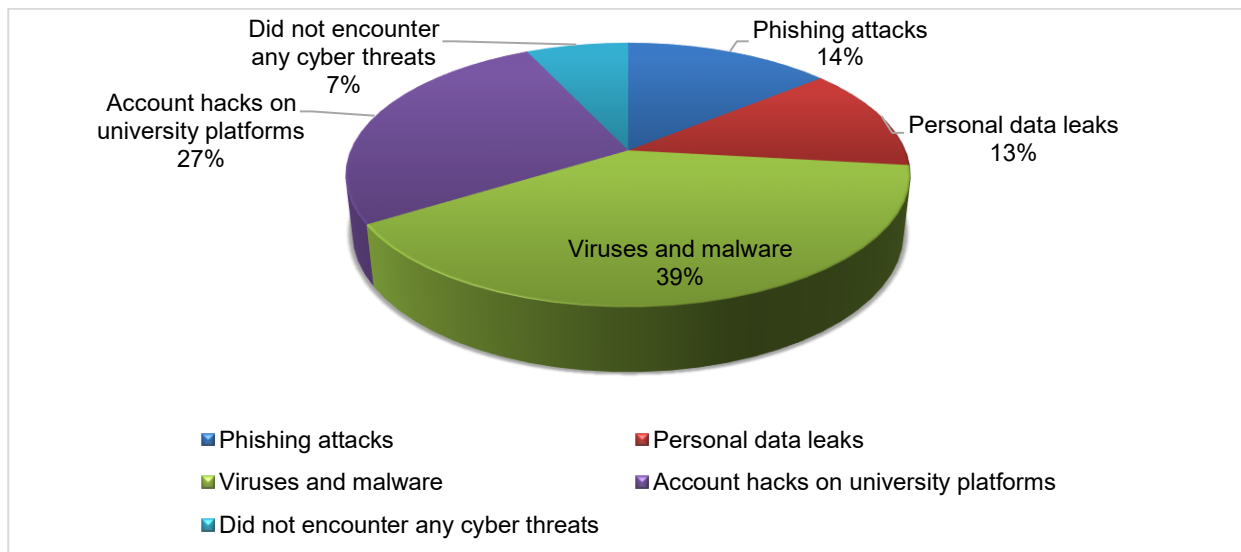
## Ethical considerations

The study adhered to ethical standards in educational research. Informed consent was obtained from all participants after they were provided with detailed information about the purpose of the study. Participation was completely voluntary and anonymous. Responses were securely stored and subsequently analysed.

## Results and Discussion

Digital technologies have increased dramatically in the Ukrainian higher education system in recent years. While implementing these technologies has some advantages (accessibility and efficiency of information), there are also some threats regarding the complexity of data protection for individuals and the entire educational institution. In particular, only 7% of respondents have not encountered cyber threats while studying or teaching.

The most common cybersecurity threats were viruses and malware (39.4%). 26.8% of cases involved hacking university platform accounts. Another 14.1% and 12.7% suffered from phishing attacks and personal data leakage. Figure 1 shows the percentage distribution of participants' responses.



**Figure 1.** Diagram of the leading cyber threats in Ukrainian universities.

Source: Author's development

The main features of cyberattacks are external manifestation, distance, speed of the crime, specificity of violation of essential characteristics, technological efficiency, automation, the expected result and the degree of complexity of the problem.

