

# Preparing pre-service teachers for the digital era: Cyberethics, cybersafety, and cybersecurity skills as a core AI competency\*

Oleksandr Termenzhy<sup>1,†</sup>, Alla Kozhevnikova<sup>1,†</sup> and Vitalii Susukailo<sup>2,\*,†</sup>

<sup>1</sup> Bohdan Khmelnytsky Melitopol State Pedagogical University, 59 Naukova Mistechka str., 69000 Zaporizhzhya, Ukraine

<sup>2</sup> Lviv Polytechnic National University, 12 Stepana Bandery str., 79000 Lviv, Ukraine

## Abstract

This study explores the emerging concept of AI competency for educators and the integration of cyberethics, cybersafety, and cybersecurity (C3) skills into pre-service teacher education. While international research has advanced in defining and assessing AI literacy and competency, Ukrainian pedagogy is only beginning to adopt these concepts. The study reviews key global frameworks, including the UNESCO AI Competency Framework for Teachers and the AICE Framework by the University of Washington, and compares them with national initiatives in Ukraine. The paper presents the curriculum of the online elective course “Pedagogical Aspects of Using Artificial Intelligence in Secondary Education Institutions”, designed for pre-service mathematics teachers at Bohdan Khmelnytsky Melitopol State Pedagogical University. The course, based on the ADDIE instructional design model, aims to foster responsible AI integration and C3 awareness in education.

## Keywords

artificial intelligence in education, cyberethics, cybersafety, and cybersecurity in teaching, pre-service teacher training, AI literacy, AI competency

## 1. Introduction

As artificial intelligence (AI) continues to reshape the educational landscape, the role of teachers is rapidly evolving. In preparing future educators for the digital era, it is no longer sufficient to focus solely on technical proficiency or digital literacy. Instead, there is a growing need to develop their AI competency that includes ethical awareness, critical thinking, and responsible digital citizenship. Among these, the triad of cyberethics, cybersafety, and cybersecurity (also known as C3) emerges as a foundational pillar of professional preparedness [1].

There is no doubt that pre-service teachers must be equipped not only to integrate AI tools into their pedagogical practice but also to navigate and model safe, ethical, and secure behavior in increasingly complex digital environments. These competencies are essential for fostering trust, protecting personal and institutional data, and ensuring equitable access to digital learning. Moreover, they empower teachers to guide students in developing responsible digital habits and resilience against online threats [2–5].

This paper explores the integration of cyberethics, cybersafety, and cybersecurity into teacher education as a core component of AI competency based on the pre-service teacher training at Bohdan Khmelnytsky Melitopol State Pedagogical University (Ukraine). Drawing on current frameworks, international policy trends, and empirical findings, it argues for a systemic approach to embedding these skills into Ukrainian teacher training programs. The aim is to ensure that future educators are not only digitally fluent but also capable of leading the next generation toward a safer and more ethically grounded digital future.

\* CSDP'2025: Cyber Security and Data Protection, July 31, 2025, Lviv, Ukraine

\* Corresponding author.

† These authors contributed equally.

✉ aleksterm@gmail.com (O. Termenzhy); Kozhevnykova\_Alla@mspu.edu.ua (A. Kozhevnikova);

vitalii.a.susukailo@lpnu.ua (V. Susukailo)

ORCID 0009-0005-0792-0103 (O. Termenzhy); 0000-0001-6987-0352 (A. Kozhevnikova); 0000-0003-4431-9964 (V. Susukailo)



© 2025 Copyright for this paper by its authors. Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).

## 2. AI Competency for educators: A conceptual overview

The use of artificial intelligence systems has led to the emergence of new concepts—AI literacy and AI Competency. These concepts are relatively new to Ukrainian pedagogy, and, unlike in international research, studies by domestic scholars devoted to the components, levels, and methods of assessing AI literacy are extremely limited. There is no universally accepted definition of these terms. However, it is important to highlight the foundational contribution of Long & Magerko (2020), who, in their article “What is AI Literacy?”, synthesized existing studies on AI literacy and developed a comprehensive competency-based approach to its formation and assessment. They [6] define AI literacy as “a set of competencies that enables individuals to critically evaluate AI technologies, communicate and collaborate effectively with AI, and use AI as a tool online, at home, and in the workplace.” They see this literacy as a set of 17 skills and as an operational definition.

