Security of Infocommunication Systems and Internet of Things

2026 Vol 4, No 1

https://doi.org/10.31861/sisiot2026.1.01001

Received 30 October 2025; revised 12 March 2026; accepted 01 June 2026; published 30 June 2026

Artificial Intelligence Assistants in Digital Learning Environments and Cybersecurity Challenges

Inna Rozlomii[1,3], Andrii Yarmilko[2,*] and Serhii Naumenko[3]

[1]Department of Information Security and Computer Engineering, Cherkasy State Technological University, Cherkasy, Ukraine
[2]Department of Automated Systems Software, Bohdan Khmelnytsky National University of Cherkasy, Cherkasy, Ukraine
[3]Departmet of Information Technology, Bohdan Khmelnytsky National University of Cherkasy, Cherkasy, Ukraine

*Corresponding author (E-mail: a-ja@vu.cdu.edu.ua)

ABSTRACT Integration of Artificial Intelligence (AI) Assistants into digital learning environments is becoming an essential part of modern educational processes. The use of AI assistants enables personalized learning that takes into account the individual needs of students, enhances communication efficiency between students and instructors, and automates routine administrative tasks. As a result, students gain access to adaptive learning materials, timely support, and valuable educational resources, significantly improving their learning experience and outcomes. This approach fosters deeper student engagement in the learning process, making education more interactive and convenient for all participants. However, the implementation of AI assistants in educational processes is accompanied by numerous cybersecurity challenges, particularly concerning data privacy protection. The article provides an in-depth examination of the risks associated with using AI technologies in learning environments. It analyzes existing technological and organizational approaches to minimizing these risks. Technological approaches include the use of advanced data encryption methods, multi-factor authentication, intrusion detection and prevention systems (IDS/IPS), and regular security audits. These measures are aimed at enhancing the protection of AI systems from potential cyberattacks and reducing the risk of data compromise. Organizational approaches involve developing security policies for users, conducting training sessions on cyber hygiene, and regularly informing them about current cyber threats. This helps foster a culture of cybersecurity among students and educators, reducing the likelihood of successful social engineering attacks. The article emphasizes the need for developing comprehensive cybersecurity strategies that consider the specific operations of AI assistants. Implementing such strategies is critically important for creating a secure digital learning environment where AI technologies are used. The proposed approaches can serve as a foundation for developing effective data protection strategies and promoting the safe integration of innovative technologies into digital learning environments.

KEYWORDS AI assistants, digital learning environments, cybersecurity, data encryption, intrusion detection.

I. INTRODUCTION

Artificial Intelligence (AI) assistants are becoming an increasingly integrated part of digital learning environments, which are an essential component of modern education [1]. Their use opens up new opportunities for optimizing the learning process, providing individualized approaches to education, automating administrative tasks, and offering timely support to students [2]. Tools such as chatbots, virtual assistants, and adaptive learning systems are already being actively employed in educational institutions to enhance the quality of education and increase learning efficiency. These tools allow for the customization of learning materials according to the needs of each student, supporting personalized learning and increasing engagement in the learning process [3].

The use of AI assistants in education also has significant potential for automating routine tasks, such as grading assignments, creating class schedules, or providing instant feedback to students [4]. This allows educators to focus more on meaningful interactions with students, preparing educational materials, and developing new teaching methods. Additionally, AI assistants can serve as crucial tools in supporting the learning process by facilitating the organization of remote or hybrid learning, which is particularly relevant in the face of global challenges such as pandemics or other crisis situations [5].

However, despite the significant advantages of implementing AI technologies in educational processes, there are several risks associated with their use [6]. The primary concerns are related to data privacy and cybersecurity. AI assistants typically require access to large amounts of personal information from students and educators, which can lead to vulnerabilities regarding data storage and unauthorized access. Moreover, the algorithms used in AI systems can be subject to manipulation or cyberattacks, which may negatively impact the quality of the learning process and compromise the security of the educational environment [7].

The purpose of this article is to analyze the cybersecurity challenges that arise during the implementation and use of AI assistants in digital learning environments.