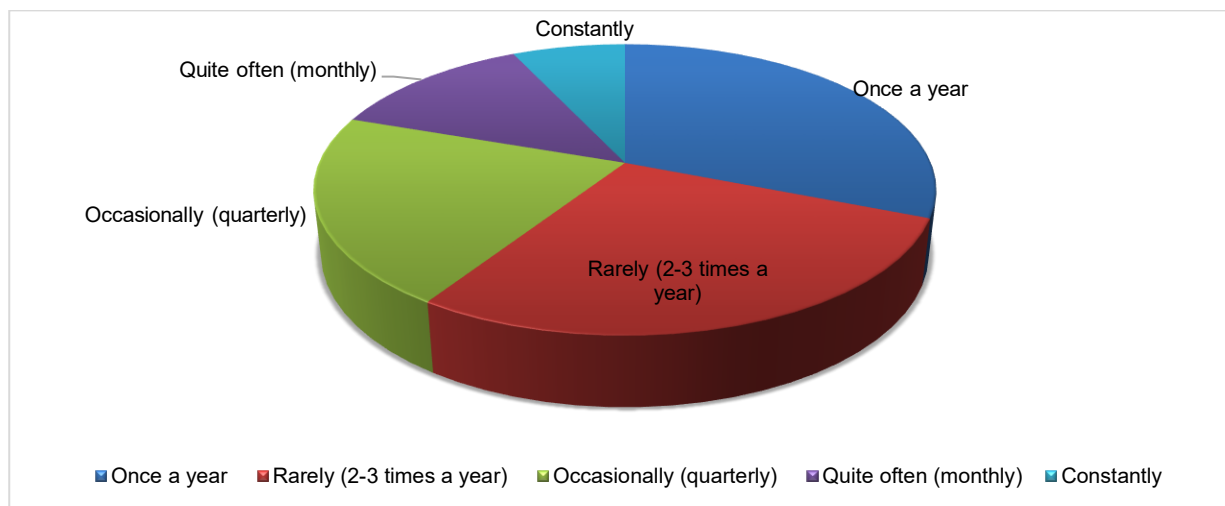
The average frequency of cyber threats (on a scale from 1 to 5) is 2.4. This generally indicates that most respondents rarely or occasionally face cyber threats. In particular, 31% face cyber threats once a year.

At the same time, 28.2% faced them 1-2 times a year (rarely). Quarterly or every few months - 21.1%. Monthly - 12.7%. Only 7% encounter it all the time while studying or teaching.

Figure 2 shows the % distribution of the frequency of cyber threats in higher education institutions in Ukraine.

To protect information from unwanted interference, cybersecurity measures should be implemented, which are understood as systemic actions of a technological, organisational and legal nature aimed at targeted detection and elimination of threats to the digital learning space. Ensuring cybersecurity requires the introduction of innovative technologies and a systematic approach. Coordinated actions at the regulatory, state and personal levels also play an essential role.

In addition, it is also worth paying attention to international assistance as a separate response to aggression in cyberspace. This is especially important if it is related to hybrid warfare.



**Figure 2.** Frequency of cyber threats.

Source: Author's development

Necessary response measures include awareness of all participants in the educational process and developing and periodically adjusting a plan to combat cyberattacks. At the same time, 49.3% of respondents indicated that they are moderately aware of cybersecurity measures at the university. At the same time, 28.2% are poorly aware.

This shows an insufficient level of cybersecurity policy in Ukrainian educational institutions. On the Likert scale, 12.7 and 4.2% of respondents indicated 4 and 5 points.

Table 3 provides detailed data on the participants' responses.

**Table 3.**

*Awareness of cybersecurity basics among survey participants.*

Score	Description	N	N %
1	Not knowledgeable at all	4	5,6%
2	Weak understanding	20	28,2%
3	Intermediate level	35	49,3%
4	Well-informed	9	12,7%
5	Very high level of awareness	3	4,2%

Source: Author's development

Combating modern cyber threats in the educational process is essential to ensuring the safety and effectiveness of learning in today's digital environment. The constant and active use of technology in education creates new challenges that require coordinated action to prevent cyber threats.

In particular, Ukraine is currently implementing measures such as developing multi-level protection systems, controlling the Internet, and training students and teachers in the basics of cybersecurity. However, it is imperative to introduce clear restrictions on access to dangerous sites or resources on the Internet, including in educational institutions, and to use software to monitor users' online activities. This will help prevent students from having access to harmful or inappropriate materials.

Data confidentiality is also essential (Newhouse et al., 2017). In particular, teachers and administrators of educational institutions should constantly monitor the protection of students' data, use appropriate encryption methods, and be aware of the rules for data protection by Ukrainian law.

However, a critical area is the development of an effective cybersecurity policy. In particular, modern higher education institutions should develop clear and effective cybersecurity policies for all participants in the educational process.

These strategies should aim to identify and eliminate threats to the digital learning space quickly. In addition, these policies should describe the rules for using digital and computer technologies, online behaviour and responding to identified cyber threat incidents. However, the survey found that not all universities have an official cybersecurity policy. However, the majority of educational institutions do have an official cybersecurity policy.

In particular, 43 respondents indicated that their university has an official cybersecurity strategy. Another 23 people said they were not aware of such a policy. Another five people noted that their institutions do not have an official cybersecurity strategy or policy.

The next question asked whether participants had received formal cybersecurity or digital competence training. Most of the participants had experience of taking digital literacy courses.