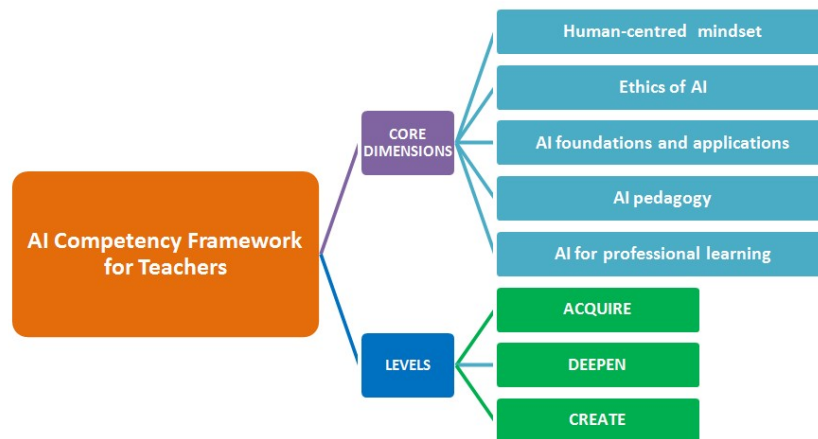
The study (Chiu, Ahmad, Ismailov&Sanusi, 2024) presented the definitions of AI literacy and competency and co-designed the framework with experienced AI teachers. AI literacy is defined as “an individual’s ability to clearly explain how AI technologies work and impact society, as well as to use them in an ethical and responsible manner and to effectively communicate and collaborate with them in any setting. It focuses on knowing (i.e. knowledge and skills)”. AI competency is defined as “an individual’s confidence and ability to clearly explain how AI technologies work and impact society, as well as to use them in an ethical and responsible manner and to effectively communicate and collaborate with them in any setting. They should have the confidence and ability to self-reflect on their AI understanding for further learning. It focuses on how well individuals use AI in beneficial ways” [7].

Currently, there is a growing global effort to develop AI competency frameworks for educators to support the meaningful and ethical integration of artificial intelligence in education. Notable examples include the UNESCO AI Competency Framework for Teachers (AI CFT, 2024) [8], which provides a strategic, human-centered approach to AI in education, and the AI Competency for Educators (AICE) Framework (2025) [9] developed by Colleague AI (University of Washington), which emphasizes practical, observable skills for educators to effectively use AI in instructional settings. These frameworks reflect complementary approaches—from global policy guidance to classroom-level implementation.

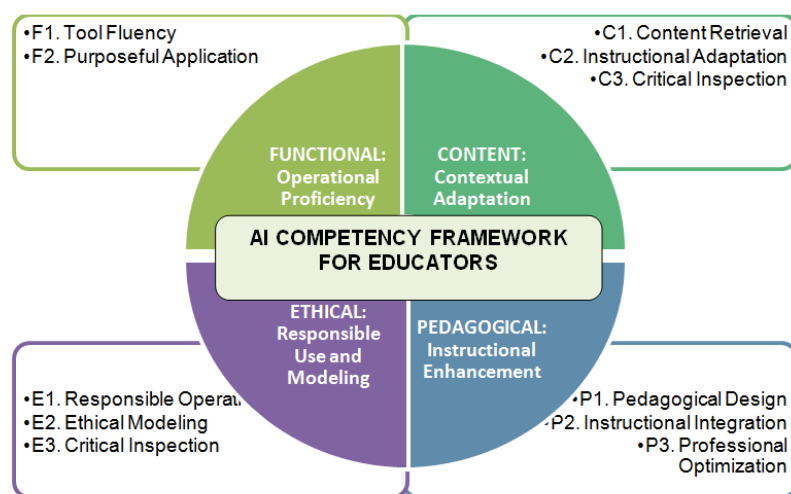
The UNESCO AI CFT is a global, normative model designed to ensure the ethical, safe, and inclusive integration of artificial intelligence in education. It outlines five key dimensions: Human-centered mindset, Ethics of AI, AI foundations and applications, AI pedagogy, and AI for professional learning (Figure 1). Grounded in the Sustainable Development Goals and UNESCO’s ICT-CFT, the framework introduces three progressive levels of competence—Acquire, Deepen, and Create—and is intended for shaping education policy, teacher certification, and international standards.