Achieving this objective involves solving the following research tasks:

- analyzing current approaches to the implementation of AI assistants in digital learning environments and identifying the associated cybersecurity challenges;
- determining the main threats to the confidentiality, integrity, and availability of educational data when AI assistants are used;
- developing a generalized risk assessment model that

considers the probability, impact, and controllability of cybersecurity threats;

- substantiating technological and organizational approaches aimed at reducing cybersecurity risks and improving the protection of digital learning environments.

II. BACKGROUND OF RESEARCH

The issue of implementing artificial intelligence assistants is gaining increasing attention in academic circles, as evidenced by numerous studies in this field [8]. This is reflected in works dedicated to exploring the use of AI assistants in digital learning environments, their impact on the quality of education, as well as the challenges related to ensuring cybersecurity and protecting personal data. For instance, in [9], the authors examine the role of AI assistants in enhancing the learning process, emphasizing the benefits of personalized learning approaches and the automation of routine tasks. They also stress the importance of protecting confidential data in the interaction between students and such assistants.

Another study [10] focuses on analyzing the security risks associated with the use of AI assistants, particularly cyber threats related to the potential for unauthorized access to personal data or manipulation of learning algorithms. The authors propose the application of cryptographic methods and technologies to mitigate these risks but note that such approaches require further research and development. In [11], the issue of regulatory frameworks for data protection in digital learning environments that utilize AI assistants is addressed. An important aspect of this work is the analysis of European standards and recommendations for ensuring privacy and information security in educational institutions.

Researchers also highlight the social and ethical aspects of AI use in educational processes. For example, [12] discusses the ethical use of artificial intelligence and the challenges associated with the responsibility for data preservation and processing. The authors of [13] emphasize the need for a comprehensive approach to developing security policies that encompass both technological and social aspects.

Despite the considerable number of studies devoted to AI assistants in education, several important research gaps remain. Existing publications mainly focus either on educational effectiveness or on general cybersecurity recommendations without providing an integrated methodology for quantitative cybersecurity risk assessment. In particular, insufficient attention has been paid to combining technological protection mechanisms with organizational security measures within a unified evaluation framework. Moreover, most existing studies do not propose formal mathematical models that enable the prioritization of cybersecurity threats according to their probability, impact, and controllability. Another limitation concerns the lack of practical recommendations that simultaneously consider the security requirements of AI assistants and the operational characteristics of digital learning environments. These unresolved issues motivate the development of the proposed risk assessment model and the comprehensive cybersecurity approaches presented in this study.

III. RESEARCH METHODOLOGY

The primary objectives of the methodology are to identify data privacy risks, assess the vulnerabilities of AI systems, and develop measures to enhance cybersecurity in educational institutions. The research methodology includes several stages aimed at analyzing the cybersecurity challenges associated with the implementation of AI assistants in digital learning environments. The research methodology involves the following stages:

- Analysis of current security challenges. Identifying the main risks associated with the use of AI assistants in learning environments, such as unauthorized data access, DoS/DDoS cyberattacks, phishing, and social engineering.
- Assessment of data privacy risks. Detecting vulnerabilities in the storage and processing of student and educator data.
- Development of technological and organizational approaches. Implementing secure programming practices and training AI models, using cryptographic methods such as data encryption, intrusion detection systems, developing cybersecurity policies for users, raising awareness through cyber hygiene training, and establishing incident response protocols.

IV. THE ROLE AND IMPACT OF AI ASSISTANTS IN DIGITAL LEARNING ENVIRONMENTS

AI assistants play a crucial role in modernizing educational systems by providing innovative approaches to learning, automating administrative tasks, and enhancing interactions between students and educators. This section explores the types of AI assistants, their successful implementation in educational institutions, and their technological features.

AI assistants can be classified into several types based on their functions and use in educational processes:

- Chatbots – the most common type of AI assistant, which automates communication with students [14]. Chatbots can answer frequently asked questions, coordinate class schedules, and send deadline reminders. They are integrated into Learning Management Systems (LMS) like Moodle or Canvas.
- Virtual Assistants – AI tools that help with task management, time organization, providing access to learning resources, and offering real-time support to students [15]. They utilize Natural Language Processing (NLP) to interact with users [16].
- Adaptive Learning Systems (ALS) – AI algorithms in these systems tailor learning materials to the needs of each student by analyzing their performance and learning pace [17]. This ensures a personalized approach to learning and enhances the efficiency of the educational process.

