Salud, Ciencia y Tecnología - Serie de Conferencias. 2024; 3:.648
doi: 10.56294/sctconf2024.648

ORIGINAL

Analysis of Cyber-psychological Protection Programs in the Education System: role, Limitations and Prospects

Análisis de los programas de protección ciberpsicológica en el sistema educativo: rol, limitaciones y perspectivas

Svitlana Khadzhyradieva[1], Marianna Todorova[1], Sergii Staikutsa[1], Liudmyla Tsybukh[1], Alla Lukiianchuk[2]

[1]State University of Intelligent Technologies and Telecommunications. Odesa, Ukraine.
[2]Higher Education Institution "Interregional Academy of Personnel Management". Bila Tserkva, Ukraine.

Cite as: Khadzhyradieva S, Todorova M, Staikutsa S, Tsybukh L, Lukiianchuk A. Analysis of Cyber-psychological Protection Programs in the Education System: Role, Limitations and Prospects. Salud, Ciencia y Tecnología - Serie de Conferencias. 2024; 3:.648. https://doi.org/10.56294/sctconf2024.648

Submitted: 17-02-2024 **Revised:** 27-06-2024 **Accepted:** 12-12-2024 **Published:** 13-12-2024

Editor: Prof. Dr. William Castillo-González

ABSTRACT

Introduction: as technology integration in education expands, the need for robust cyber-psychological protection programs becomes paramount. This study delves into analysing cyber-psychological protection initiatives within the education system.
Objectives: this research aims to investigate the effectiveness and potential challenges of cyber-psychological protection programs in educational settings. Focusing on their role in safeguarding participants against online threats, the study explores limitations hindering their efficacy and prospects for future enhancements.
Method: this paper uses a comprehensive analysis of digital literacy and cybersecurity programs offered by universities such as Harvard University, Stanford University, the University of Washington, and several Ukrainian universities. The study was formed based on comparative analysis and content analysis.
Results: the results showed that cyber-psychological protection programs are pivotal in enhancing awareness among students, educators, and administrative staff regarding potential cyber threats. Moreover, these programs work towards establishing a cybersecurity culture within educational institutions. The findings indicate that cyber-psychological protection programs are vital in fostering a secure learning environment. However, resource constraints and the evolving nature of cyber threats pose significant limitations.
Conclusions: the study recommends exploring external resources, embracing innovative technologies, fostering collaboration, and establishing standardised measures. Recognising the dynamic landscape of cyber threats, the conclusions underscore the importance of continual adaptation and collaboration to ensure effective cyber-psychological protection in education.

Keywords: Cyberpsychology; Online Programs; Cybersecurity Culture; Recommendations.

RESUMEN

Introducción: a medida que se expande la integración de la tecnología en la educación, la necesidad de programas sólidos de protección ciberpsicológica se vuelve primordial. Este estudio profundiza en el análisis de las iniciativas de protección ciberpsicológica dentro del sistema educativo.
Objetivos: el objetivo principal de esta investigación es investigar la efectividad y los desafíos potenciales de los programas de protección ciberpsicológica en entornos educativos. Centrándose en su papel en la protección de los participantes contra las amenazas en línea, el estudio explora las limitaciones que obstaculizan su eficacia y las perspectivas de futuras mejoras.
Método: en este artículo se utilizó un análisis exhaustivo de los programas de alfabetización digital y

ciberseguridad ofrecidos por universidades como la Universidad de Harvard, la Universidad de Stanford, la Universidad de Washington y varias universidades ucranianas. El estudio se formó sobre la base de un análisis comparativo y un análisis de contenido.
Resultados: los resultados mostraron que los programas de protección ciberpsicológica desempeñan un papel fundamental en la mejora de la conciencia entre los estudiantes, educadores y personal administrativo sobre las posibles amenazas cibernéticas. Además, estos programas trabajan para establecer una cultura de ciberseguridad dentro de las instituciones educativas.
Conclusiones: en la conclusión, el estudio recomienda explorar recursos externos, adoptar tecnologías innovadoras, fomentar la colaboración y establecer medidas estandarizadas. Reconociendo el panorama dinámico de las amenazas cibernéticas, las conclusiones subrayan la importancia de la adaptación y la colaboración continuas para garantizar una protección ciberpsicológica eficaz en la educación.

Palabras clave: Ciberpsicología; Programas En Línea; Cultura De Ciberseguridad; Recomendaciones.

INTRODUCTION

In an era marked by the incessant advancement of technology, educational institutions find themselves at the forefront of a digital revolution. Integrating cutting-edge digital technologies into pedagogical and administrative practices not only enhances the efficiency of educational processes but also opens up new avenues for cyber threats.

As the education sector becomes more reliant on digital platforms for myriad activities, the potential risks associated with cyber threats escalate. Data breaches, ransomware attacks, and unauthorised access to sensitive information pose significant challenges to the smooth functioning of educational institutions. The consequences of such incidents extend beyond mere disruptions, affecting the trust and confidence of students, faculty, and other stakeholders.

The need for robust cybersecurity measures in education goes beyond the mere protection of data; it encompasses preserving the integrity of academic processes and ensuring privacy for both students and faculty members. Educational institutions house a wealth of sensitive data, ranging from academic records to financial information, making them attractive targets for cyber adversaries.

A comprehensive cybersecurity strategy is imperative to create a resilient defence against the ever-evolving tactics employed by malicious actors in the digital realm. Moreover, recent global events have accelerated the adoption of remote and online learning, further amplifying the significance of cybersecurity in education. The shift towards virtual classrooms and digital collaboration tools introduces additional layers of vulnerability that demand immediate attention.