In contrast, the AICE Framework (2025) developed by Colleague AI is a practical, practice-oriented model that defines AI competency through four interrelated dimensions: Functional (tool fluency), Content (adaptation and critique), Pedagogical (instructional integration), and Ethical (responsible use and modeling) (Figure 2). AICE shifts the focus from knowledge about AI to observable, teachable educator practices. It is designed to support teacher professional growth, self-assessment, micro-credentials, and EdTech development by making AI integration measurable, actionable, and instructionally grounded.

In Ukraine the concept of AI literacy was introduced in 2024 within the framework of the joint project of the Ministry of Education and the Ministry of Digital Transformation of Ukraine titled “Guidelines on Artificial Intelligence for General Secondary Education Institutions”. The working group of Ukrainian researchers defines AI literacy as “understanding by participants of the educational process of the basic principles of responsible use of artificial intelligence systems, possessing the skills to recognize when AI is being used, as well as awareness of its limitations and the risks associated with irresponsible use” [10].



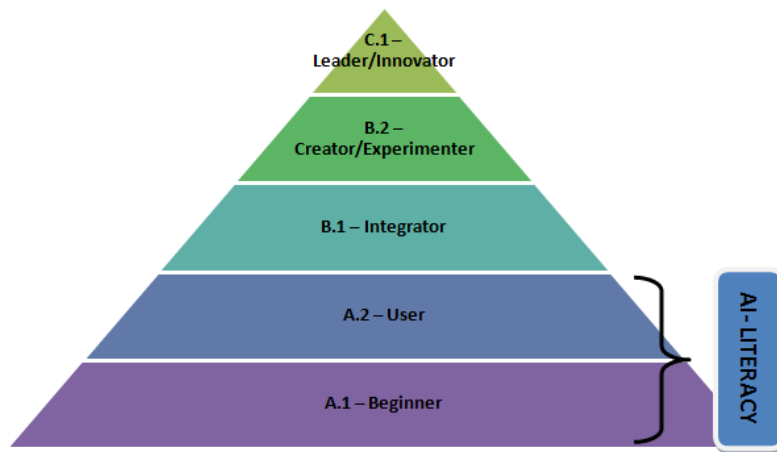
**Figure 1:** AI Competency Framework for Teachers (2024, UNESCO) [8]



**Figure 2:** AI Competency for Educators Framework (2025, University of Washington) [9]

In addition to the concept of AI literacy, Ukrainian educators also introduce the term “AI competency for educators”. This competency is “characterized by the knowledge, skills, and attitudes necessary to understand and effectively use AI in various contexts: understanding the roles of AI in education, using it in pedagogical practice in an ethical and effective way, and the ability to identify AI and its applications” [10]. It is noted that although AI competency is not explicitly defined in the current Professional Teacher Standard in Ukraine [11], it is potentially relevant to the implementation of all professional functions of a teacher and is an integral part of educators’ ICT competence.