Successful examples of AI assistant implementation in educational institutions demonstrate the effectiveness of these technologies. For instance, Georgia State University introduced a virtual assistant named "Pounce" to support communication with students [18]. This chatbot helps students with questions about admissions, financial aid, class schedules, and more. As a result of

implementing the bot, the university reduced misunderstandings and improved student interaction.

Another example is the use of adaptive learning systems in schools and universities, such as the Knewton platform, which allows for the customization of learning materials to meet students' needs, providing a personalized learning experience [19]. These systems enhance the learning process's efficiency by offering educational resources that match students' knowledge levels and learning speeds.

The technological features of AI assistants include the use of Machine Learning (ML), NLP, cloud computing, and Application Programming Interfaces (APIs). Specifically, ML algorithms enable systems to learn from large datasets and improve their recommendations over time. NLP facilitates interaction with users through natural language, making communication easier and more effective.

Cloud computing allows for the scaling of AI solutions, storing large amounts of data, and ensuring their accessibility from anywhere in the world. Additionally, using APIs enables the integration of AI assistants with other LMS, such as Moodle or Canvas, making the learning process more seamless and convenient.

Fig. 1 presents a chart demonstrating the effectiveness of implementing various types of AI assistants in educational institutions, based on their functionality and level of automation. The quantitative values presented in Fig. 1 were obtained through an expert-based comparative assessment of AI assistant categories according to two evaluation criteria: functional capabilities and degree of process automation. The assessment employed a normalized five-level scoring procedure, after which the obtained scores were transformed into percentage values to simplify visual comparison. The presented values therefore illustrate the relative performance of the considered AI assistant categories rather than statistical measurements collected from a particular educational institution. Fig. 1 highlights the differences in functionality and automation between chatbots, virtual assistants, and adaptive learning systems.

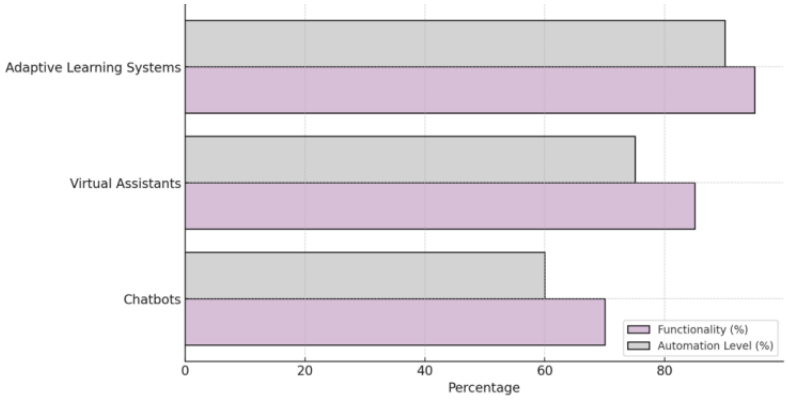

FIG. 1. Chart of AI assistants implementation effectiveness.

Specifically, chatbots are effective for automating routine communications, such as answering common student questions. Virtual Assistants (VAs) have a higher level of functionality and automation, enabling them to assist with more complex tasks, such as organizing learning and managing schedules. ALS exhibit the highest levels of both functionality and automation. They are also capable of tailoring learning materials to meet individual student needs, providing a highly personalized approach to education.

Fig. 2 presents a risk and security model that illustrates key aspects to consider when implementing AI assistants, particularly regarding data privacy, protection against cyberattacks, and ensuring system reliability.