The urgency of securing online learning environments and protecting the confidentiality of virtual interactions heightens the relevance of cybersecurity initiatives in education.

This dynamic and evolving landscape underscores the critical need to examine cyber-psychological protection programs thoroughly. These programs focus on technical aspects and consider the human element in cybersecurity.

Understanding how individuals interact with digital systems, recognising potential weaknesses in human behaviour, and implementing strategies to foster a cyber-secure culture are paramount in fortifying educational institutions against the multifaceted challenges posed by cyber threats. The scholars described some issues.

Korniichuk et al.[1] investigated using the case study method in medical education. Through a meta-analysis, Tsekhmister[2] evaluated the effectiveness of blended learning in biomedical engineering. Prokopenko[3] analysed aspects of the state information policy and its definitions for the future. Krymets[4] wrote about the nature of future education through philosophical reflections. Vasylyuk-Zaitseva et al.[5] discussed the application of artificial intelligence in the future of Ukrainian education.

Yemelyanova et al.[6] investigated the educational crisis in today's information and digital society. Krylova et al.[7] examined the role of social networks in combating gender-based violence. Tsoli[8] explored teachers' perceptions of entrepreneurial education before and after implementing a pilot program. Although philosophical reflections on future education provide insights, researchers could further elaborate on practical implications, potential hurdles, and alternative perspectives in shaping cyber education and cyber protection of the future.

This scholarly article is dedicated to meticulously examining and evaluating the roles, constraints, and future trajectories of cyber-psychological protection programs within the educational sector. The objective is to ascertain the present state of cybersecurity in education and delineate strategies for enhancing countermeasures against cyber threats within educational establishments. The examination will elucidate pivotal facets encompassing the judicious use of technology, psychological dimensions of cybersecurity, and constraints that may impede the optimal functionality of programs within the educational milieu.

https://doi.org/10.56294/sctconf2024.648

METHOD

The primary goal of this study was to conduct a comprehensive analysis of universities' digital literacy and cybersecurity programs, focusing on selected institutions such as Harvard University, Stanford University, the University of Washington, and the Ukrainian initiative DigiUni. To achieve this goal, the study employs a qualitative approach.

This study's universe encompasses a range of institutions and initiatives involved in digital literacy programs. These organisations should also represent different approaches to developing digital competencies, integrating new technologies, and addressing cybersecurity issues. The selected universe aims to include both global and local organisations.

The study used a purposive sampling approach to select institutions and initiatives. The following criteria were used to select institutions and initiatives:

1. Inclusion of institutions that actively provide resources, courses, and initiatives related to digital literacy.
2. Inclusion of programs that provide information on modern digital learning technologies
3. Availability of publicly available materials for analysis
4. Inclusion of innovative pedagogical approaches or emerging technologies in their curriculum.

Instruments used to collect data

Several methods and tools were used to collect data, allowing for individual digital literacy programs and initiatives to be included in the analysis. First, a documentary analysis of publicly available documents, websites, program descriptions, training materials, presentations and reports was used. Unique invitations were sent to individual platforms to collect data, indicating that the authors were willing to process data from their sites. The primary sources were individual university and organization websites, reports on the implementation of programs available in academic databases or initiative websites and projects posted in the open access.

Statistical processing

1. Harvard University - Digital literacy resource platform

Data analysis: assessed the range of digital literacy resources offered, analysed the target audience and the diversity of courses provided, and evaluated the pedagogical approaches employed in the digital literacy programs.

2. Stanford University - Digital Education

Data analysis: explored the variety of online courses and resources available for digital literacy and investigated the incorporation of emerging technologies in educational materials.

3. University of Washington - Teaching and learning technologies

Data Analysis: examined the structure and content of digital literacy and cybersecurity courses and explored any collaborations with external organisations or industry partners.

4. DigiUni - Digital University - an Open Ukrainian initiative

Material Source: Information provided by Kyiv National University, named after Taras Shevchenko.

Data Analysis: I reviewed the initiative's goals and objectives, evaluated the structure of the digital literacy and cybersecurity programs, and investigated any partnerships with external entities or international collaborations.

5. NEXT – Digital transformation to support the new generation of workers

Material Source: information related to the NEXT program.

Data Analysis: examined the components of informal extracurricular education within the program and assessed the potential impact.

6. Unity Initiative by Cormack Consultancy Group

Material Source: Information provided by the Cormack Consultancy Group.

Data Analysis: Evaluated the goals and scope of the Unity Initiative in the education sector.

Content Analysis

Objective: To systematically examine the content and structure of selected universities' digital literacy and cybersecurity programs.

Implementation: Analyzed course descriptions and educational materials. Identified key themes, learning objectives, and pedagogical strategies.

https://doi.org/10.56294/sctconf2024.648

Programmatic Impact Assessment

Objective: To assess the broader impact of digital literacy and cybersecurity programs on educational ecosystems.

Implementation: Examined the goals and outcomes of the programs and evaluated their potential influence on shaping the skills and competencies.

Comparative Analysis

Object: The role of modern programs is based on comparing their perspectives and limitations. *Implementation:* Expansion of constraints and prospects for using and implementing these programs is based on comparative analysis.