However, 34 people had received formal cybersecurity training. Given the challenges of hybrid warfare, this is a relatively low figure. This indicates a need for a more thorough approach to developing a policy for providing a digital learning space.

Table 4 details the responses of the survey participants.

**Table 4.**

*Definition of cybersecurity policy and status of formal cyber defence training.*

Questions	N	%
<b>Does your university have an official cybersecurity policy?</b>		
+ (Yes)	43	30,53%
(No) -	23	16,33%
Unknown	5	3,55%
<b>Have you received formal cybersecurity training?</b>		
+ (Yes)	31	43,66%
(No) -	26	36,62%
I am going to pass shortly	14	19,72%
<b>Have you received formal training in digital literacy?</b>		
+ (Yes)	50	70,42%
(No) -	11	15,49%
I am going to pass shortly	10	14,08%

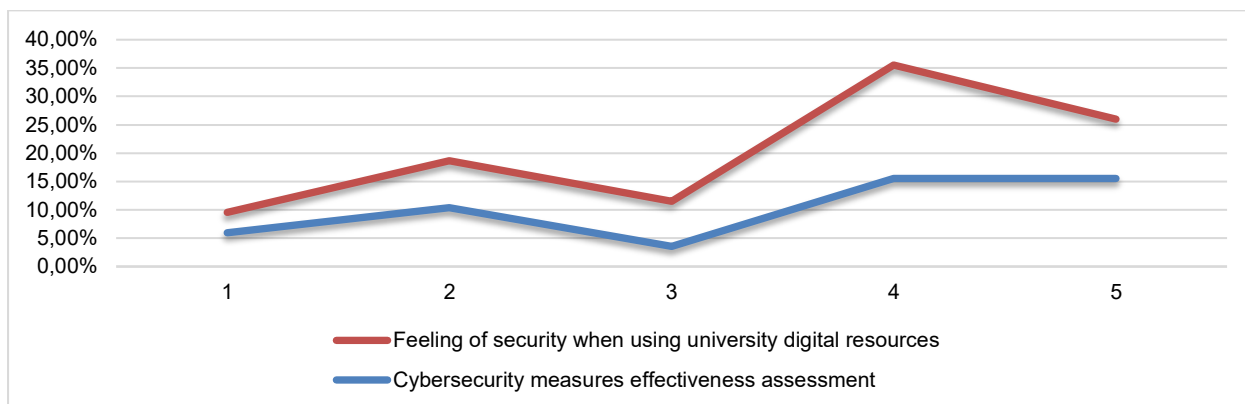
*Source: Author's development*

The analysis of the responses showed that universities where faculty members participated in digital competency training or received cybersecurity training had significantly fewer cases of cyberattacks.

In addition, professors with high cybersecurity knowledge actively teach students the key basics of online protection. This also reduces the risk of incidents. All participants in the educational process rated the effectiveness of cybersecurity measures at universities at 4 points.

Figure 3 shows the participants' assessments of the effectiveness of cybersecurity measures. In addition, most participants acknowledged feeling secure when using university digital resources (average score of 3 and 5) (see Figure 3).

Integrating two-factor authentication for students and teachers is a promising area for further development of cyberspace. Most respondents emphasised the importance of strengthening authentication at all levels of access to university digital platforms.



**Figure 3.** Assessment of the level of cybersecurity at the university.

*Source: Author's development*

Thus, introducing two-factor authentication will reduce the risk of unauthorised access. It is also essential to audit access to information systems. Monitoring all user actions on the university's digital platforms will affect the timely detection of suspicious activities and ensure a quick response to threats. On the other hand, ensuring data backup and recovery is also essential.

According to the respondents, it is necessary to have a reliable backup system to save important data. For this reason, automatic backups are crucial. In addition, ensuring it is protected from encryption in case of ransomware attacks is a key measure.

However, a significant measure is regular cybersecurity training. It is also worth conducting phishing tests to help raise awareness of the leading cyber threats and mechanisms for detecting and responding to them among all participants in the educational process.

## Discussion

Modern digital challenges require timely and thorough responses. Threats in cyberspace pose a serious problem for the functioning of higher education. This is especially true for Ukraine, where the risks of cyberattacks are incredibly high because of Russian armed aggression.

