DIGITAL SECURITY SKILLS OF COMPUTER SCIENCE TEACHERS: GENERALIZATION OF THE RESULTS OF SCIENTIFIC PAPERS

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

Summary

The ubiquitous use of IT exposes society and its institutions (government, commercial, educational, etc.) to various cyber threats, ranging from malware and phishing to sophisticated attacks targeting sensitive data and infrastructure. The growing reliance on digital tools requires increased awareness and skills in digital security. The escalation of cyber threats highlights the urgent need to find robust approaches to digital security education, starting with the proactive training of computer science teachers. In the article, we substantiate the problem of preparing future computer science teachers to form students' digital security skills and the need for a proactive approach to building educational programs for training computer science teachers, which should pay special attention to the development of critical thinking of young people and skills in solving problems related to digital security. This will enable future teachers to respond to and adapt to new threats. It is emphasized that educational programs should include an educational component that provides practical exercises and simulations to gain practical experience with safety tools and methods. It is substantiated that integrating digital security courses into educational programs for training computer science teachers should go beyond isolated modules or optional courses and become a normative component of the educational program.

Key words: future computer science teacher, digital security, digital security skills, vocational training, education.

DOI https://doi.org/10.23856/6703

1. Introduction

The digital age has revolutionized education by integrating information technology (IT) into teaching and learning *(Yurchenko et al., 2023)*. This shift, while beneficial, poses problems, especially about informational influences *(Rudenko et al., 2023a)* and digital security. Therefore, IT integration requires actualization, understanding, and perception of the problem of digital security *(Drushliak, 2022)*, which should be considered not only at the state level but also at the level of education. The rapid pace of technological progress supports the relevance of non-formal education *(Yurchenko et al., 2021)*. Online platforms offer a wide variety of digital security training courses. At the same time, the constant emergence of new threats makes existing educational materials obsolete. This forces educators to respond to challenges and look for ways to improve cybersecurity education, which naturally begins with schools. Therefore, the problem of preparing future computer science teachers for the formation of students' digital security skills is relevant.

Analysis of current research. An analysis of computer science teacher training programs shows a particular disparity in digital security education. Some educational programs for training computer science teachers include modules on cybersecurity, but some programs still need

to provide) the formation of knowledge and skills in this area *(Kozhukhova & Proshkin, 2021)*. At the same time, educational programs often focus on the theoretical aspects of cyber threats and neglect practical skills to counter them in real life *(Port & Kessler, 2014)*. Given the growing complexity of cyber threats, this aspect determines the critical role of digital security in various sectors of the economy, and therefore, a comprehensive training program for specialists to develop integral practical skills to counter various cyber threats becomes necessary.

Another challenge is identifying gaps in knowledge and skills related to digital security. These include a lack of understanding of emerging threats (phishing, malware, ransomware, etc.) *(Yousif Yaseen, 2022)*, lack of knowledge of security protocols and counter-threat practices *(Yu et al., 2011)*, as well as limited experience in responding to incidents and ignorance of methods for their remediation. Due to the time barracks, most programs fail to adequately address digital security's ethical and legal implications, such as data privacy and intellectual property rights *(Feng et al., 2022)*. This prevents future teachers from teaching their students effectively. Research highlights the importance of digital literacy, including digital security, in the 21st century *(Boer et al., 2023)*. The lack of specific training in digital security can also lead to a decrease in the quality of student training *(Mostaghimi et al., 2017)*. The rapid development of technology also requires providing professional development opportunities for educators to ensure that existing knowledge is up-to-date on the latest cybersecurity trends. The constant emergence of new technologies makes establishing standardized methods for assessing cybersecurity skills challenging.

In many educational programs for training computer science teachers, there needs to be more emphasis on practical learning. The predominantly theoretical approach limits students' ability to develop practical skills, especially critical thinking, necessary to solve cybersecurity problems *(Rudenko et al., 2024)*. The use of virtual and cloud environments in educational institutions in Ukraine requires significant investments in resources and infrastructure, as well as the continuous development of cybersecurity skills of teachers and university staff.

