Dubinsky V. Training of computer science teachers for the formation of cybersecurity skills in students: actualization of problems and their possible solutions. *Освіта. Інноватика. Практика,* 2024. Том 12, № 10. С. 6-11. https://doi.org/10.31110/2616-650X-vol12i10-001.

Dubinsky V. Training of computer science teachers for the formation of cybersecurity skills in students: actualization of problems and their possible solutions. *Osvita. Innovatyka. Praktyka – Education. Innovation. Practice,* 2024. Vol. 12, No 10. S. 6-11. https://doi.org/10.31110/2616-650X-vol12i10-001.

DOI: 10.31110/2616-650X-vol12i10-001

Віталій ДУБИНСЬКИЙ
Сумський державний педагогічний університет імені А.С. Макаренка, Україна
https://orcid.org/0009-0003-1103-7765
v.dubinsky@fizmatsspu.sumy.ua

ПІДГОТОВКА ВЧИТЕЛІВ ІНФОРМАТИКИ ДО ФОРМУВАННЯ В УЧНІВ НАВИЧОК КІБЕРБЕЗПЕКИ: АКТУАЛІЗАЦІЯ ПРОБЛЕМ ТА ЇХ МОЖЛИВІ РІШЕННЯ

Анотація. *У статті подається аналіз проблеми підготовки вчителів інформатики до формування в учнів навичок кібербезпеки. Узагальнення наявних наукових результатів дає уявлення про загальні тенденції та проблеми в цій галузі: наголошується на необхідності постійного оновлення навчальних програм з інформатики та кібербезпеки, щоб йти в ногу з розвитком технологій та стандартів; акцентується потреба поєднання практичних навичок з фундаментальними знаннями в освіті з кібербезпеки; підкреслюється важливість педагогічних і методичних знань поряд із предметними знаннями у підготовці вчителів інформатики; опанування інноваційних цифрових стратегій викладання і навчання інформатики; змішаний спосіб викладання курсів (очний, гібридний або онлайн) і різноманітність методів навчання; розвиток методичної компетентності вчителів інформатики через різні підходи до такого розвитку (спецкурси, програми стажування, наставництво, спільне планування уроків та рефлексивна практика тощо). За результатами аналізу сформульовано рекомендації щодо модернізації програм підготовки вчителів для формування в учнів навичок кібербезпеки: інтеграція змістових модулів з кібербезпеки в курси з методики навчання інформатики; розробка й упровадження спеціалізованих курсів з кібербезпеки у освітньо-професійні програми підготовки вчителів; використання цифрових інструментів та технологій симуляції; сприяння постійному професійному розвитку вчителів у галузі кібербезпеки; сприяння співпраці та обміну знаннями з фахівцями-практиками в галузі кібербезпеки; приведення навчальних програм підготовки вчителів інформатики у відповідність до міжнародних стандартів у галузі кібербезпеки. Вважаємо перспективними подальші дослідження для вивчення змісту освітніх програм підготовки вчителів інформатики, аналіз ефективності різних методів навчання для розвитку навичок кібербезпеки у майбутніх вчителів інформатики.*

Ключові слова: *вчителів інформатики; навички кібербезпеки; IT; освітні програми; професійна підготовка; професійна освіта.*

Vitaliy DUBINSKY
Sumy State Pedagogical University named after A.S. Makarenko, Sumy, Ukraine
https://orcid.org/0009-0003-1103-7765
v.dubinsky@fizmatsspu.sumy.ua

TRAINING OF COMPUTER SCIENCE TEACHERS FOR THE FORMATION OF CYBERSECURITY SKILLS IN STUDENTS: ACTUALIZATION OF PROBLEMS AND THEIR POSSIBLE SOLUTIONS