Therefore, the purpose of the proposed study is to analyse the impact of cybersecurity on higher education in Ukraine, identify key threats, and formulate key recommendations for improving the security of educational institutions. This task has involved finding answers to questions about the most widespread cyber threats in the higher education system, determining participants' level of awareness in the educational process to ensure adequate digital space, and finding recommendations for improving cybersecurity in higher education.

Additionally, the goal has been to confirm that cyber threats are much lower in modern colleges and universities that use systemic cybersecurity measures like multi-level authentication and regular system updates and that teachers and students better at using technology are less likely to be attacked online.

The proposed results show that digital technologies have increased dramatically in the Ukrainian higher education system in recent years. Accordingly, only 7% of respondents have not faced cyber threats while studying or teaching. The most common cybersecurity threat is viruses and malware (identified by 39.4%).

Hacking of university platform accounts (26.8%), phishing (14.1%), and personal information leakage (12.7%) are also common.

At the same time, most respondents rarely face cyber threats, with only 7% experiencing them constantly during their studies or teaching. The findings confirm the conclusions of other researchers regarding the extent to which digital technologies (and thus digital dangers) are integrated into modern higher education.

Other researchers believe that hacking personal student accounts is more widespread and is associated with students' low digital competence.

However, such data is not supported by empirical measurements or statistics (Bannikov et al., 2022; Cabaj et al., 2018; Muktiarni et al., 2019). Accordingly, it is difficult to support this position, as many researchers consider viruses and other malware the most significant threat. Researchers also agree that permanent cyber threats are rare.

Therefore, students behave quite cautiously in the digital environment, which does not create additional threats to their learning. Accordingly, scientists believe this reduces the workload of the technical staff of educational institutions (Crick et al., 2019). This allows us to confirm the hypothesis that the higher the level of digital competence of teachers and students, the lower the risk of cyberattacks on university learning systems.

The proposed results also show that to protect information from unwanted interference, cybersecurity measures should be implemented, which are understood as systemic actions of a technological, organisational, and legal nature aimed at targeted identification and elimination of threats to the digital learning space.

Ensuring cybersecurity requires the introduction of innovative technologies and a systematic approach. Coordinated actions at the regulatory, governmental, and personal levels also play an essential role. In addition, international assistance should also be considered as a separate response to aggression in cyberspace. At the same time, 49.3% of respondents indicated that they were moderately aware of cybersecurity measures at the university, and only 28.2% were poorly aware.

This shows an insufficient level of cybersecurity policy in Ukrainian educational institutions. This is comparable to the findings of other researchers who have dealt with this issue (Pozharytskyi et al., 2022). Other researchers who studied students' awareness of countering cyber threats concluded that the overall average indicators in this area are high (Catota et al., 2019; Politova et al., 2022).

Notably, the survey found that not all universities have an official cybersecurity policy. However, most educational institutions do have a formal cybersecurity policy. 43 people indicated that their university has a formal cybersecurity strategy. However, only 34 people have received formal cybersecurity training. Given the challenges of hybrid warfare, this is a relatively low figure. Existing research generally shows that implementing cybersecurity policies typically increases the level of countering threats (Ricci et al., 2018; Rodinova et al., 2024).

This significantly reduces the risk of information leakage, data breaches, etc. In the Ukrainian context, such approaches are only being implemented. At the same time, this allows us to confirm the hypothesis that modern higher education institutions that implement systemic cybersecurity measures have a much lower level of cyber threats. For a long time, timely software updates have been problematic in the Ukrainian context. However, as demonstrated in the proposed study, such a dependence is indeed observed.

The analysis of the responses showed that universities where teachers participated in digital competence training or received cybersecurity training had significantly fewer cases of cyberattacks. In addition, professors with high cybersecurity knowledge actively teach students the key basics of online protection. This also reduces the risk of incidents. All participants in the educational process rated the effectiveness of cybersecurity measures at universities at 4 points.



The integration of two-factor authentication for students and lecturers is a promising area for further development of cyberspace, as noted by most respondents. On the other hand, ensuring data backup and recovery is also essential (Zhyvko et al., 2020). The respondents' answers show that training staff and students on detecting phishing attacks and other types of social engineering is an essential protection aspect.

The proposed recommendations are supported by the work of other scholars who have drawn attention to the importance of further developing practical cybersecurity tools (Dei et al., 2024; Guo, 2023). Some scholars emphasise the importance of continuous learning, as digital challenges are constantly evolving, along with countermeasures. Accordingly, this observation will require further scientific discussion. Other researchers point to the need to develop digital competencies at a reasonably young age. The results also suggest that both views are relevant and can be incorporated into general recommendations.