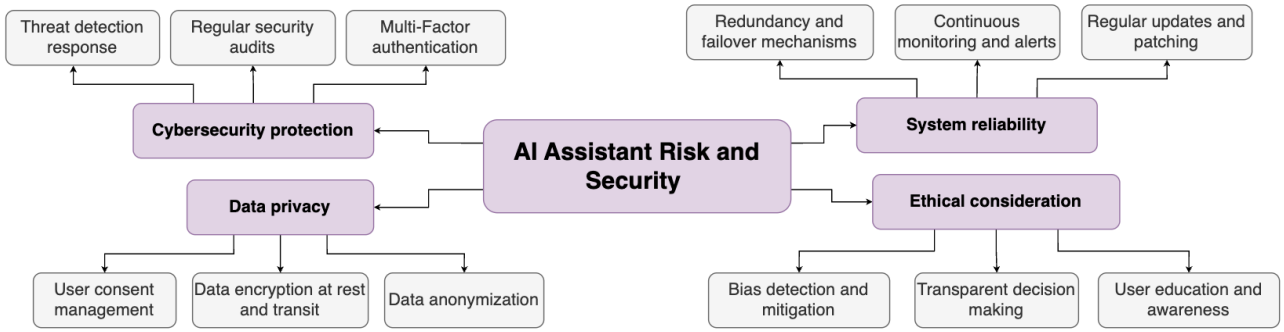

FIG. 2. AI assistant risk and security model.

This model illustrates the key aspects of risks and security measures that are crucial to consider when implementing AI assistants in educational processes to ensure their safety and effectiveness. Specifically, one of the main aspects is Data Privacy. This involves using data encryption methods to protect information during transmission and storage, as well as access control to sensitive data based on user roles. This helps minimize the risks of unauthorized access to important information and ensures its confidentiality in educational environments.

Another important aspect is Protection Against Cyberattacks. Here, Intrusion Detection Systems (IDS) are employed to detect and prevent unauthorized access and threats. Regular Security Audits also play a crucial role, providing ongoing assessment of system security to timely identify vulnerabilities and apply appropriate measures to address them.

The third key aspect of the risk and security model concerns System Reliability. This includes Backup and Recovery mechanisms that ensure system continuity in the event of failures or attacks. Additionally, Redundancy Mechanisms are used to provide extra resources to support system reliability and availability.

A. Cybersecurity challenges in using AI assistants. When implementing AI assistants in educational institutions, various cybersecurity challenges arise related to data privacy, protection against cyberattacks, and ensuring system reliability. Table 1 presents the main threats and their impact on learning environments.

Table 1 summarizes the main security threats that may arise during the implementation of AI assistants in educational institutions, including their impact and risk mitigation measures. Unauthorized access to data and social engineering are particularly dangerous threats, as they can lead to the leakage of confidential information and cause significant damage to the institution's reputation. Implementing multi-factor authentication, data encryption, and regular cybersecurity awareness training can significantly reduce these risks.

TABLE 1. Main security threats in using AI assistants in educational environments.

Threat	Description	Impact	Mitigation measures
Unauthorized access	Unauthorized access to sensitive data (e.g., personal data)	Data breaches, identity theft, reputational damage	Multi-factor authentication, data encryption
Social Engineering	Manipulation to gain access to information or systems	Data loss, malware infection	Cyber hygiene training, phishing simulations
Man-in-the-Middle (MITM)	Intercepting communications between users and AI systems	Data compromise, loss of communication integrity	SSL/TLS encryption, VPN
AI Algorithm Vulnerability	Weaknesses in AI algorithms that can be exploited	AI system malfunction, data manipulation	Strong algorithms, regular updates and testing
Denial of Service (DoS/DDoS)	Overloading systems to cause service disruptions	Service unavailability, disruption of learning	DDoS protection, network monitoring

B. Privacy and personal data protection risks. Privacy and personal data protection risks are among the key issues when implementing AI assistants in educational institutions. Major threats, such as unauthorized data access, social engineering, and insider attacks, can lead to significant losses of confidential information and violations of privacy for students and faculty. For instance, unauthorized access to data could result in the theft of personal information, which might be used for phishing or other fraudulent activities. Similarly, social engineering can lead to system infections with malware, jeopardizing data integrity or causing data leaks.

To effectively counter these risks, comprehensive measures are needed, including data encryption, access control, intrusion detection systems, and regular security audits. Additionally, educating staff and students about cybersecurity hygiene and increasing their awareness of current cyber threats are crucial.

To assess the risk level during the implementation of AI assistants in educational institutions, a mathematical model is proposed, taking into account the probability of a threat (P) and its impact (I) on the system (1).

$$R = \sum_{i=1}^{n} P_i \cdot I_i \cdot \left(1 - \frac{C_i}{M_i}\right) \cdot S_i, \qquad (1)$$

where R – the overall risk level; P_i – the probability of threat i occurring; I_i – the impact of threat i on the system; C_i – the level of control over threat i; M_i – the maximum level of control that can be applied; S_i – the importance factor of threat i.