Abstract. *The article presents an analysis of the problem of preparing computer science teachers for the formation of cybersecurity skills in students. The generalization of the available scientific results gives an idea of the general trends and problems in this field: the need for constant updating of the curriculum in computer science and cybersecurity is emphasized to keep pace with the development of technologies and standards; emphasizes the need to combine practical skills with fundamental knowledge in cybersecurity education; stresses the importance of pedagogical and methodological knowledge along with subject knowledge in the training of computer science teachers; mastering innovative digital strategies for teaching and learning computer science; a mixed way of teaching courses (face-to-face, hybrid or online) and a variety of teaching methods; development of methodological competence of computer science teachers through different approaches to such development (special courses, internship programs, mentoring, joint lesson planning and reflective practice, etc.). Based on the results of the analysis, recommendations were formulated for the modernization of teacher training programs for the formation of students' cybersecurity skills: integration of content modules on cybersecurity into courses on methods of teaching computer science; development and implementation of specialized cybersecurity courses in educational and professional teacher training programs; use of digital tools and simulation technologies; promoting the continuous professional development of teachers in the field of cybersecurity; promoting cooperation and knowledge exchange with cybersecurity practitioners; bringing computer science teacher training curricula in line with international standards in the field of cybersecurity. We consider further research to be promising in studying the content of educational programs for training computer science teachers and analyzing the effectiveness of various teaching methods for developing cybersecurity skills in future computer science teachers.*

Keywords: *computer science teachers; cybersecurity skills; IT; educational programs; vocational training; vocational education.*

Introduction. The rapid development of information technology has significantly increased the risks associated with cybersecurity. Cyber threats are constantly evolving, exploiting new vulnerabilities and creating constant challenges. These threats include data theft, phishing, ransomware, identity fraud, and other malicious activities targeting individuals, organizations, and government agencies [9]. As active Internet and digital tools users, young people are especially vulnerable to cyber threats [5]. They often face issues such as

account hacking, phishing attacks, exposure to malicious content, and manipulation on social media platforms. Many of these problems arise from a lack of awareness or understanding of basic cybersecurity practices. Solving this problem requires active efforts to form the necessary cybersecurity skills in schoolchildren early on. School, especially computer science classes, is a great platform for exposing students to secure digital practices and cybersecurity fundamentals. However, for this process to be effective, teachers must be prepared to teach these topics.

Analysis of current research. The scientific and pedagogical literature lacks specific details on the titles and scope of courses directly aimed at developing cybersecurity skills within teacher training programs. This gap in the literature highlights the need for more research and analysis of existing applications to identify how cybersecurity is integrated into teacher training. However, several papers offer insights into related areas indirectly contributing to developing cybersecurity skills. For example, in a discussion of network security education [1] emphasizes the importance of "protecting hardware, information systems, and electronic data", which are important cybersecurity objects. This suggests that network security courses can be essential components of computer science teacher training in cybersecurity. The article also mentions the use of "existing teacher knowledge frameworks" to analyze and improve "educator knowledge constructs" in network security education [1], which indicates that a systematic approach to incorporating cybersecurity concepts into teacher training is essential. In addition, the analysis of educators' digital competencies [8] touches on the importance of "digital security and responsible use of the online environment in educational activities." This suggests that digital literacy and online safety courses can improve teachers' cybersecurity awareness and skills. At the same time, despite the apparent need, the analysis of modern professional training programs for computer science teachers indicates significant gaps. These programs often do not contain unique components aimed at developing competencies in the field of cybersecurity. As a result, future computer science teachers are not sufficiently prepared to impart important knowledge to their students [17]. This gap highlights the importance of in-depth cybersecurity training for computer science teachers. A proactive approach to appropriate teacher training will enable them to respond effectively to new challenges, thereby contributing to broader efforts to create digital security in the information society.

The article aims to actualize the problems of preparing computer science teachers to form students' cybersecurity skills and formulate recommendations for their solutions.