RESULTS

Cybersecurity protection programs within the education system are designed to ensure the security and safeguarding of informational resources and the personal data of students and educational staff in the era of advanced technologies and digital interaction. These programs encompass various measures to prevent, detect, and respond to potential threats within the academic information space. A crucial component of these initiatives includes digital literacy development programs, often based at modern universities. [9, 10] For instance, Harvard University has developed the Digital Citizenshio+ Resource Platform, a comprehensive resource designed to cultivate digital literacy (https://dcrp.berkman.harvard.edu/). This platform includes educational materials and tools for advancing digital skills. Stanford University offers diverse online courses and resources for digital literacy through the Stanford Digital Learning platform (https://online.stanford.edu/). The Media Lab Learning Initiative at the Massachusetts Institute of Technology comprises projects and resources focused on advancing digital literacy and pioneering innovative technologies. Simultaneously, the University of Washington has initiated the Digital Literacy Initiative, aiming to enhance skills in technology use and understanding of the digital environment. On a broader scale, the European University has introduced "DigComp", a standard for competencies in digital literacy that can serve as a foundation for developing national-level programs (https://online.stanford.edu/). In Ukraine, a collaborative effort between national and international universities has given rise to several digital literacy and cybersecurity projects. One prominent initiative, the "DigiUni - Digital University - an Open Ukrainian Initiative", is spearheaded by Kyiv National University, named after Taras Shevchenko. The primary objective of this project is to establish a unified digital educational ecosystem in Ukraine.[11] This ecosystem aims to deliver continuous, high-quality, inclusive, and transparent education, regardless of participants' locations. The project leverages existing digital innovations in the educational field and adopts a clear paradigm for incorporating future innovations.

This project is international, involving universities from Germany, Spain, France, the Czech Republic, and Poland. Simultaneously, this project fosters cooperation among Ukrainian universities, including Lviv Ivan Franko National University, Ukrainian Catholic University, Chernivtsi National University named after Yury Fedkovich, Sumy State University, National Technical University "Kharkiv Polytechnic University", Mariupol State University, Kherson State University, and others.[11]

Another project under "NEXT – Digital Transformation to Support the New Generation of Workers" envisions the development of informal extracurricular education focusing on digital skills, soft skills, mental health, and legal aspects of digitization for students. The project also aims to prepare university faculty to provide students with qualified trainers for informal learning. Additionally, it involves the creation of innovative educational resources aligned with the latest trends in digital technologies.[11] The initiative strengthens team collaboration among students through a competition in teamwork projects and digital skills. Advanced laboratories for metaverse communications are also set to be established in Ukrainian universities as part of this project. The project is coordinated by the Slovak Technical University in Bratislava, and additional coordination is provided by Lviv Ivan Franko National University, the National Technical University of Ukraine "Kyiv Polytechnic Institute named after Igor Sikorsky," National University "Odesa Polytechnic," and Cherkasy State Technological University. Simultaneously, Sumy State University collaborates with the University of Liverpool (United Kingdom) under the "Unity Initiative" program initiated by the British consulting company in education, Cormack Consultancy Group. This collaboration, supported by the governments of the UK and Ukraine, aims to develop long-term cooperation between British and Ukrainian universities and provide urgent targeted support to Ukrainian universities during both wartime and peacetime. Within the program, Sumy State University and the University of Liverpool implement a joint project, "Collaboration for the Digitization and Digital Transformation of Ukraine," focused on knowledge exchange and collaborative scientific research.[11] Currently, numerous programs exist for both students and educators. The table below summarizes their main directions of activity (See table 1).

Table 1. The main directions of programs on digital literacy

Aspects	Description
Cybersecurity training	Conducting regular training sessions and seminars for students, teaching staff, and administrative personnel on cybersecurity matters. Implementing mandatory cybersecurity courses into educational plans and programs.[12,13,14]
Digital literacy development	Providing education to students and teachers on recognizing phishing attacks, viruses, and other forms of cyber threats. Utilizing interactive games and simulations to train cybersecurity skills.
Protection of personal data	Implementing strict policies for the storage and processing of personal data of students and educators. Ensuring confidentiality and security of information about students.
Network security	Implementing measures to secure the network infrastructure of school systems, including firewalls, antivirus tools, and other protective measures. Continuously monitoring and analyzing network activity to detect potential threats.
Community partnership	Collaborating with cybersecurity agencies and law enforcement authorities for information exchange and support in case of need.

Mechanisms of cyberpsychological protection play an important role for the human psyche:[15,16]

1. Decreasing emotional stress. Defense mechanisms help reduce the impact of negative emotions that can arise from stressful situations. This helps to avoid pain or discomfort.
2. Regulation of self-esteem. In difficult situations, self-esteem can decrease, leading to feelings of guilt or rejection. Cyberpsychological defense mechanisms help to increase self-esteem, protecting against negative emotions.
3. Maintaining mental stability. Mechanisms such as displacement, projection, and intellectualization help to forget past dangerous or stressful situations and maintain a positive mindset.

The overall objective of these programs is to ensure the safety of participants in the educational process within the online environment and to cultivate a culture of cybersecurity among both students and personnel. In a rapidly evolving digital landscape, these initiatives aim to equip students and staff with essential skills and knowledge to navigate the internet securely. By fostering a culture of cybersecurity, these programs seek to empower individuals to recognize and respond to potential cyber threats, creating a safer educational environment for everyone involved. Although the effectiveness of the cyber-psychological protection program in the education system is undeniably valuable, this comprehensive analysis reveals some limitations that need to be addressed.[14] The figure shows the main limitations on the development of the cyber-psychological protection program in the system of modern education (figure 1).