The proposed model evaluates the overall cybersecurity risk as a weighted aggregation of individual threats while simultaneously considering the effectiveness of implemented security controls. The probability component reflects the likelihood of a specific threat occurring within the educational environment, whereas the impact component characterizes the expected consequences for confidentiality, integrity, and availability of educational data. The control coefficient represents the effectiveness of existing technological and organizational protection measures and proportionally decreases the contribution of mitigated threats to the final risk value. Finally, the importance coefficient enables prioritization of threats according to their criticality for AI-assisted educational services. Such an approach supports comparative analysis of different cybersecurity scenarios and assists decision-makers in selecting appropriate protection measures.

V. TECHNOLOGICAL AND ORGANIZATIONAL APPROACHES TO ENHANCING CYBERSECURITY

Given the challenges and risks associated with implementing AI assistants in educational institutions, it is critically important to develop both technological and organizational approaches to ensure an adequate level of cybersecurity.

- Technological Approaches. One of the most crucial technological approaches is employing secure programming practices and training AI models. This includes using robust cryptographic methods for data protection, such as AES-256 for data encryption in transit and at rest, and implementing SSL/TLS security protocols for network communications. Additionally, continuous updating and testing of AI models are necessary to identify potential vulnerabilities and enhance their resilience against attacks. The use of lightweight encryption methods that provide reliable protection while optimizing

computational resource usage is also vital, especially in resource-intensive environments like mobile or embedded systems used by AI assistants [20].

- Another important approach is the deployment of IDS and Intrusion Prevention Systems (IPS), which monitor network activity and detect suspicious actions in real-time. This enables rapid threat response and minimizes the risk of successful attacks. Regular security audits are also a key aspect for evaluating the current security status of systems and identifying potential gaps that could be exploited by malicious actors. Additionally, implementing container orchestration systems [21] for managing AI assistants in various environments is significant. Containerization allows for the isolation of different system components, controlling resource access and minimizing risks associated with software vulnerabilities [22]. Container orchestration also facilitates quick updates without disrupting the entire system, thereby enhancing attack resilience and ensuring the continuity of the educational process.

- Organizational Approaches. At the organizational level, it is crucial to develop security policies and guidelines for faculty and students regarding the use of AI assistants. These policies should include password management rules, measures to prevent phishing attacks, incident reporting protocols, and recommendations for the secure use of AI systems. Increasing user awareness of cybersecurity through training workshops, seminars, and simulated testing also plays a significant role. This helps build a culture of security among students and faculty, which, in turn, reduces the risks of successful social engineering attacks, such as phishing or social engineering.

The obtained results demonstrate that the highest cybersecurity effect can be achieved only through the combined implementation of technological and organizational protection measures. While technological mechanisms reduce the probability of successful cyberattacks by strengthening system resilience, organizational measures significantly decrease risks associated with human factors, including phishing and social engineering. The proposed risk assessment model enables educational institutions to prioritize cybersecurity investments according to the estimated threat levels and available protection resources. Consequently, the proposed framework supports more informed cybersecurity management decisions and contributes to improving the overall resilience of AI-assisted digital learning environments.

VI. CONCLUSION

The article examines the role and impact of AI assistants in modern educational systems, as well as the challenges and risks associated with their implementation. The analysis indicates that while AI assistants significantly enhance the educational process and interaction between students and educators, they also introduce new cybersecurity threats.

The study's findings show that implementing AI assistants in educational institutions substantially increases the effectiveness of the learning process but comes with numerous cybersecurity challenges and risks. The analysis identified key threats such as unauthorized data access, MITM attacks, social engineering, vulnerabilities in AI algorithms, and DoS/DDoS attacks.

The proposed risk assessment approaches, including the developed mathematical model, helped identify critical threats and determine which aspects to focus on for risk mitigation. The use of the risk model in practical scenarios aided in identifying necessary technological measures, such as data encryption, multi-factor authentication, IDS/IPS implementation, and regular security audits.

Additionally, the study emphasized the importance of organizational measures, such as user training in cybersecurity hygiene and the development of comprehensive security policies for faculty and students using AI assistants. These measures contribute to building a security culture within the educational environment, helping to prevent social engineering attacks and reducing the likelihood of successful cyberattacks.