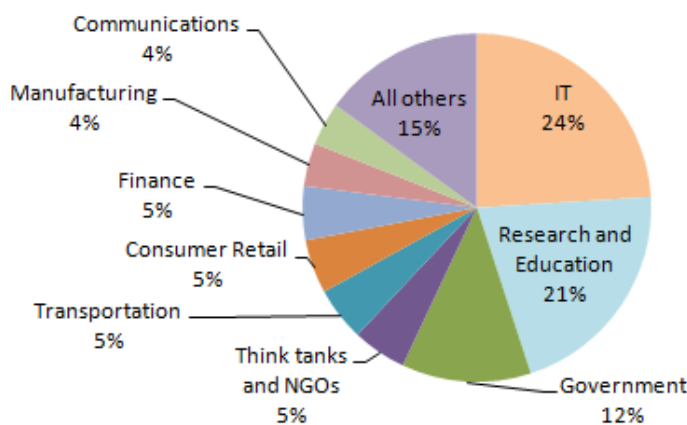
Experts of the Ministry of Education and Science of Ukraine [10] have provided a detailed description of the role and place of AI competency for teachers within the structure of the UNESCO ICT Competency Framework for Teachers [12], and have identified five levels of AI competency for teachers: A.1—Beginner, A.2—User, B.1—Integrator, B.2—Creator/Experimenter, C.—Leader/Innovator. They have also outlined the correlation between the concepts of AI literacy and AI competency (see Figure 3). As the diagram shows, AI literacy constitutes the foundational levels (A.1 and A.2) of AI competency for teachers.



**Figure 3:** Five levels of AI Competence for Teachers (2024, Ministry of Education and Science of Ukraine) [10]

### 3. Integrating cyberethics, cybersafety, and cybersecurity into pre-service teacher education

In 2024, the cybersecurity threat landscape has reached an unprecedented scale and complexity. According to Microsoft Digital Defense Report [13], their systems detect over 600 million cyberattacks every day. Globally, the state of cybersecurity in education remains a growing concern as schools, colleges, and universities become increasingly reliant on digital technologies and online learning platforms. Thus, education and research sector became the second most targeted sector by nation-state threat actors (21% of cyberattacks). In addition to offering intelligence such as research and policy discussions, education and research institutions are often used as testing grounds by threat actors before they pursue their actual targets. Educational institutions are frequent targets of cyberattacks due to the vast amount of sensitive data they handle and often limited cybersecurity infrastructure.



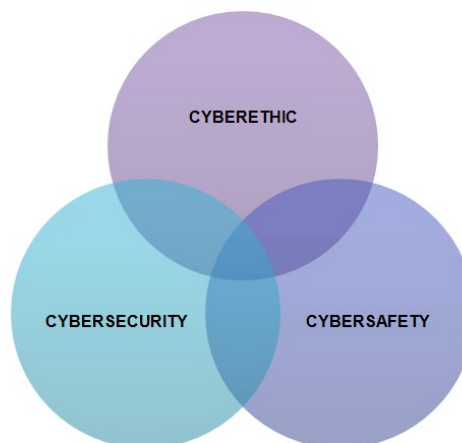
**Figure 4:** Top 10 targeted sectors worldwide from “Microsoft Digital Defense Report: The Foundations and New Frontiers of Cybersecurity” (2024) [13]

This alarming statistic highlights the urgent need to create a **cybersecure educational environment** that can protect students, educators, and institutions from growing digital threats. Consequently, the integration of **cybersecurity awareness and practices** into pre-service teacher training becomes essential. In addition to addressing technical and ethical aspects of cyber education, it is important to consider the role of innovative digital tools in enhancing cybersecurity awareness and skills among pre-service teachers. Recent studies emphasize the importance of

integrated information systems, such as electronic record books, to guarantee the integrity and security of distance learning environments [14]. Moreover, AI-driven approaches for analyzing digital evidence and behavior patterns can support the development of more effective cybersecurity curricula and forensic readiness in educational settings [15]. Intelligent rule-based systems also contribute to the automation of cybersecurity policy enforcement and adaptive control mechanisms within educational infrastructures [16]. The holistic management of information protection, supported by decision support systems, further strengthens institutional resilience against emerging cyber threats [17]. Finally, methodologies for establishing Information Security Management Systems (ISMS) provide essential frameworks for embedding cybersecurity culture and practice into educational institutions [18]. Advancements in secure authentication and authorization services ensure that future educators not only understand cybersecurity principles but can also apply robust user management practices [19]. Additionally, frameworks for information classification aligned with SOC 2 Type II standards help educational organizations maintain compliance and protect sensitive data effectively [20].

Future educators must be equipped not only with pedagogical and digital skills but also with the knowledge and competencies to recognize, prevent, and respond to cyber risks within the school context.