Results. The available literature emphasizes the importance of mastering teaching methods. Still, it does not directly address the formation of digital security skills in courses on the methods of teaching computer science of these methods. For example, in [6] discusses the role of "methodological courses" in the formation of pedagogical and methodological knowledge for future teachers of computer science but does not specify whether these courses include the preparation of future teachers to master the concepts of digital security and the formation of appropriate methodological skills of teachers. Similarly, [3] analyzes methods of teaching computer science but focuses on general pedagogical approaches rather than specific strategies for teaching and teaching digital security. The lack of clear attention to digital security in the computer science teaching methods courses in each educational and professional program confirms the conclusion that there is insufficient attention to training computer science teachers to develop students' digital security skills. The available scientific literature primarily focuses on general pedagogical approaches and the content of knowledge in computer science, ignoring specific pedagogical problems and strategies related to digital security education. However, some works indirectly touch on related topics. While specific cybersecurity courses are helpful, such as [7], integrating cybersecurity concepts into existing computer science courses can also be effective. Researchers [4] argue that this may involve including security modules in programming courses from databases and computer networks. This will provide a more holistic understanding of safety principles. Their statement is based on the implementation of security modules in the CS2 course, which demonstrated the feasibility and effectiveness of this approach. There is a lack of specific details in the scientific literature regarding the titles and scope of courses dedicated to developing cybersecurity skills within teacher training programs. However, we can focus on such courses' potential content and structure. A comprehensive cybersecurity course for computer science teachers can cover various topics (Fig. 1).

Effective cybersecurity education requires a balanced approach combining fundamental knowledge and practical skills [16]. Therefore, teacher training programs should provide educators with the opportunity not only to learn the theoretical foundations of cybersecurity but also to apply these concepts in practical settings [15]. This can include practical actions such as adjusting security settings, analyzing security vulnerabilities, and responding to simulated cyberattacks. Research [16] emphasizes the importance of access to "experimental bases, practical training laboratories, and a staff of teachers and researchers" to facilitate this balance between theory and practice.

Along with subject knowledge, pedagogical training is important in training computer science teachers [6]. Methodological courses should provide educators with the necessary pedagogical knowledge and skills to effectively teach cybersecurity concepts. This may include learning different learning strategies, such as project-based, inquiry-based, and collaborative learning, and adapting them to the specific context of

cybersecurity education. Friend et al. [6] emphasize the importance of "methodological courses" as a source of knowledge of "pedagogical and methodological content" for future teachers of computer science, emphasizing the need for special pedagogical training within the framework of teacher training programs.