The scientific contribution of this study lies in the proposed generalized cybersecurity risk assessment model for AI-assisted digital learning environments, which combines threat probability, potential impact, control level, and threat importance within a unified evaluation framework. The practical significance of the obtained results consists in providing educational institutions with structured technological and organizational recommendations that can support the design of secure AI-assisted learning infrastructures, improve cybersecurity decision-making, and reduce the likelihood of successful cyberattacks.

Overall, the proposed approaches can serve as a foundation for developing effective cybersecurity strategies in educational institutions using AI assistants and promoting the safe integration of innovative technologies into educational processes. Further research could focus on evaluating new data protection methods, implementing AI for threat detection, and developing cybersecurity standards for educational institutions.

ACKNOWLEDGMENT

This research was funded by the Ministry of Education and Science of Ukraine under grant 0125U000637.

AUTHOR CONTRIBUTIONS

I.R. – conceptualization, methodology; A.Y. – validation, formal analysis; I.R., S.N. – investigation; I.R., A.Y., S.N. – writing-original draft preparation, writing-review and editing.

COMPETING INTERESTS

The authors declare no competing interests.

REFERENCES

[1] E. Dimitriadou and A. Lanitis, “A critical evaluation, challenges, and future perspectives of using artificial intelligence and emerging technologies in smart classrooms,” *Smart Learn. Environ.*, vol. 10, no. 1, p. 12, 2023, doi: 10.1186/s40561-023-00231-3.

[2] A. Alam, “Employing adaptive learning and intelligent tutoring robots for virtual classrooms and smart campuses: Reforming education in the age of artificial intelligence,” in R. N. Shaw, S. Das, V. Piuri, and M. Bianchini, Eds., *Adv. Comput. Intell. Technol., Lecture Notes in Electrical Engineering*, vol. 914. Singapore: Springer, 2022, pp. 395–406, doi: 10.1007/978-981-19-2980-9_32.

[3] B. Cope, M. Kalantzis, and D. Searsmith, “Artificial intelligence for education: Knowledge and its assessment in AI-enabled learning ecologies,” *Educ. Philos. Theory*, vol. 53, no.