Although learning institutions have been quick to profit from the Internet's gifts, they have been slow to recognize their responsibility to educate their communities about cyberethics, cybersafety, and cybersecurity (Pusey&Sadera, 2011). Cyberethics, cybersafety, and cybersecurity, also known as C3, are interconnected domains focused on responsible and secure technology use [1].



**Figure 5:** C3 Framework: cyberethics, cybersafety, and cybersecurity [21]

**Cyberethics** refers to the moral choices individuals make when using Internet-capable technologies and digital media. Issues related to cyberethics include copyright infringement, online etiquette, hacking, and internet addiction [1]. **Cybersafety** encompasses the actions individuals take to minimize the dangers they may encounter while using Internet-connected technologies. Common cybersafety concerns include online predators, unwanted communications, computer viruses, and spyware. This domain also emphasizes raising awareness about how user behavior can contribute to the spread of malware and the various tactics (such as phishing, pharming, and spoofing) used to deceive individuals online. **Cybersecurity** involves technical measures designed to protect data, identity information, and hardware from unauthorized access or damage [22]. Cybersecurity practices include the use of antivirus software, Internet content filters, firewalls, and secure password protocols.

The rise of artificial intelligence in teaching and administration further amplifies the need for secure systems that protect students' privacy and ensure data integrity. Creating a safe and resilient digital learning environment is essential not only for safeguarding information but also for

fostering trust, supporting inclusive access, and enabling effective use of innovative technologies in education. In this context, pre-service teachers, trained in the information age, should possess the skills that would allow them to utilize educational information and communication technologies actively and effectively and be competent in technology-based applications such as computer-assisted education [8, 22, 23].

The research study of cyber security awareness among students of higher education in India (Kant, 2023) found that Indian students living in urban areas were found to be more aware of cyber security than students living in rural areas, however, no significant difference was found between them based on the level of study, gender or the nature of the course [24].

In Turkey, according to Haseski (2020), pre-service teachers should improve their competency in cyber security, furthermore, personal cyber security achievement score was a significant predictor of the attitude towards computer-assisted education. In the article «Cyber Security Skills of Pre-Service Teachers as a Factor in Computer-Assisted Education» various recommendations were presented for future studies and applications on the subject [22].

In the USA the study “Pre-Service Teachers’ Perceptions of Information Assurance and Cyber Security” [25] indicated a lack of best practices in information assurance that was no different from that of general computer end-users to protect personal electronic information (Agamba& Keengwe, 2014). There is clear demand for cyber security education that will require effort beyond simple declarative knowledge of security principles to more robust acquisition of security skills for applying then in authentic digital threat environments in the USA (Navarrete, 2023) [26].

**The Ukrainian scholars, Kovalenko and Osypchuk (2024), in their article, describe the safe educational environment within general secondary education institutions in Ukraine, which includes a cyber-safe educational component. This environment contributes to the professional development of educators through the implementation of various measures aimed at ensuring cybersecurity within schools. The scholars outline a cybersecurity policy for general secondary education institutions, which can be implemented through recommendations such as setting strong passwords and updating them regularly, as well as keeping device software and operating systems up to date to prevent cyberattacks [27].**

#### **4. Designing a course on C3 skills and AI competency for pre-service teachers**

In Ukraine, the issue of creating a cybersafe educational environment is particularly pressing. According to the UNICEF report “*Life for Children During the War*” (2024) [28], 60% of children aged 7 to 18 are engaged in hybrid forms of learning, while 17% of students are enrolled in distance education. In frontline areas, 53% of children aged 6–17 study exclusively online due to the ongoing war. In Ukraine, approximately 30 universities (including Bohdan Khmelnytsky Melitopol State Pedagogical University) have been forcibly relocated to safer regions due to occupation and active hostilities. The educational process is ongoing online, supported by cloud technologies and educational platforms.

This shift toward online and hybrid learning environments increases children’s exposure to cyber risks such as phishing, cyberbullying, identity theft, and exposure to harmful content. In such a context, Ukrainian educators must also be competent in cybersafety, cyberethics, and cybersecurity to ensure that digital learning is not only effective but also safe and ethically responsible.