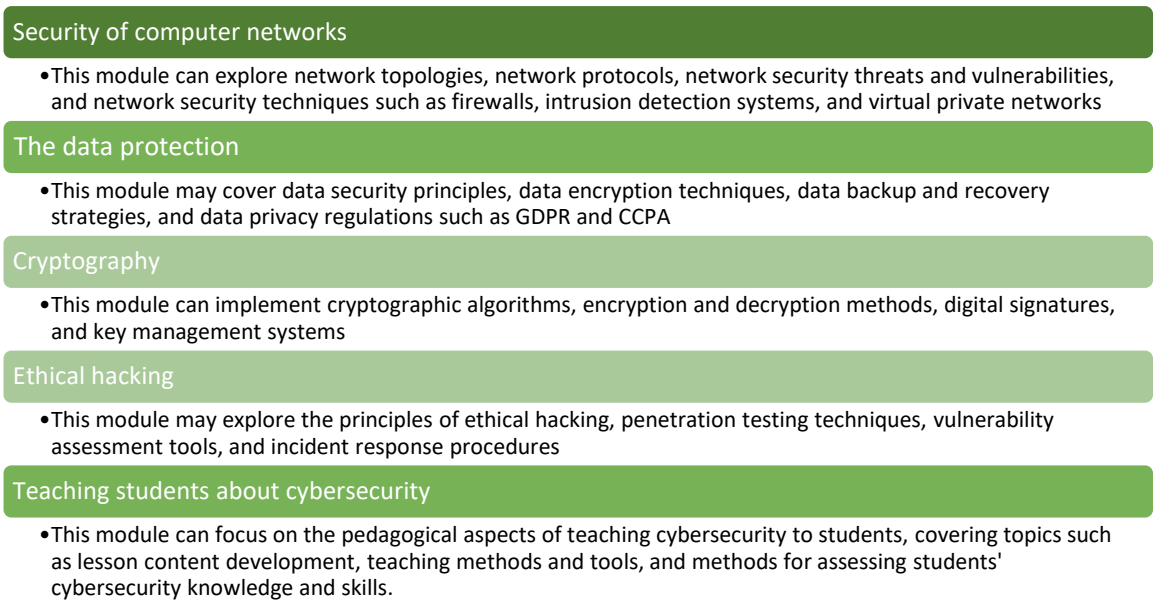

Fig. 1. Possible content of the cybersecurity course for computer science teachers

The concept of information and digital culture [18] and methodological competence, encompassing the knowledge, skills, and abilities necessary for effective teaching, is especially relevant in teaching cybersecurity students from a modern school. Computer science teachers must not only understand the concept of cybersecurity but also have pedagogical knowledge to convey these concepts to students effectively. This includes the ability to develop interesting educational activities and correctly assess students' understanding [14] and the ability to adapt teaching strategies to meet the diverse needs of students. Researchers [15] emphasize the importance of methodological competence, such as "goal setting, content selection, instructional strategies, assessment methods, and adaptability," which are essential for effective cybersecurity education.

Integration of the content of digital security into courses of methods of teaching computer science requires consideration of different pedagogical approaches [11]. Project-based learning, where students participate in real-world cybersecurity projects, can effectively develop practical skills and problem-solving abilities. Inquiry-based learning, where students explore cybersecurity issues and build their own solutions, can foster critical thinking and analytical skills. Collaborative learning, where students work together on cybersecurity tasks and projects, can foster teamwork and communication skills. Using case studies where students analyze real-world cybersecurity incidents and develop response strategies can improve their understanding of security threats and vulnerabilities. In addition, using gamified learning activities and interactive simulations can make cybersecurity training more interesting and enjoyable.

Digital tools and technologies, such as virtual labs, simulations, and online platforms, can significantly improve teacher cybersecurity training. These tools can provide engaging learning experiences by allowing educators to explore cybersecurity concepts [2]. For example, virtual labs can simulate real-world cyberattacks, providing teachers with hands-on experience analyzing security vulnerabilities and implementing security measures. Using game technologies and interactive simulations can further increase motivation to learn, making developing cybersecurity skills more effective and enjoyable.

Scholarly sources provide limited specific guidance on the forms, methods, and means of teaching that directly contribute to developing teachers' cybersecurity skills. However, several papers discuss related pedagogical approaches and technological tools that can be adapted for cybersecurity education. Thus, in [4], the authors describe the use of Model-Eliciting Activities (MEAs) as a "problem-solving project" to help students demonstrate their understanding of security concepts. This approach, which shifts teaching from a teacher-centered approach to a student-centered approach, can be effectively used in teacher training programs to engage them in active learning and application of cybersecurity principles. The study concludes that a significant percentage of solutions developed by students demonstrated "creativity and suitability for real-world applications" [4] and also testifies to the potential of MEAs in promoting the development of practical cybersecurity skills.

In the article [1] mentions the use of "existing teacher knowledge frameworks" to analyze and improve "teacher knowledge constructs" in network security education. This highlights the importance of using

established pedagogical frameworks for teacher training and adapting them to the cybersecurity context. Discussion in the document of "knowledge about curricula and pedagogical content of knowledge specific to the teaching of network security" [1] is the starting point for developing a more comprehensive framework for training cybersecurity teachers. The emphasis on digital competencies for educators suggests that integrating digital tools and technologies into cybersecurity education can be beneficial. The proposed model of digital competencies [8] can be expanded to include specific knowledge and skills in cybersecurity and using appropriate digital tools. For example, virtual labs and simulations can provide teachers with hands-on experience with cybersecurity scenarios.