12, pp. 1229–1245, 2021, doi: 10.1080/00131857.2020.1728732.
[4] V. Kuleto et al., "Exploring opportunities and challenges of artificial intelligence and machine learning in higher education institutions," *Sustainability*, vol. 13, no. 18, p. 10424, 2021, doi: 10.3390/su131810424.
[5] M. Hooda, C. Rana, O. Dahiya, A. Rizwan, and M. S. Hossain, "Artificial intelligence for assessment and feedback to enhance student success in higher education," *Math. Problems Eng.*, vol. 2022, no. 1, p. 5215722, 2022, doi: 10.1155/2022/5215722.
[6] A. Alam, "Possibilities and Apprehensions in the Landscape of Artificial Intelligence in Education," in *Proc. 2021 Int. Conf. Comput. Intell. Comput. Appl. (ICCICA)*, Nagpur, India, 2021, pp. 1–8, doi: 10.1109/ICCICA52458.2021.9697272.
[7] A. Maedche et al., "AI-based digital assistants: Opportunities, threats, and research perspectives," *Bus. Inf. Syst. Eng.*, vol. 61, no. 4, pp. 535–544, 2019, doi: 10.1007/s12599-019-00600-8.
[8] M. L. Owoc, A. Sawicka, and P. Weichbroth, "Artificial intelligence technologies in education: Benefits, challenges and strategies of implementation," in M. L. Owoc and M. Pondel, Eds., *Artif. Intell. Knowl. Manage., IFIP Advances in Information and Communication Technology*, vol. 599, Cham, Switzerland: Springer, 2021, pp. 37–58, doi: 10.1007/978-3-030-85001-2_4.
[9] S. F. Ahmad, M. M. Alam, M. K. Rahmat, M. S. Mubarik, and S. I. Hyder, "Academic and administrative role of artificial intelligence in education," *Sustainability*, vol. 14, no. 3, p. 1101, 2022, doi: 10.3390/su14031101.
[10] G. J. Hwang, H. Xie, B. W. Wah, and D. Gašević, "Vision, challenges, roles and research issues of Artificial Intelligence in Education," *Comput. Educ.: Artif. Intell.*, vol. 1, p. 100001, 2020, doi: 10.1016/j.caeai.2020.100001.
[11] W. Holmes, J. Persson, I. A. Chounta, B. Wasson, and V. Dimitrova, *Artificial Intelligence and Education: A Critical View Through the Lens of Human Rights, Democracy and the Rule of Law*. Strasbourg, France: Council of Europe, 2022, ISBN 978-92-871-9236-3.
[12] A. Aldoseri, K. N. Al-Khalifa, and A. M. Hamouda, "Re-thinking data strategy and integration for artificial intelligence: Concepts, opportunities, and challenges," *Appl. Sci.*, vol. 13, no. 12, p. 7082, 2023, doi: 10.3390/app13127082.
[13] M. Decuypere, E. Grimaldi, and P. Landri, "Introduction: Critical studies of digital education platforms," *Crit. Stud. Educ.*, vol. 62, no. 1, pp. 1–16, 2021, doi: 10.1080/17508487.2020.1866050.
[14] Y. Chen, S. Jensen, L. J. Albert, S. Gupta, and T. Lee, "Artificial intelligence (AI) student assistants in the classroom: Designing chatbots to support student success," *Inf. Syst. Front.*, vol. 25, no. 1, pp. 161–182, 2023, doi: 10.1007/s10796-022-10291-4.
[15] R. Reyes, D. Garza, L. Garrido, V. De la Cueva, and J. Ramirez, "Methodology for the implementation of virtual assistants for education using Google Dialogflow," in L. Martínez-Villaseñor, I. Batyrshin, and A. Marín-Hernández, Eds., *Advances in Soft Computing (MICAI 2019), Lecture Notes in Computer Science*, vol. 11835, Cham, Switzerland: Springer, 2019, pp. 440–451, doi: 10.1007/978-3-030-33749-0_35.
[16] I. Rozlomii, N. Yehorchenkova, A. Yarmilko, and S. Naumenko, "Data protection in the utilization of natural language processors for trend analysis and public opinion: Cryptographic aspect," in *Proc. 2nd Int. Workshop Social Commun. Inf. Act. Digit. Humanities (SCIA-2023)*, Lviv, Ukraine, 2023, pp. 1–11, doi: 10.5281/zenodo.21131868.
[17] T. Kabudi, I. Pappas, and D. H. Olsen, "AI-enabled adaptive learning systems: A systematic mapping of the literature," *Comput. Educ.: Artif. Intell.*, vol. 2, p. 100017, 2021, doi: 10.1016/j.caeai.2021.100017.
[18] K. M. Fuad, "Organizational intelligence in digital innovation: Evidence from Georgia State University," Ph.D. dissertation, Georgia State Univ., Georgia, USA, 2022, doi: 10.31922/Z1BC-1A51.
[19] S. Dutta, S. Ranjan, S. Mishra, V. Sharma, P. Hewage, and C. Iwendi, "Enhancing educational adaptability: A review and analysis of AI-driven adaptive learning platforms," in *Proc. 2024 4th Int. Conf. Innov. Pract. Technol. Manage. (ICIPTM)*, Noida, India, 2024, pp. 1–5, doi: 10.1109/ICIPTM59628.2024.10563448.
[20] I. Rozlomii, A. Yarmilko, and S. Naumenko, "Data security of IoT devices with limited resources: Challenges and potential solutions," in *Proc. doors 2024: 4th Edge Computing Workshop*, Zhytomyr, Ukraine, CEUR Workshop Proceedings, vol. 3666, pp. 85–96, 2024, doi: 10.55056/ceur-ws.org/Vol-3666/paper13.pdf.
[21] Y. V. Voievodin and I. O. Rozlomii, "Advanced software framework for comparing balancing strategies in container orchestration systems," in *Proc. doors 2024: 4th Edge Computing Workshop*, Zhytomyr, Ukraine, CEUR Workshop Proceedings, vol. 3666, pp. 60–69, 2024, doi: 10.55056/ceur-ws.org/Vol-3666/paper09.pdf.
[22] Y. Voievodin and I. Rozlomii, "Application Security Optimization in Container Orchestration Systems Through Strategic Scheduler Decisions," in *Proc. CPITS-2024: Cybersecurity Providing in Information and Telecommunication Systems*, Kyiv, Ukraine, CEUR Workshop Proceedings, vol. 3654, pp. 471–478, 2024, doi: 10.5281/zenodo.21132895.