Therefore, teacher training programs must prioritize the development of cybersecurity competencies. This includes equipping pre-service teachers with practical knowledge and skills to identify, prevent, and respond to cyber threats, create protective digital policies in schools, and educate students on responsible online behavior.

Our research focuses on the issue of preparing future teachers to effectively use the potential of artificial intelligence in their professional practice [29]. In particular, it addresses the development



of their competencies in the areas of digital safety, cyberethics, and cybersecurity (C3) in displaced university in Ukraine.

We have developed a syllabus for the online elective course “**Pedagogical Aspects of Using Artificial Intelligence in Secondary Education Institutions**” designed for students majoring in **Secondary Education (Mathematics)** at both the first and second levels of higher education (2 ECTS, 60 hours) at Bohdan Khmelnytsky Melitopol State Pedagogical University (Ukraine). The provisional course outline is presented in **Table 1**.

**Table 1**

The content of the elective course “Pedagogical Aspects of Using Artificial Intelligence in Secondary Education Institutions”

| №  | Topic  | Hours | Format                         |
|----|--|-------|--------------------------------|
| 1  | Introduction: Digital transformation in education and the role of AI             | 4     | Lecture + discussion           |
| 2  | Fundamentals of AI: Concepts, algorithms, examples                               | 6     | Lecture + workshop             |
| 3  | Educational applications of AI: adaptive learning, chatbots, generative tools    | 4     | Webinar + case studies         |
| 4  | Pedagogical transformation: Changing roles of teachers in AI-driven environments | 4     | Lecture + reflection           |
| 5  | Ethics, digital rights, and responsibilities in AI usage                         | 8     | Webinar + situational analysis |
| 6  | Basics of cybersecurity in educational settings                                  | 8     | Lecture + practical session    |
| 7  | AI-related threats to privacy and safety: phishing, deepfakes, data breaches     | 8     | Case analysis + group work     |
| 8  | AI for teaching mathematics  | 8     | Lecture + workshop             |
| 9  | Practical strategies for safe and responsible AI use in schools                  | 6     | Mini-projects + simulations    |
| 10 | Final session: Student project presentations and reflection                      | 4     | Presentations                  |

The main aim of this course is to develop a comprehensive understanding among pre-service teachers of the pedagogical opportunities, challenges, and limitations of using AI in secondary mathematical education, with a specific focus on C3 issues: cyber-ethics, cybersecurity, and the cyber-safety in digital learning environment. Course is based on **UNESCO AI CFT**, **AI Competency for Educators Framework** and *Guidelines on Artificial Intelligence for General Secondary Education Institutions* from the Ministry of Education and Science of Ukraine. Assessment course methods include ongoing assessment (quizzes, participation, and case discussions), mini-project (lesson or digital activity involving AI tools) and final presentation of project outcomes.

The course was developed based on the ADDIE instructional design model [30], which involves a step-by-step approach to the creation of educational products. The process included five key stages: analysis of learning needs (Analysis), designing the structure and content (Design), development of learning materials (Development), practical implementation (Implementation), and evaluation of effectiveness (Evaluation). The course “**Pedagogical Aspects of Using Artificial Intelligence in Secondary Education Institutions**” will be integrated into the learning management system (LMS) of Bohdan Khmelnytsky Melitopol State Pedagogical University—Moodle.

At the end of the course, students are offered to complete a Generative Artificial Intelligence Literacy Test (GLAT), developed by a group of Australian researchers [31]. This is the only available specialized instrument that takes into account the specific features of generative AI and has been developed in accordance with established procedures in psychological and educational measurement. The test consists of 20 multiple-choice items covering four dimensions: “Knowledge and Understanding,” “Application,” “Evaluation and Creation,” and “Ethics.” We translated the GLAT test items into Ukrainian and adapted it for Ukrainian students. This particular test will be used in our pedagogical experiment as a diagnostic tool for assessing AI literacy among prospective mathematics teachers, as it offers a reliable and more objective method for evaluating literacy in the field of generative AI.