A wide range of digital tools and technologies can be used to enhance the skills of computer science teachers in cybersecurity. Virtual labs, like those offered by Cisco and other vendors, can provide realistic simulations of network environments and cybersecurity scenarios. Penetration testing tools like Metasploit and Nmap can allow teachers to practice ethical hacking and identify security vulnerabilities. Data analysis tools like Splunk and Wireshark can help teachers analyze network traffic and identify security threats. Additionally, online platforms like Cybrary and Coursera offer many cybersecurity courses and resources teachers can access for professional development.

Discussion. The rapid development of technologies and threats to cybersecurity necessitates the constant updating of educational programs for training teachers of computer science [16]. This requires a proactive approach to developing an informatics teacher training program that includes regular revisions to ensure content remains relevant and compliant with current industry standards and best practices. Scientists emphasize that "cybersecurity curricula become obsolete too quickly" and therefore need frequent updates, perhaps annually. Given the rapidly evolving nature of cybersecurity, continuous learning and professional development in this field are essential for computer science teachers. Teacher training programs should provide basic cybersecurity skills and encourage and support ongoing learning through workshops, online courses, conferences, and professional communities. Scientists [16] emphasize the importance of lifelong learning in cybersecurity.

Educational and professional teacher training programs could benefit from introducing specialized courses focused on developing cybersecurity skills. These courses cover network security, data protection, cryptography, ethical hacking, and incident response. The content should be adapted to the needs of computer science teachers, emphasizing the pedagogical aspects of teaching these concepts to students. Current courses in computer science teaching methodologies should be revised to include a digital security teaching methodology that involves the study of modules on cybersecurity concepts, learning strategies, and assessment methods. The use of project-based learning can be especially effective for this.

Cybersecurity training can be improved by integrating digital tools and technologies like virtual labs, simulations, and online platforms. Teacher training programs should allow educators to participate in ongoing learning through various channels [10]. Seminars and conferences offered by professional organizations such as ISC2 and SANS can provide specialized training on specific cybersecurity topics. Online courses offered by platforms such as edX and Udacity can offer flexible and affordable learning opportunities. Professional certifications such as CompTIA Security+ and CISSP can demonstrate teachers' competence in cybersecurity and enhance their professional qualifications. Attending conferences is a chance to get acquainted with positive educational practices using digital tools [12]. Additionally, participating in online communities and forums, such as r/cybersecurity on Reddit and the information security site Stack Exchange, can provide teachers with access to knowledge and expertise from cybersecurity professionals. These tools can provide teachers with hands-on experience with cybersecurity scenarios, analyzing security vulnerabilities, and implementing security measures. Interactive learning environments and gamified learning activities can increase student engagement and motivation.

Cybersecurity is an ever-evolving field that requires continuous learning and skill development. Teacher training programs should encourage and support continuous professional development in cybersecurity by providing access to workshops, online courses, conferences, and professional communities. This may include partnering with cybersecurity organizations and industry experts to offer specialized training opportunities for teachers. This can also be implemented through additional training in seminars, online courses on cybersecurity, and the formation of self-development skills in formal learning. It should be noted that the emphasis is on continuous learning in cybersecurity [16], indicating that teacher training programs should provide basic cybersecurity skills and encourage continuous professional development in this area.

Creating opportunities for computer science teachers to share their experiences, best practices, and resources related to cybersecurity education can be very beneficial. This can include creating online communities, organizing workshops and conferences, and developing collaborative projects focused on cybersecurity education. such as Google Classroom and Microsoft Teams, can facilitate communication and collaboration between teachers. Shared repositories such as GitHub and GitLab can provide a platform for sharing learning materials, lesson plans, and cybersecurity resources. Professional learning communities organized by schools, districts, or professional organizations can provide a forum for teachers to discuss

cybersecurity education issues and share best practices. In particular, the article [13] presents the features of the choice of courses for the formation of information hygiene of students, which provide for the development of cybersecurity skills. Additionally, mentoring programs, where experienced cybersecurity professionals mentor computer science teachers, can provide valuable guidance and support. Hence, encouraging collaboration and knowledge sharing among computer science teachers is essential to promote effective cybersecurity education.