The methodology used in the study has certain limitations that should be considered when further using the results. The proposed methodology has been primarily based on conducting a survey and identifying relevant data. It should be borne in mind that the respondents' personal experiences may differ; therefore, their answers may be subjective. In addition, it should be borne in mind that Russian aggression (and the related challenge of hybrid warfare) has not been experienced in other European countries. Therefore, specific provisions in the responses may indicate a real military impact on the functioning of digital security in wartime.

## Conclusions

Consequently, the most common threats to a secure digital learning space are viruses and malware, hacking of university platform accounts, phishing attacks, and personal data leakage. The surveyed participants in the educational process have an average awareness of ensuring an adequate digital space, indicating the need to improve cybersecurity protection policies.

The respondents' answers pointed to the importance of optimising the cybersecurity space by integrating a two-factor authentication system for students and teachers, implementing system audits, more expansive use of automated threat detection systems, and using encryption to protect data. At the same time, the findings showed that training staff and students to detect phishing attacks and other types of social engineering is a vital protection aspect. The study proved the need to introduce mandatory digital literacy and cyber awareness training and tests. These measures should be implemented to improve cybersecurity in Ukrainian universities.

This research has also opened up new areas for investigation. In particular, future research should be conducted among teachers and students who have taken digital literacy courses or participated in cyber education seminars. This will allow us to assess the impact of these events on the participants' awareness of the educational process. In addition, future work should characterise the latest cyber defence mechanisms, as digital threats will continue to improve and require appropriate innovative protection.

## Bibliographic references

- AlDaajeh, S., Saleous, H., Alrabaei, S., Barka, E., Breiteringer, F., & Raymond Choo, K.-K. (2022). The Role of National Cybersecurity Strategies on the Improvement of Cybersecurity Education. *Computers & Security*, 119, 102754. <https://doi.org/10.1016/j.cose.2022.102754>
- Bannikov, V., Zalialetdzinau, K., Siasiev, A., Ivanenko, R., Saveliev, D., (2022). Computer Science Trends and Innovations in Computer Engineering against the Backdrop of Russian Armed Aggression. *IJCSNS International Journal of Computer Science and Network Security*, 22(9), 465-470. [http://ijcsns.org/07\\_book/html/202209/202209060.html](http://ijcsns.org/07_book/html/202209/202209060.html)
- Bingham, C. (2024). Education and Artificial Intelligence at the Scene of Writing: A Derridean Consideration. *Futurity Philosophy*, 3(4), 34–46. <https://doi.org/10.57125/fp.2024.12.30.03>