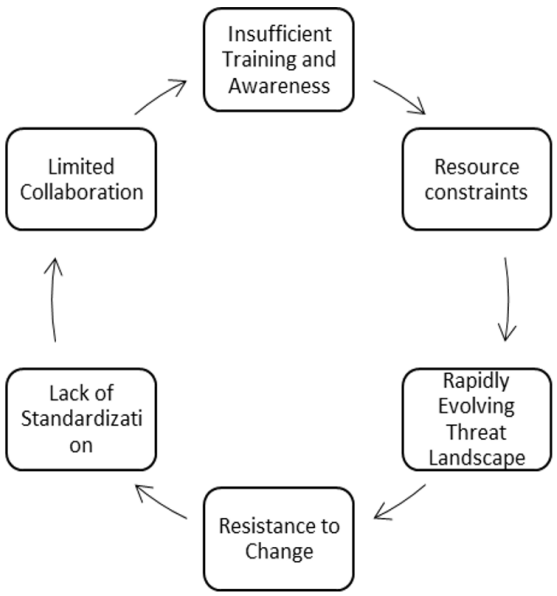

Figure 1. The main limitations on the development of the cyber-psychological protection program in the system of modern education

The figure demonstrates that a significant limitation is the shortage of resources. Many educational institutions, especially those with constrained budgets, encounter challenges in allocating sufficient financial

and human resources to implement and sustain reliable cyber-psychological protection programs. This limitation impedes the development of comprehensive initiatives, rendering the educational environment more vulnerable to contemporary cyber threats. However, it is crucial to acknowledge that the cyber threat landscape is dynamic and continually evolving. Cybercriminals employ sophisticated tactics, and new threats emerge regularly. Traditional cyber-psychological protection programs may struggle to keep pace with these rapid changes, complicating the support for consistently high levels of protection.[18,19] Continuous efforts are required to update and adapt programs to effectively address new risks. Another important limitation is resistance to change. Modern research has demonstrated that resistance to accepting new technologies, practices, or changes in thinking is a common barrier in educational institutions.[6]

Overcoming this resistance requires not only effective communication but also the development of a culture that values and prioritizes cybersecurity. Simultaneously, scientific studies have proven that the absence of standardized instructions or a universal foundation for cyber-psychological protection programs can lead to inconsistencies between different educational institutions. In some cases, the effectiveness of cyber-psychological protection programs is diminished due to inadequate training and awareness initiatives. Therefore, it is essential not only to implement protective measures but also to ensure that all stakeholders, including students, educators, and administrative staff, receive continuous and relevant training to stay informed about evolving threats. Moreover, effective cybersecurity often requires collaboration and information sharing between educational institutions. On the other hand, limited collaboration can lead to missed opportunities for learning from each other's experiences and collectively strengthening cybersecurity measures. Overcoming these limitations demands a holistic approach that combines technology, policy improvements, and a cultural shift towards prioritizing cybersecurity in the education system. As cyber threats continue to evolve, overcoming these challenges will be crucial for creating resilient and adaptive cyber-psychological protection programs. Therefore, there is a promising solution for each of these challenges. The table summarizes in detail the main challenges and prospects for the implementation of modern cyber-psychological protection programs in the education system. The limitation section is divided into "challenges", which describes the main obstacles, and "impact", which describes the importance of this challenge for the development of an effective system for countering cyber threats. The perspective section consists of "decision" and "impact" (table 2).

Table 2. The main challenges and prospects for the implementation of modern cyber-psychological protection programs in the education system

Limitations	
Resource constraints	
Challenge	Many educational institutions, particularly those with limited budgets, face challenges in allocating adequate financial and human resources.
Impact	This limitation hinders the development of comprehensive initiatives, making the educational environment more vulnerable to cyber threats.
Rapidly evolving threat landscape	
Challenge	The dynamic nature of cyber threats poses a challenge for traditional programs to keep pace with emerging risks.
Impact	Difficulty in maintaining consistently high levels of protection due to the evolving tactics of cybercriminals.
Resistance to change	
Challenge	Some stakeholders may resist adopting new cybersecurity measures, hindering program effectiveness.
Impact	Overcoming resistance requires not just effective communication but also a cultural shift that prioritizes and values cybersecurity.
Lack of standardization	
Challenge	Absence of standardized guidelines can lead to inconsistencies between educational institutions.
Impact	Varying levels of preparedness and effectiveness across institutions may result in inadequate protection.
Insufficient training and awareness	
Challenge	Inadequate training and awareness initiatives can compromise the effectiveness of cyber-psychological protection programs.
Impact	Stakeholders may lack the knowledge needed to recognize and respond to evolving cyber threats, leaving the educational environment exposed.
Limited collaboration	
Challenge	Effective cybersecurity often requires collaboration and information sharing among educational institutions.

Impact	Limited collaboration may result in missed opportunities to learn from each other's experiences and collectively strengthen cybersecurity measures.
Prospects	
Integration of advanced technologies	
Prospect	Leveraging technologies like artificial intelligence and machine learning to enhance program efficiency.
Impact	Improved adaptability to evolving cyber threats, ensuring sustained high levels of protection.
Collaboration and information sharing	
Prospect	Establishing collaborative networks for information sharing among educational institutions.
Impact	Strengthening collective resilience against cyber threats through shared insights and experiences.
Continuous training and adaptation	
Prospect	Emphasizing continuous training and adaptability of programs to address emerging risks.
Impact	Ensuring ongoing relevance and effectiveness in the face of evolving cyber threats
Global best practices sharing	
Prospect	Facilitating the sharing of global best practices in cybersecurity within the education sector.
Impact	Institutions can learn from successful models worldwide, fostering innovation and the adoption of effective strategies.
Public-private partnerships	
Prospect	Encouraging partnerships between educational institutions and private cybersecurity firms.
Impact	Access to industry expertise and resources, enhancing the capability to implement state-of-the-art cybersecurity measures.
Development of cybersecurity standards	
Prospect	Collaborative efforts to establish standardized cybersecurity standards for educational institutions.
Impact	Providing a clear framework for implementation, ensuring consistency and effectiveness across diverse educational environments.