Regularly reviewing and updating computer science teacher training programs to align them with international standards and cybersecurity best practices can ensure that teachers are equipped with the latest knowledge and skills in the field and that their training meets global standards. This involves regularly reviewing and updating curricula to reflect current trends and developments in cybersecurity. Organizations such as ISO and NIST provide various resources and frameworks that can guide the development of cybersecurity curriculums and ensure that teacher training programs meet global standards. Aligning computer science teacher training curricula with international cybersecurity standards is essential to provide teachers with the latest cybersecurity knowledge and skills. The ISO/IEC 27000 standard provides a framework for information security management systems that can be used to develop cybersecurity training programs. The NIST Cybersecurity Framework provides a set of standards, guidelines, and best practices for managing cybersecurity risks, which can also be incorporated into teacher training programs. In addition, ENISA (European Union Agency for Cybersecurity) offers a variety of resources and training materials that can be used to improve cybersecurity education.

Conclusions. The study provides an idea of the general trends and problems in preparing computer science teachers to form students' cybersecurity skills. Scientific research emphasizes the need for constant updating of curricula in the field of IT, emphasizes the need to create practical skills in cybersecurity, emphasizes the importance of future teachers mastering not only subject knowledge of cybersecurity but also psychological, pedagogical, and methodological knowledge and skills to form cybersecurity skills in students; mastering innovative digital strategies for teaching and learning computer science. Scientists note this as an effective blended way of teaching courses and prove the effectiveness of various teaching methods. Some scientific investigations emphasize the need to develop the methodological competence of computer science teachers.

Based on the analysis of the literature provided, several recommendations can be made for the modernization of teacher training programs for the formation of students' cybersecurity skills: integration of cybersecurity into courses on teaching methods; development and implementation of specialized courses on cybersecurity in the educational and professional teacher training program; use of digital tools and simulation technologies; promotion of continuous professional development; teachers in the field of cybersecurity; promoting collaboration and knowledge sharing with professionals; bringing curricula in line with international standards. We consider further research to be promising in studying the content of educational programs for training computer science teachers and analyzing the effectiveness of various teaching methods for developing cybersecurity skills in future computer science teachers.

References

1. Ata R., Yıldırım K. Turkish pre-service teachers' perceptions of digital citizenship in education programs. *Journal of Information Technology Education: Research*, 2019. Vol. 18. Pp. 419-438. DOI: https://doi.org/10.28945/4392.
2. Buts K. Methodological recommendations for teaching the elective course "Fundamentals of Cybersecurity". *Scientific notes of young scientists*, 2021. Vol. 8. URL: https://phm.cuspu.edu.ua/ojs/index.php/SNYS/article/view/1895.
3. Chauvot J.B., Gurkan, D., Cathy H. Exploring Network Security Educator Knowledge. *Journal of Cybersecurity Education, Research and Practice*, 2023. No. 2. Article 6. DOI: https://doi.org/10.32727/8.2023.20.
4. Earwood B., Yang J., Kim Y. R. Effective Learning of Cybersecurity Concepts with Model-Eliciting Activities. *2021 IEEE International Conference on Engineering, Technology & Education (TALE),* Wuhan, Hubei Province, China, 2021. Pp. 01-07. DOI: https://doi.org/10.1109/TALE52509.2021.9678713.
5. Eremenko A. Formation of information security skills of 7th grade students using interactive technologies. *Our school: scientific and practical studies*, 2023. No. 4. P. 20-26. DOI: https://doi.org/10.61339/2786-6947.2023.4.315462.
6. Friend M., Leftwich A., Ben Schafer J., Simon B., Morrison B. B. Teaching the Methods of Teaching CS. In Proceedings of the *52nd ACM Technical Symposium on Computer Science Education (SIGCSE '21)*. Association for Computing Machinery, New York, NY, USA, 2021. Pp. 459-460. DOI: https://doi.org/10.1145/3408877.3432573.
7. Golovko D.Yu. Bepek in the digital space: electronic training course. Bila Tserkva: BINPO DZVO "UMO" NAPS of Ukraine, 2024. 54 p.
8. Kohut U. P., Sikora O. V., Vdovychyn T. Y. Formation of the teacher's individual educational trajectory for the development of digital competence. *ITLT*, vol. 91, No. 5. pp. 186-204. DOI: https://doi.org/10.33407/itlt.v91i5.5006.
9. Ostroha, M. M., Yurchenko, A. O., Korovay, A. O. Information hygiene and information noise. *Academic Visions*, 2023. Vol. 22. URL: https://academy-vision.org/index.php/av/article/view/511.
10. Osypchuk T.O. The Role of Digital Educational Resources in the Development of Digital Competence of Teachers in the Context of Cybersecurity. *Modern Technologies for Visualization of Collections of Digital Educational Resources*: Collection of Materials of the Round Table (for the All-Ukrainian Festival of Science), May 14, 2024, Kyiv. Nilan-LTD, Vinnytsia, Ukraine. P. 66-69.