- Blažič, B. J. (2021). Changing the landscape of cybersecurity education in the EU: Will the new approach produce the required cybersecurity skills? *Education and Information Technologies*, 27, 3011-3036. <https://doi.org/10.1007/s10639-021-10704-y>
- Bobro, N., Bielikov, V., Matveyeva, M., Salamakha, A., & Kharchun, V. (2024). Advancing Public Administration: Enforcing Strategic Methods and Utilising Tools. *Archives des Sciences*, 74(3), 201–206. <https://doi.org/10.62227/as/74332>
- Bohomaz, O., Koreneva, I., Lihus, V., Kambalova, Y., Shevchuk, V., & Tolchieva, H. (2023). Sobre o desenvolvimento do potencial educacional e científico no século XXI. *Conhecimento & Diversidade*, 15(38), 479–495. <https://doi.org/10.18316/rcd.v15i38.11100>
- Buriachok, V., Korshun, N., Zhylytsov, O., Sokolov, V., & Skladannyi, P. (2023). Implementation of Active Cybersecurity Education in Ukrainian Higher School. In *Information Technology for Education, Science, and Technics, Lecture Notes on Data Engineering and Communications Technologies*, 178, 533–551. Springer Nature Switzerland. [https://doi.org/10.1007/978-3-031-35467-0\\_32](https://doi.org/10.1007/978-3-031-35467-0_32)
- Cabaj, K., Domingos, D., Kotulski, Z., & Respício, A. (2018). Cybersecurity education: Evolution of the discipline and analysis of master programs. *Computers & Security*, 75, 24–35. <https://doi.org/10.1016/j.cose.2018.01.015>
- Catota, F. E., Morgan, M. G., & Sicker, D. C. (2019). Cybersecurity education in a developing nation: the Ecuadorian environment. *Journal of Cybersecurity*, 5(1), tyz001. <https://doi.org/10.1093/cybsec/tyz001>
- Cheng, E. C. K., & Wang, T. (2022). Institutional Strategies for Cybersecurity in Higher Education Institutions. *Information*, 13(4), 192. <https://doi.org/10.3390/info13040192>
- Crick, T., Davenport, J. H., Irons, A., & Prickett, T. (2019). A UK Case Study on Cybersecurity Education and Accreditation. In *2019 IEEE Frontiers in Education Conference (FIE)*. IEEE. <https://doi.org/10.1109/fie43999.2019.9028407>
- Dei, H., Shvets, D., Lytvyn, N., Sytnichenko, O., & Kobus, O. (2024). Legal Challenges and Perspectives of Cybersecurity in the System of State Governance of Educational Institutions in Ukraine. *Journal of Cyber Security and Mobility*, 13(5), 963–982. <https://doi.org/10.13052/jcsm2245-1439.1357>
- Devadze, A., & Gechbaia, B. (2024). Using Virtual Reality in the Educational Process to Increase Students' Motivation and Interest. *E-Learning Innovations Journal*, 2(2), 21–35. <https://doi.org/10.57125/elij.2024.09.25.02>
- Galushchenko, O., Pidbereznykh, I., Piroh, O., Khrapach, D., & Tolmachov, O. (2024). Cybersecurity and geopolitical dimensions of external information interventions in Ukraine: Analysis of current trends. *Data and Metadata*, 3, 345. <https://doi.org/10.56294/dm2024.345>
- Guchua, A., & Zedelashvili, T. (2023). Challenges arising from cyber security in modern global security (on the example of the Russia-Ukraine war). *Eastern Review*, 11(2), 79–88. <https://doi.org/10.18778/1427-9657.11.18>
- Guo, Y.-C. (2023). Development Opportunities, Challenges, and Strategies for Cybersecurity Insurance in the Digital Economy Era. *Global Economic Perspectives*, 1(3), 11-15. <https://doi.org/10.37155/2972-4813-0103-3>
- Haque, M. A., Ahmad, S., John, A., Mishra, K., Mishra, B. K., Kumar, K., & Nazeer, J. (2023). Cybersecurity in Universities: An Evaluation Model. *SN Computer Science*, 4, 569. <https://doi.org/10.1007/s42979-023-01984-x>
- Horlynskyi, V., & Horlynskyi, B. (2019). Cybersecurity as a component of information security of Ukraine. *Collection "Information technology and security"*, 7(2), 136–148. <https://doi.org/10.20535/2411-1031.2019.7.2.190559>
- Khan, M. A., Merabet, A., Alkaabi, S., & Sayed, H. E. (2022). Game-based learning platform to enhance cybersecurity education. *Education and Information Technologies*, 27, 5153-5177. <https://doi.org/10.1007/s10639-021-10807-6>
- Kharlamova, G., Stavytskyy, A., & Komendant, O. (2022). Aligning Higher Education in Ukraine with the Demands for Data Science Workforce. *Communications in Computer and Information Science*, 1635, 97–111. [https://doi.org/10.1007/978-3-031-14841-5\\_7](https://doi.org/10.1007/978-3-031-14841-5_7)
- Korhonen, T., Juurola, L., Salo, L., & Airaksinen, J. (2021). Digitisation or Digitalisation: Diverse Practices of the Distance Education Period in Finland. *Center for Educational Policy Studies Journal*, 11(Sp.Issue), 165-193. <https://doi.org/10.26529/cepsj.1125>