Source:[20,21]

In the realities of the deployment of Russian military aggression, schoolchildren and teenagers, their parents and teachers also need psychological support. In such conditions, individual initiatives, introduced both with the support of the government and volunteers, and thanks to the international support of global human rights and medical structures, have demonstrated themselves highly.[22]

The "Close" ("Poruch" in Ukrainian) project is a psychological support group for teenagers and parents whose normal lives have been disrupted by the war. Psychologists are ready to provide help both offline and online, making sure that the experiences of Ukrainian citizens do not become insurmountable traumas for the rest of their lives. Online meetings will be held on ZOOM, each session is attended by no more than 10 participants and a leading psychologist.[23] Participation in groups is free, the time of meetings is agreed with each participant. During these classes, children will have the opportunity to share their experiences, feel the support of peers and professionals, and also find ways to support themselves and their loved ones in difficult times. This is a chance to be part of a community of people who understand and support each other.[24]

"Close" psychologists not only help teenagers, but also support parents. Since parents need to take care not only of their own mental health and psychological well-being, but also of their children's condition, the workload increases significantly. As experts say, in such situations there is no such thing as excessive support. Adult participants will discuss a variety of topics, including how to support yourself and your loved ones, managing emotions during difficult times, overcoming pain, finding yourself in new life circumstances, planning for uncertain times, and finding resources. Importantly, the project involves professional psychologists who have the skills to help war survivors and those seeking professional training for this important work in these challenging times.[24]

The "Close" project also recognizes the critical importance of cybersecurity in today's interconnected world. In the context of providing psychological support for adolescents and parents affected by the consequences of war, a dedicated focus on cyber protection becomes imperative. Cybersecurity measures will be implemented to safeguard the online meetings held on ZOOM, ensuring the privacy and confidentiality of participants. The project organizers are committed to utilizing state-of-the-art technologies and best practices to prevent any potential cyber threats or unauthorized access during the virtual sessions. Participants will be educated on the

importance of maintaining online security and practicing responsible digital behavior. Psychologists involved in the project will provide guidance on protecting personal information, recognizing potential online risks, and ensuring a secure virtual environment for all participants.[24]

One of the factors contributing to information security is the application of artificial intelligence technologies. Artificial intelligence is a prevailing trend embraced by all developed countries worldwide. The global market for AI-based technological solutions will be divided among competitive nations, complicating the country's development in strategically vital sectors of the economy and slowing down its progress. Artificial intelligence encompasses a set of technological solutions that simulate human cognitive functions and yield results equivalent to human intellectual activity when performing specific tasks.[25] The active development of information technologies underscores the relevance of studying information security issues, namely:

- Threats to information resources, various means, and security measures;
- Barriers to penetration;
- Vulnerable points in the information security system.[26]

In general, information security should be understood as the totality of means, methods, and processes (procedures) that ensure the protection of information assets and, consequently, guarantee the preservation of efficiency and practical utility in both the technical infrastructure of information systems and the information stored and processed within such systems.[27] The utilization of artificial intelligence in information security systems gains particular significance and relevance in the spectrum of societal relations. Using artificial intelligence for cyberpsychological protection programs in the education system can be an effective approach to ensure the security of users and data (table 3).

Table 3. The utilization of artificial intelligence in cybersecurity

Approach	Characteristic
User Behavior Analysis	- Utilize machine learning algorithms to analyze typical user behavior patterns. - Detect anomalies in behavior, such as unknown login attempts or changes in regular activities.
Email and Message Filtering	- Use AI to automatically filter out fraudulent or phishing messages. - Develop systems that can recognize suspicious attachments or links in emails.
Real-time Threat Detection	- Develop systems that identify potential threats and attacks in real-time through the analysis of network traffic. - Employ machine learning algorithms to predict and identify new types of attacks.
Training Staff and Students	- Create interactive online courses on cybersecurity that leverage AI technologies to simulate real attack scenarios. - Utilize chatbots to educate users on avoiding threats and recognizing suspicious activity.
Monitoring Social Media	- Use text analysis algorithms to detect negative or threatening messages on social media. - Respond to psychological aspects identified in texts that may indicate potential issues.
Access Control	- Use AI technologies to develop access control systems that automatically adapt to changes in user behavior.

Source: [28]

It's important to consider ethical aspects and data privacy when implementing such systems. Additionally, the system should be continuously updated to detect and adapt to new threats effectively.[29] In addressing these limitations and exploring new prospects, the education system can better navigate the evolving cybersecurity landscape, fostering a safer and more resilient environment for students, educators, and staff. To sum up, while cyber-psychological protection programs play a crucial role in fostering a secure digital environment in education, addressing resource constraints, adapting to the dynamic threat landscape, and overcoming resistance to change are imperative for sustained effectiveness. Prospects lie in technological integration, collaboration, and continuous adaptation to ensure robust cybersecurity measures within the education system.

DISCUSSION

The analysis of cyber-psychological protection programs in the education system demonstrated the existence of a considerable number of online tools for its provision. A variety of functionality makes it possible to widely use them during cyber-psychological support and protection of students, their parents and teachers. Therefore, the results of this research confirm the conclusions of Martínez-Ferrer et al.[30] that the modern market of cyberpsychological programs is quite developed.