11. Rudenko Y. O., Drushliak M. G., Shamonya V. G., Ostroha M. M., Semenikhina O. V. Development of the ability of student youth to resist information influences. *Information technologies and teaching aids*. 2023. Vol. 94(2). Pp. 54-71. DOI: https://doi.org/10.33407/itlt.v94i2.5162.
12. Rudenko Y., Ahadzhanov-Honsales K., Ahadzhanova S., Batalova A., Diemientiev Y., Semenikhina O. Interactive Boards as Digital Tools in the Modern Educational Process. *47th MIPRO ICT and Electronics Convention (MIPRO)*, Opatija, Croatia, 2024. Pp. 329-333. DOI: https://doi.org/10.1109/MIPRO60963.2024.10569393.
13. Rudenko Y., Ahadzhanov-Honsales K., Ahadzhanova S., Batalova A., Bieliaieva O., Yurchenko A., Semenikhina O. Modeling the choice of an online course for information hygiene skills using the saaty method. *Informatyka, Automatyka, Pomiary W Gospodarce I Ochronie Środowiska*, 2024. Vol. 14(2). Pp. 127-132. DOI: https://doi.org/10.35784/iapgos.5691.
14. Rudenko Yu., Proshkin V., Naboka O., Yurchenko A., Semenikhina O. Using Bloom's taxonomy to assess information hygiene skills. *E-learning & Artificial Intelligence (AI) Scientific Editor Eugenia Smyrnova-Trybulska "E-learning",* 15, Katowice–Cieszyn 2023. Pp. 137-148. DOI: https://doi.org/10.34916/el.2023.15.12.
15. Shyshenko I., Semenikhina O. Specific principles of introducing innovations in the professional training of future specialists. *IT and Educational Analytics*, 2024. Vol. 1(1). Pp. 36-41.
16. Sokolov V., Sklodanny P. Comparative analysis of strategies for building the second and third levels of educational programs in the specialty 125 "Cybersecurity". *Electronic Professional Scientific Edition "Cybersecurity: Education, Science, Technology"*, 2023. Vol. 4(20). Pp. 183-204. DOI: https://doi.org/10.28925/2663-4023.2023.20.183204.
17. Yashchyk O. Strengthening the global culture of cyber security on the Internet. *Scientific Journal of the Mykhailo Dragomanov Ukrainian State University. Series 2. Computer-Oriented Learning Systems*, 2019. Vol. 19 (26). Pp. 136-140. URL: https://sj.udu.edu.ua/index.php/kosn/article/view/24.
18. Yurchenko A., Momot R., Semenikhina O. On the development of information and digital culture of teachers using computer visualization. *Education. Innovation. Practice*, 2024. Vol. 12, No. 6. Pp. 93-99. DOI: https://doi.org/10.31110/2616-650X-vol12i6-014.