- Kuzminykh, I., Yevdokymenko, M., Yeremenko, O., & Lemeshko, O. (2021). Increasing Teacher Competence in Cybersecurity Using the EU Security Frameworks. *International Journal of Modern Education and Computer Science*, 13(6), 60–68. <https://doi.org/10.5815/ijmecs.2021.06.06>
- Lakhno, V., Kurbaizayov, N., Lakhno, M., Kryvoruchko, O., Desiatko, A., Tsiutsiura, S., & Tsiutsiura, M. (2024). Analysis of digital footprints associated with cybersecurity behavior patterns of users of University Information and Education Systems. *International Journal of Electronics and Telecommunications*, 70(3), 673–682. <https://doi.org/10.24425/ijet.2024.149596>
- Melenti, Y., Yevseiev, S., Korol, O., Milevskiy, S., & Khvostenko, V. (2024). Application of the innovative approach in the modernization of higher education institutions of the security service of Ukraine. *Ukrainian Scientific Journal of Information Security*, 30(1), 179–189. <https://doi.org/10.18372/2225-5036.30.18619>
- Muktiarni, M., Widiaty, I., Abdullah, A. G., Ana, A., & Yulia, C. (2019). Digitalisation trend in education during industry 4.0. *Journal of Physics: Conference Series*, 1402, 077070. <https://doi.org/10.1088/1742-6596/1402/7/077070>
- Nehrey, M., Voronenko, I., & Salem, A.-B. M. (2022). Cybersecurity Assessment: World and Ukrainian Experience. In *2022 12th International Conference on Advanced Computer Information Technologies (ACIT)*. IEEE. <https://doi.org/10.1109/acit54803.2022.9913081>
- Newhouse, W., Keith, S., Scribner, B., & Witte, G. (2017). *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework*. National Institute of Standards and Technology. <https://doi.org/10.6028/nist.sp.800-181>
- Politova, O., Pustovoichenko, D., Hrechanyk, N., Yaroshchuk, K., & Nenko, S. (2022). ICT-oriented Training of Future HEI Teachers: A Forecast of Educational Trends 2022-2024. *International Journal of Computer Science and Network Security*, 22(4), 387-393. <https://doi.org/10.22937/IJCSNS.2022.22.4.45>
- Potii, O. V., Korneyko, O. V., & Gorbenko, Y. I. (2015). Cybersecurity in Ukraine: Problems and Perspectives. *Information & Security: An International Journal*, 32, 71–94. <https://doi.org/10.11610/isij.3201>
- Pozharytskyi, P., Iliencko, O., Vlasenko, N., Krasnova, Y., & Borysenko, O. (2022). Future prospects for the development of pro-environmental higher education. *Ad Alta*, 12(2), 133-138. <https://www.magnanimitas.cz/ADALTA/120228/PDF/120228.pdf>
- Ricci, J., Breitingner, F., & Baggili, I. (2018). Survey results on adults and cybersecurity education. *Education and Information Technologies*, 24(1), 231–249. <https://doi.org/10.1007/s10639-018-9765-8>
- Rodinova, N., Pylypchuk, N., Domashenko, S., Havrylyuk, I., & Androsovykh, A. (2024). Ukrainian Economy in the Era of Digital Branding: Risks and Opportunities. *Futurity Economics & Law*, 4(4), 4–24. <https://doi.org/10.57125/fel.2024.12.25.01>
- Sullivan, J. E., & Kamensky, D. (2017). How cyber-attacks in Ukraine show the vulnerability of the U.S. power grid. *The Electricity Journal*, 30(3), 30–35. <https://doi.org/10.1016/j.tej.2017.02.006>
- Terepyschyi, S., & Kostenko, A. (2022). Mapping the Landscapes of Cybersecurity Education during the War in Ukraine 2022. *Warmia Studies*, 59, 125–135. <https://doi.org/10.31648/sw.8331>
- Ulven, J. B., & Wangen, G. (2021). A Systematic Review of Cybersecurity Risks in Higher Education. *Future Internet*, 13(2), 39. <https://doi.org/10.3390/fi13020039>
- Zabasta, A., Peuteman, J., Kunicina, N., Kazymyr, V., Hvesenya, S., Hnatov, A., Paliyeva, T., & Ribickis, L. (2020). Research on Cross-Domain Study Curricula in Cyber-Physical Systems: A Case Study of Belarusian and Ukrainian Universities. *Education Sciences*, 10(10), 282. <https://doi.org/10.3390/educsci10100282>
- Zhao, Y., Pinto Llorente, A. M., & Sánchez Gómez, M. C. (2021). Digital competence in higher education research: A systematic literature review. *Computers & Education*, 168, 104212. <https://doi.org/10.1016/j.compedu.2021.104212>
- Zhyvko, Z., Rudyi, T., Senyk, V., & Kucharska, L. (2020). Legal basis of ensuring cyber security of Ukraine: Problems and ways of eliminating. *Economics, Finance and Management Review*, (2), 82–90. <https://doi.org/10.36690/2674-5208-2020-2-82>