Moreover it is proved the conception of those scientists who note the further rapid evolution of cyber-psychological protection, since the digital environment is developing quite dynamically, generating new threats. Responding to these changes will be an important element for the development and implementation of cyber-

psychological protection programs in the future.[32]

In particular, the results of this study determined that the formation of remote psychological support tools was influenced by the Russian military invasion. Thanks to him, separate initiatives in cyberspace were introduced, which became a strong basis for overcoming the negative consequences of the war for students, their parents and teachers. Therefore, even such offline challenges will require the development of appropriate programs and platforms for psychological support and accompaniment. Furthermore, the study sheds light on the unique intersection of geopolitical events and the evolution of cyber-psychological protection tools.[33,34]

The influence of the Russian military invasion became a catalyst for the development of innovative initiatives in cyberspace, serving as a resilient foundation to address the psychological toll on students, parents, and teachers affected by the conflict.[35,36] This underscores the adaptability of cyber-psychological programs in responding to real-world challenges that extend beyond the digital realm, emphasizing the critical need for ongoing research and the implementation of tailored programs to navigate the complex landscape of psychological support during and after offline crises.

On the other hand, Rakhimov[37] emphasized the fusion of technology and morality in modern society. This tendency manifests itself in various important aspects, including the emergence of artificial intelligence as the basis for a new moral paradigm, the change in morality under the influence of artificial intelligence, and the balance and autonomy between innovative technological advances and traditional moral principles. Canetti et al.,[38] in fact, doubted the possibilities of applying artificial intelligence technologies in education.

The complicated analysis demonstrated that artificial intelligence technologies can have a very practical effect when organizing psychological support. Therefore, their involvement in the organization and support of the educational process is quite important and promising.

While some researchers, such as Bui and Pasalich[39], contend that cyber threats may not inflict significant damage to compromise the immunity of non-combatants, this perspective is met with skepticism. The findings of the study suggest that the repercussions of prolonged disruptions during conventional warfare provide valuable insights for extrapolating the potential ripple effects of cyber threats. It is essential to acknowledge the interconnectedness of digital and physical realms, as the consequences of cyber threats can have far-reaching implications, influencing not only the digital landscape but also the well-being and resilience of non-combatant populations. In alignment with the conclusions drawn by Kumar and Tandon,[26] there is a growing consensus on the importance of implementing robust cyber defense programs for non-combatants.

Recognizing the impact of cyber threats beyond military contexts emphasizes the need for comprehensive strategies to safeguard individuals, educational institutions, and communities at large. Such initiatives are vital not only for mitigating immediate threats but also for fostering a resilient and secure environment in the face of evolving cyber challenges.[40]

However, it is imperative to acknowledge the limitations inherent in the proposed study. The focus on programmatic impact assessment, while crucial for evaluating goals and outcomes, may fall short in comprehensively assessing the long-term and multifaceted impacts on educational ecosystems.

The dynamic nature of skills development and competencies over time may not be fully captured by this assessment. Additionally, the comparative analysis, while informative, may be constrained by its single-dimensional perspective, potentially overlooking various factors influencing program effectiveness, such as teaching methodologies, available resources, and contextual adaptations. To address these limitations and enhance the robustness of future research, there is a need to extend the comparative analysis beyond the confines of selected universities.

A more inclusive approach involving a diverse set of institutions globally would provide a broader and more nuanced perspective on the various approaches and effectiveness of digital literacy and cybersecurity education.

This expanded scope would enable researchers to consider regional nuances, cultural variations, and resource disparities, ultimately contributing to a more comprehensive understanding of the challenges and opportunities in promoting cybersecurity education on a global scale.

CONCLUSION

Hence, modern cyberpsychological protection programs emphasize different aspects: digital literacy, protection of private data and psychological stability and protection of Internet users. These programs play a crucial role in enhancing cybersecurity and awareness among participants in the educational process.

However, identified limitations such as resource shortages, rapid evolution of cyber threats, resistance to change, lack of standardization, and insufficient training and awareness cast doubt on the stability and comprehensiveness of protection in the educational setting.

Thus, these perspectives determine the main recommendations: educational institutions may consider opportunities to engage external resources, such as partnerships with private cybersecurity firms or participation in global cybersecurity initiatives.

https://doi.org/10.56294/sctconf2024.648

In conclusion, despite existing challenges and limitations, recommendations involving the engagement of external resources, the utilization of advanced technologies, collaboration, and ongoing training can pave the way for ensuring robust and highly effective cyber-psychological protection in the education system.

REFERENCES

1. Korniichuk OY, Bambyzov LM, Kosenko VM, Spaska AM, Tsekhmister YV. Application of the Case Study Method in Medical Education. IJLTER. 2021 Jul 30;20(7):175–91. doi: 10.26803/ijlter.20.7.10

2. Tsekhmister Y. Effectiveness of Blended Learning in Biomedical Engineering: A Meta-Analysis. JHETP [Internet]. 2023 Mar 25 [cited 2024 Dec 12];23(5). Available from: https://articlegateway.com/index.php/JHETP/article/view/5976

3. Prokopenko O. Some aspects of the state information policy of the modern state: definitions of the future. Futurity Economics&Law. 2022 Dec 25;60–72. doi: 10.57125/FEL.2022.12.25.08

4. Krymets L. What must the education of the future be like to be really future? (Attempts of philosophical reflection). Futurity Philosophy. 2022 Dec 30;28–41. doi: 10.57125/FP.2022.12.30.03