## Conclusions

Priority directions for our further research include the scientific justification of pedagogical conditions that ensure the preparation of pre-service teachers for the implementation of AI technologies in their professional activities and development of their C3 skills; the creation of methodological recommendations for fostering pre-service teachers’ readiness to use AI technologies in the educational process; as well as conducting a pedagogical experiment to evaluate the effectiveness of the developed elective course in forming this readiness among pre-service teachers.

## Declaration on Generative AI

While preparing this work, the authors used the AI programs Grammarly Pro and GPT-4o to correct text grammar and Strike Plagiarism to search for possible plagiarism. After using this tool, the authors reviewed and edited the content as needed and took full responsibility for the publication’s content.

## References

- [1] P. Pusey, W. A. Sadera. Cyberethics, Cybersafety, and Cybersecurity: Preservice Teacher Knowledge, Preparedness, and the Need for Teacher Education to Make a Difference. *J. Digital Learning in Teacher Education*, 28 (2), 2011. 82–85. doi:10.1080/21532974.2011.10784684
- [2] O. Burov, et al., Cybersecurity in Educational Networks, *Advances in Intelligent Systems and Computing*, 359–364, 2020. doi:10.1007/978-3-030-39512-4\_56
- [3] V. Buriachok, V. Sokolov, Implementation of Active Learning in the Master’s Program on Cybersecurity, *Advances in Computer Science for Engineering and Education II*, vol. 938 (2020) 610–624. doi:10.1007/978-3-030-16621-2\_57.
- [4] V. Buriachok, et al., Implementation of Active Cybersecurity Education in Ukrainian Higher School, *Information Technology for Education, Science, and Technics*, vol. 178 (2023) 533–551. doi:10.1007/978-3-031-35467-0\_32
- [5] M. Astafieva, et al., Formation of High School Students’ Resistance to Destructive Information Influences, in: *Cybersecurity Providing in Information and Telecommunication Systems*, vol. 3421 (2023) 87–96.
- [6] D. Long, B. Magerko. What Is AI Literacy? Competencies and Design Considerations, in: *2020 CHI Conference on Human Factors in Computing Systems*, 2020, 1–16. doi:10.1145/3313831.3376727
- [7] T. K. F. Chiu, Z. Ahmad, M. Ismailov, I. T. Sanusi, What are Artificial Intelligence Literacy and Competency? A Comprehensive Framework to Support Them, *Computers and Education Open*, 6 (2024). doi:10.1016/j.caeo.2024.100171