Despite the gaps, there are positive trends to strengthen digital security education. Specialized courses and modules focused on cybersecurity are being developed as part of computer science teacher training programs *(Kozhukhova & Proshkin, 2021)*. The increasing availability of online resources, such as open educational resources, provides opportunities for educators to complement/deepen curricula. Integrating digital literacy frameworks *(DigCompEdu framework, Ng et al., 2023)* in teacher training programs helps standardize curricula. However, the rapid evolution of cyber threats requires constant updating of curricula, which requires significant resources and expertise *(Tang & Fan, 2024)*. The need for qualified teachers (instructors, practitioners, etc.) with computer science and digital security expertise creates a staffing problem.

Preparing future computer science teachers to address digital security issues effectively requires significant investments in institutional support resources. A critical barrier is the need for more sufficient resources (finances, computer hardware, software, etc.), which hinders the effective implementation of teacher training programs *(Kozhukhova & Proshkin, 2021)*. In particular, this includes insufficient funding for specialized software and hardware and access to up-to-date cybersecurity training materials. Many institutions need more money, making allocating sufficient funds for comprehensive digital security training difficult. The lack of specialized infrastructure, such as secure online learning environments and well-equipped computer labs, further exacerbates this problem. A significant obstacle is the need for specialized technical support personnel to assist teachers and educators. The need for clear guidelines and policies for integrating digital security into educational programs also poses certain risks.

The effectiveness of the implementation of educational programs depends on the teacher's level of preparedness. Many may need more digital security knowledge *(Rahmatullah et al., 2022)*, affecting their ability to train future teachers effectively. This lack of confidence and experience may be due to limited familiarity with cybersecurity concepts, insufficient professional development opportunities, and the nature of digital security. security, which is rapidly evolving under the influence of various threats. Researchers record a specific resistance of teachers to the introduction of new technologies *(Rahmatullah et al., 2022)*. Therefore, teacher training educational programs provide opportunities to build confidence and competence in digital security, which can be achieved through introducing more practical classes, facilitating, and creating a supportive learning environment.

The digital divide (in access to technology, the Internet, and existing IT skills) limits many students' ability to provide quality cybersecurity education *(Tang & Fan, 2024)*. Unequal access to technology and internet connectivity between students and teachers creates a disparity in learning opportunities. lack the necessary tools and resources to fully participate in digital security training, hindering their ability to develop the essential skills. Overcoming this barrier requires implementing strategies to bridge the digital divide, ensuring equal access to technology for all students and teachers *(Tang & Fan, 2024)*.

Practical education in the field of digital security requires the formation and development of interdisciplinary links between different disciplines of professional training of teachers, including computer science, mathematics, education, and information security *(Yuan et al., 2009)*. More development of these disciplines can create obstacles to effective learning. Teachers of IT disciplines may lack pedagogical knowledge about teaching methods and cyber threats, while educators may not understand digital security concepts sufficiently. The lack of interdisciplinary connections can lead to the fact that curricula will be either too technical or too theoretical, unable to effectively equip future computer science teachers with the necessary combination of technical and pedagogical skills.

Traditional methods for assessing digital security skills may need to be revised to cover the breadth and depth of understanding of the basic concepts and approaches required for cybersecurity *(Fang, 2024)*. Assessing practical skills, such as identifying and responding to threats, requires a unique approach that goes beyond traditional written exams *(Rudenko et al., 2023b)*. The dynamic nature of digital security manifestations necessitates continuously adapting assessment methods to ensure they remain relevant and practical. Developing reliable and valid assessment tools that will correctly measure knowledge and skills in the field of digital security becomes another challenge to ensure the effectiveness of educational programs.

Effective teaching of digital security courses requires a comprehensive approach that goes beyond simple lectures and includes active learning strategies. An important aspect is understanding students' specific needs and prior knowledge *(Kozhukhova & Proshkin, 2021)*. And although today's students often have a high level of digital literacy *(Martin et al., 2024)*, their knowledge of security principles may be limited. Teachers should assess the level of students' existing knowledge and, based on this, teach new material *(Ng et al., 2023)*, and therefore there is a need to search/choose appropriate teaching methods.

The analysis reveals problems in the training of future computer science teachers in the field of digital security. Generalization and systematization of the research allow us to formulate proposals for improving educational programs for training computer science teachers in this area. Therefore, **the study aims** to summarize the problems of preparing future computer science teachers to form digital security skills in students and formulate recommendations for improving relevant educational programs.