5. Vasylyuk-Zaitseva S, Kosenyuk H, Tanasiichuk I, Boyko J. Application of artificial intelligence in Ukrainian education of the future. Futurity Education. 2023 Sep 25;77–103. doi: 10.57125/FED.2023.09.25.05

6. Yemelyanova O, Bakhmat N, Huda O, Shvets T, Boichuk A. The educational crisis in today's information and digital society. Eduweb. 2023 Apr 8;17(2):267–84. doi: 10.46502/issn.1856-7576/2023.17.02.23

7. Krylova SA, Malynovska TM, Bidzilya YM, Barchan OV, Hetsko HI. Social Networks as a Means of Combating Gender-Based Violence. Cuest Pol. 2022 Mar 7;40(72):164–81. doi: 10.46398/cuestpol.4072.09

8. Tsoli K. Perception of Teachers on Entrepreneurial Education Before and After the Implementation of a Pilot Program. Futurity Education. 2023 Sep 25;3(3):178–95. doi: 10.57125/FED.2023.09.25.10

9. Bulavko GV, Davidenko NA, Davidenko II, Ishchenko AA, Mokrinskaya EV, Pavlov VA, Studzinsky SL, Tonkopieva LS, Chuprina NG. Photovoltaic Characteristics of Film Composites Based on Glycidylcarbazole Cooligomer with Symmetrical Cationic Polymethine Dyes. Theor Exp Chem [Internet]. 2013 Sep [cited 2024 Dec 28];49(4):219-23. Available from: https://doi.org/10.1007/s11237-013-9318-6

10. Muniandy L, Muniandy B, Samsudin Z. Cyber Security Behaviour among Higher Education Students in Malaysia. JIACS. 2017 Feb 3;1–13. doi: 10.5171/2017.800299

11. Ivan Franko National University of Lviv, International Office [Internet]. Ongoing projects; [cited 2024 Dec 12]. Available from: https://international.lnu.edu.ua/european-programmes-and-projects/erasmus/key-action-2/ongoing-projects/

12. Alqazzaz A, Tabrez Quasim M, Mujib Alshahrani M, Alrashdi I, Ayoub Khan M. A Deep Learning Model to Analyse Social-Cyber Psychological Problems in Youth. Computer Systems Science and Engineering. 2023;46(1):551–62. doi: 10.32604/csse.2023.031048

13. Krap A, Bataiev S, Bobro N, Kozub V, Hlevatska N. Examination of digital advancements: Their influence on contemporary corporate management methods and approaches. Multidiscip Rev [Internet]. 2024 Jun 12 [cited 2024 Dec 27];7:2024spe026. Available from: https://doi.org/10.31893/multirev.2024spe026

14. Tsekhmister Y, Yakovenko O, Miziuk V, Sliusar A, Pochynkova M. The Effect of Online Education on the Teachers' Working Time Efficiency. JCT. 2022 Sep 15;11(6):44. doi: 10.5430/jct.v11n6p44

15. Podila LM, Bandreddi JP, Campos JI, Niyaz Q, Yang X, Trekles A, et al. Practice-Oriented Smartphone Security Exercises for Developing Cybersecurity Mindset in High School Students. In: 2020 IEEE International Conference on Teaching, Assessment, and Learning for Engineering (TALE) [Internet]. Takamatsu, Japan: IEEE; 2020 [cited 2024 Dec 12]. p. 303–10. Available from: https://ieeexplore.ieee.org/document/9368440/

16. Vovchenko O, Leonova I, Soroka I, Klymenko I, Tsekhmister Y. The Impact of Emotional Intelligence on

the Academic Performance of Students with Intellectual Disabilities in Inclusive Education. J Intellect Disabl Diagn Treat. 2022 Aug 31;10(4):187–96. doi: 10.6000/2292-2598.2022.10.04.4

17. Rahman NAA, Sairi IH, Zizi NAM, Khalid F. The Importance of Cybersecurity Education in School. IJIET. 2020;10(5):378–82. doi: 10.18178/ijiet.2020.10.5.1393

18. Fullwood C. Online Support Groups: Enhancing the User Experience with Cyber-Psychological Theory. In: Attrill A, Fullwood C, editors. Applied Cyberpsychology [Internet]. London: Palgrave Macmillan UK; 2016 [cited 2024 Dec 12]. p. 106–22. Available from: http://link.springer.com/10.1057/9781137517036_7

19. Jusić M. Lessons from cyberpsychology that educators should be reminded of. DHS-Društvene i humanističke studije: časopis Filozofskog fakulteta u Tuzli. 2023;22(22):567–592.

20. McDermott CD, Jeannelle B, Isaacs JP. Towards a Conversational Agent for Threat Detection in the Internet of Things. In: 2019 International Conference on Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA) [Internet]. Oxford, United Kingdom: IEEE; 2019 [cited 2024 Dec 12]. p. 1–8. Available from: https://ieeexplore.ieee.org/document/8899580/

21. Peni NRN, Dewi DAK. Development research framework for designing functions class using desmos. FeD. 2023 Nov 9;3(4):73–94. https://doi.org/10.57125/FED.2023.12.25.05

22. Bielialov T, Vlasiuk T, Vergun A, Kononenko A, Chernysh O. Formation of a graduate system for assessing professional activities in the entrepreneurship education system. JEE. 2019;22:1–8.