- [8] D. Maher. Pre-Service Teachers' Digital Competencies to Support School Students' Digital Literacies, *Handbook of Research on Literacy and Digital Technology Integration in Teacher Education*, 2019, 29–46.
- [9] A. Liu, M. Sun. AI Competency for Educators (AICE) Framework: Defining and Developing Practical AI Competency in Education, 2025. <https://www.colleague.ai/ai-competency-for-educators-aice-framework/>
- [10] Guidelines on Artificial Intelligence for General Secondary Education Institutions Project of the Ministry of Education and the Ministry of Digital Transformation of Ukraine, 2024. <https://mon.gov.ua/static-objects/mon/sites/1/news/2024/05/21/Instruktyvno.metodychni.rekomendatsiyi.shchodo.SHI.v.ZZSO-22.05.2024.pdf>
- [11] Professional Standard “Teacher of a General Secondary Education Institution” Ministry of Education and Science of Ukraine, 2024. <https://mon.gov.ua/npa/pro-zatverdzhennia-profesiinoho-standartu-vchytel-zakladu-zahalnoi-serednoi-osvity>
- [12] UNESCO ICT Competency Framework for Teachers, 2018. <https://unesdoc.unesco.org/ark:/48223/pf0000265721>
- [13] Microsoft Digital Defense Report: The Foundations and New Frontiers of Cybersecurity, 2024. <https://www.microsoft.com/en-us/security/security-insider/threat-landscape/microsoft-digital-defense-report-2024>
- [14] H. Hulak, et al., Formation of Requirements for the Electronic RecordBook in Guaranteed Information Systems of Distance Learning, in: *Cybersecurity Providing in Information and Telecommunication Systems*, (CPITS 2021), 2923, 2021, 137–142.
- [15] O. Mykhaylova, T. Fedynyshyn, V. Sokolov, R. Kyrychok, Person-of-Interest Detection on Mobile Forensics Data—AI-Driven Roadmap, in: *Cybersecurity Providing in Information and Telecommunication Systems*, 3654, 2024, 239–251.
- [16] S. Vasilishyn, et al., Information Technologies for the Synthesis of Rule Databases of an Intelligent Lighting Control System, *J. Theor. Appl. Inf. Technol.* 100(5) (2022) 1340–1353.
- [17] V. Lakhno, V. Kozlovskii, Y. Boiko, A. Mishchenko, I. Opirskyy, Management of Information Protection based on the Integrated Implementation of Decision Support Systems, *Eastern-European J. Enterprise Technol.* 5(9(89)) (2017) 36–41. doi:10.15587/1729-4061.2017.111081
- [18] V. Susukailo, I. Opirsky, O. Yaremko, Methodology of ISMS Establishment Against Modern Cybersecurity Threats, in: *Lecture Notes in Electrical Engineering*, Springer International Publishing, Cham, 2021, 257–271. doi:10.1007/978-3-030-92435-5\_15
- [19] D. Shevchuk, et al., Designing Secured Services for Authentication, Authorization, and Accounting of Users, in: *Cybersecurity Providing in Information and Telecommunication Systems (CPITS-2023-II)*, 3550, 2023, 217–225.
- [20] O. Deineka, et al., Information Classification Framework According to SOC 2 Type II, in: *Cybersecurity Providing in Information and Telecommunication Systems II (CPITS-II 2024)*, 3826, 2024, 182–189.
- [21] D. Pruitt-Mentle. C3 Framework Promoting Responsible Use. *Educational Technology Policy, Research and Outreach*, 2000.
- [22] H. I. Haseski. Cyber Security Skills of Pre-Service Teachers as a Factor in Computer-assisted Education, *Int. J. Res. Educ. Sci. (IJRES)*, 6(3), 2020, 484–500.
- [23] A. List, Defining Digital Literacy Development: An Examination of Pre-Service Teachers' Beliefs, *Computers & Education*, 138, 2019, 146–158.
- [24] R. Kant. Cyber-Security Awareness in India: How Much Students of Higher Education Are Aware? *GESJ: Educ. Sci. Psychol.* 2(67) 59–72.
- [25] J. Agamba, J. Keengwe, Pre-Service Teachers' Perceptions of Information Assurance and Cyber Security, *Int. J. Inf. Commun. Technol. Educ.* 8(2) (2014) 94–101.
- [26] C. Navarrete. Preparing Pre-Service Teachers to Teach Cyber Security Education: Examining Theoretical Approaches, in: *ICERI2023 Proceedings*, 2023, 2215–2221.

- [27] V. Kovalenko, T. Osypchuk. The Problem of Developing Digital Competence in Cyber Security of Teachers of General Secondary Education Institutions, *Physical Math. Educ.* 39(2) (2024) 35–41. doi:10.31110/fmo2024.v39i2-05
- [28] UNICEF. Life for Children during the War. Ukraine, 2024. <https://www.unicef.org/ukraine/en/documents/life-children-during-war>
- [29] O. A. Termenzhy, A. V. Kozhevnykova. Comparative Analysis of Modern Tools for Assessing AI-Literacy, *Tsyfrovyzatsiia osvity: upravlinnia zminamy: zb. nauk. pr. za materialamy Vseukrainskoi naukovo-praktychnoi konferentsii «Tsyfrovyzatsiia osvity: upravlinnia zminamy»*, 2025, 269–275.
- [30] S. Kurt. The ADDIE Model: Instructional Design Educational Technology, 2024. <http://educationaltechnology.net/the-addie-model-instructional-design/>
- [31] Y. Jina, R. Martinez-Maldonado, D. Gašević and, L. Yana. GLAT: The Generative AI Literacy Assessment Test, 2024. doi:10.48550/arXiv.2411.00283