Inna Rozlomii

PhD in Information Technologies, Docent, Associate Professor Department of Information Security and Computer Engineering, Cherkasy State Technological University. Research interests: Internet of Things, lightweight cryptography, cyber-physical systems. Author of more than 150 publications.

ORCID ID: 0000-0001-5065-9004

Andrii Yarmilko

PhD in Information Technologies, Docent, Associate Professor at Department of Automated Systems Software, Bohdan Khmelnytsky National University of Cherkasy. Research interests: computer vision and pattern recognition, industrial internet of things, human-machine interaction, information security and dependability of embedded systems. Author of more than 120 publications.

ORCID ID: 0000-0003-2062-2694

Serhii Naumenko

PhD Student at Department of Information Technology, Bohdan Khmelnytsky National University of Cherkasy. Research interests: Internet of Things, lightweight cryptography, cyber-physical systems. Author of more than 70 publications.

ORCID ID: 0000-0002-6337-1605

AI-асистенти у цифрових навчальних середовищах та виклики кібербезпеки

Інна Розломій[1,3], Андрій Ярмілко[2,*], Сергій Науменко[3]

[1]Кафедра інформаційної безпеки та комп'ютерної інженерії, Черкаський державний технологічний університет, Черкаси, Україна
[2]Кафедра програмного забезпечення автоматизованих систем, Черкаський національний університет імені Богдана Хмельницького, Черкаси, Україна
[3]Кафедра інформаційних технологій, Черкаський національний університет імені Богдана Хмельницького, Черкаси, Україна

*Автор-кореспондент (Електронна адреса: a-ja@vu.cdu.edu.ua)

АНОТАЦІЯ Інтеграція асистентів штучного інтелекту (AI) у цифрові навчальні середовища стає важливою частиною сучасних освітніх процесів. Використання AI асистентів дозволяє забезпечити персоналізоване навчання, що враховує індивідуальні потреби студентів, підвищити ефективність комунікації між студентами та викладачами, а також автоматизувати рутинні адміністративні завдання. Завдяки цьому студенти отримують доступ до адаптивних навчальних матеріалів, своєчасної підтримки та корисних навчальних ресурсів, що значно покращує їх освітній досвід і результати навчання. Такий підхід сприяє глибшому залученню студентів до навчального процесу, робить навчання більш інтерактивним і зручним для всіх учасників. Проте, впровадження AI асистентів у навчальні процеси супроводжується численними викликами у сфері кібербезпеки, особливо щодо захисту конфіденційності даних. У статті детально розглянуто ризики, пов'язані з використанням AI технологій у навчальних середовищах. У статті проведено аналіз наявних технологічних та організаційних підходів до мінімізації зазначених ризиків. До технологічних підходів віднесено використання сучасних методів шифрування даних, багатофакторної автентифікації, систем виявлення та запобігання вторгнень, а також проведення регулярних аудитів безпеки. Ці заходи спрямовані на підвищення рівня захищеності AI систем від потенційних кібератак та зменшення ризиків компрометації даних. Організаційні підходи включають розробку політик безпеки для користувачів, проведення навчальних тренінгів з кібергігієни та регулярне інформування про сучасні кіберзагрози. Це дозволяє сформувати культуру кібербезпеки серед студентів та викладачів і зменшити ймовірність успішних соціальних атак. Особливу увагу в статті приділено необхідності розробки комплексних стратегій кібербезпеки, які враховують специфіку роботи AI асистентів. Впровадження таких стратегій є критично важливим для створення безпечного цифрового навчального середовища, де використовуються AI технології. Запропоновані підходи можуть слугувати основою для розробки ефективних стратегій захисту даних і сприяти безпечному впровадженню інноваційних технологій у цифрові навчальні середовища.

КЛЮЧОВІ СЛОВА асистенти AI, цифрові навчальні середовища, кібербезпека, шифрування даних, виявлення вторгнень.