23. Borysiuk I, Haioshko OB, Korniichuk O, Tsekhmister Y, Demianchuk M. Alternative Approaches to Clinical Practice in Medical Education During the Covid-19 Pandemic. JCT. 2022 Feb 10;11(2):75. doi: 10.5430/jct.v11n2p75

24. UNICEF Ukraine [Internet]. Psychological support project “PORUCH” launched in Ukraine; 2022 Mar 22; [cited 2024 Dec 12]. Available from: https://www.unicef.org/ukraine/press-releases/poruch

25. Shevchuk I, Filippova L, Krasnova A, Bazyl O. Virtual Pedagogy: Scenarios for Future Learning with VR and AR Technologies. Futurity Education. 2023 Nov 5;95–117. doi: 10.57125/FED.2023.12.25.06

26. Kumar P, Tandon U. Factors Impacting Educators’ Intention Towards E-Learning Adoption. ECS Trans. 2022 Apr 24;107(1):6561–8. doi: 10.1149/10701.6561ecst

27. Androsova N. Digital Opportunities for the Development of Inclusive Education in Primary School in Ukraine: A Teacher’s Experience. ELIJ. 2023 Mar 25;1(1):4–21. doi: 10.57125/ELIJ.2023.03.25.01

28. Semenets-Orlova I, Klochko A, Shkoda T, Marusina O, Tepliuk M. Emotional Intelligence as the Basis for the Development of Organizational Leadership During the Covid Period (Educational Institution Case). EEA [Internet]. 2021 May 29 [cited 2024 Dec 12];39(5). Available from: http://ojs.ual.es/ojs/index.php/eea/article/view/5074

29. Kalmykova O. Ukraine, Russia, and International Law: Occupation, Armed Conflict and Human Rights. Law, Business and Sustainability Herald. 2022;2(2):4–10.

30. Martínez-Ferrer B, León-Moreno C, Musitu-Ferrer D, Romero-Abrio A, Callejas-Jerónimo J, Musitu-Ochoa G. Parental Socialization, School Adjustment and Cyber-Aggression among Adolescents. IJERPH. 2019 Oct 19;16(20):4005. doi: 10.3390/ijerph16204005

31. Bulavko GV, Davidenko NA, Ishchenko AA, Studzinsky SL, Shkavro AG. Peculiarities of the photovoltaic properties of films based on photoconducting polymer and organic dye in samples with free surfaces and between electric contacts. Tech Phys Lett [Internet]. 2015 Feb [cited 2024 Dec 28];41(2):191-4. Available from: https://doi.org/10.1134/s1063785015020182

32. Amankwa E. Relevance of Cybersecurity Education at Pedagogy Levels in Schools. JIS. 2021;12(04):233–49. doi: 10.4236/jis.2021.124013

33. Romero-Carazas R. Collection Management Model for Late Payment Control in the Basic Education Institutions. Edu - Tech Enterprise 2024;2:12–12. https://doi.org/10.71459/edutech202412.

34. Carrasco MÁA, Apaza VTT. Budget execution of public expenditure of the municipalities. Edu - Tech Enterprise 2024;2:10–10. https://doi.org/10.71459/edutech202410.

35. Jacinto-Alvaro J, Casco RJE, Macha-Huamán R. Social networks as a tool for brand positioning. Edu - Tech Enterprise 2024;2:9–9. https://doi.org/10.71459/edutech20249.

36. Tsekhmister Y, Konovalova T, Tsekhmister B. Using behavioral analytics to personalize learning experiences in digital medical education: a case study. Academia. 2023 Oct 23;83-103 Σελίδες. doi: 10.26220/aca.4543

37. Rakhimov T. Research on moral issues related to the use of artificial intelligence in modern society. Futurity Philosophy. 2023 Jun 30;30–43. doi: 10.57125/FP.2023.06.30.03

38. Canetti D, Gross ML, Waismel-Manor I. Immune from Cyberfire? In: Allhoff F, Henschke A, Strawser BJ, editors. Binary Bullets [Internet]. Oxford University Press; 2016 [cited 2024 Dec 12]. p. 157–76. Available from: https://academic.oup.com/book/10515/chapter/158423481

39. Bui NH, Pasalich DS. Insecure Attachment, Maladaptive Personality Traits, and the Perpetration of In-Person and Cyber Psychological Abuse. J Interpers Violence. 2021 Mar;36(5–6):2117–39. doi: 10.1177/0886260518760332

40. Tsekhmister Y. Effectiveness of Blended Learning in Biomedical Engineering: A Meta-Analysis. J High Educ Theory Pract [Internet]. 2023 Mar 25 [cited 2024 Dec 28];23(5). Available from: https://doi.org/10.33423/jhetp.v23i5.5976

FINANCING

The authors did not receive financing for the development of this research.

CONFLICT OF INTEREST

The authors declare that there is no conflict of interest.

AUTHORSHIP CONTRIBUTION

Conceptualization: Svitlana Khadzhyradieva, Marianna Todorova, Sergii Staikutsa, Liudmyla Tsybukh, Alla Lukiianchuk.

Methodology: Svitlana Khadzhyradieva, Marianna Todorova, Sergii Staikutsa, Liudmyla Tsybukh, Alla Lukiianchuk.

Research: Svitlana Khadzhyradieva, Marianna Todorova, Sergii Staikutsa, Liudmyla Tsybukh, Alla Lukiianchuk.

Drafting - original draft: Svitlana Khadzhyradieva, Marianna Todorova, Sergii Staikutsa, Liudmyla Tsybukh, Alla Lukiianchuk.

Writing - proofreading and editing: Svitlana Khadzhyradieva, Marianna Todorova, Sergii Staikutsa, Liudmyla Tsybukh, Alla Lukiianchuk.