2. Main part

Based on the results of the presented analysis, we highlight the problems of preparing future computer science teachers for the formation of students' digital security skills (Fig. 1).

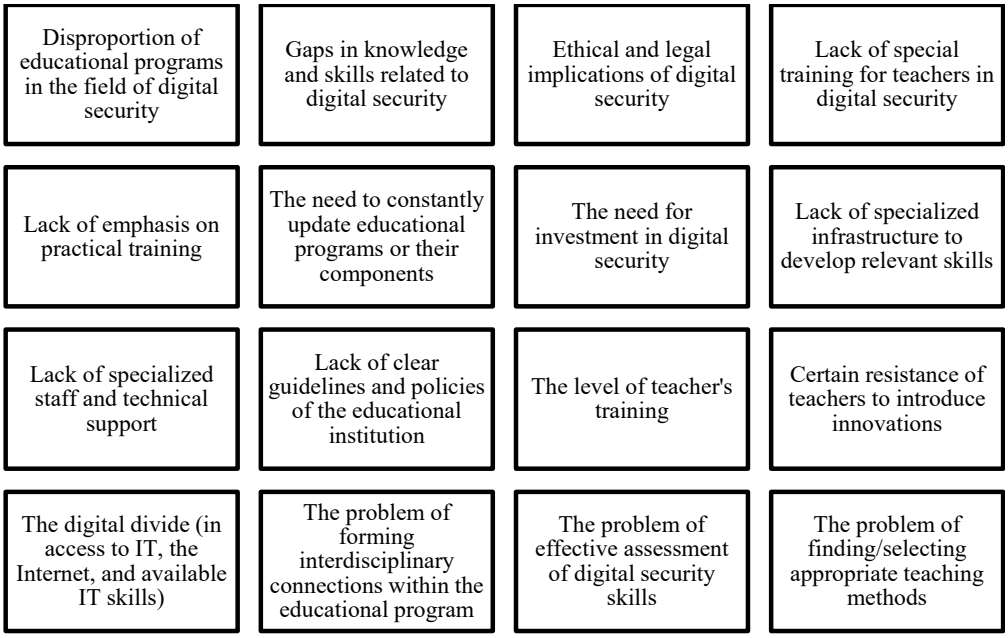

Fig.1. Problems of preparing future teachers of computer science for the formation of students' digital security skills

The problems identified during the analysis made it possible to formulate recommendations for improving the relevant educational programs. Consequently, educational curricula often need more depth and breadth for future computer science teachers to teach digital security students effectively. Therefore, the necessary improvement should include not only the formation of theoretical knowledge but also practical skills, which is possible based on introducing a separate educational component of the academic program for training computer science teachers.

Firstly, such an educational component should focus exclusively on digital security training. As a standalone course, it should delve into effective methodologies for teaching the often complex and abstract ideas and concepts of digital security. The course should provide teachers with the knowledge to develop engaging lessons appropriate for their age, from assessing students' understanding of digital threats and digital security to their ability to avoid digital threats. Such an educational component will allow you to study the problems of cybersecurity and the peculiarities of forming relevant skills more deeply.

Secondly, the formation of digital security skills should be integrated into the existing professional training courses (various educational components) to ensure the successful formation of relevant knowledge and skills in the field of digital security. This integration of educational components should be wider than technical aspects. It must include ethical considerations, legal frameworks, and social implications. This approach will ensure that digital security is not seen as an isolated topic but as an integral part of computer science education.

Thirdly, such an educational component should provide a variety of teaching methods and resources for their further transfer to the professional practice of the future computer science teacher. This can include hands-on exercises, simulations, and case studies of various problems (life situations, problem cases, etc.) to make the educational process more interesting and relevant.

We note the importance of continuous professional development of teachers in the field of digital security. The rapidly evolving nature of digital security requires continuous professional development as a constant learning process and continuous improvement of teaching practices, especially in the context of the evolution of technology *(Kozhukhova & Proshkin, 2021)*. Therefore, it is considered appropriate to conduct regular seminars/trainings to inform teachers about the latest threats, vulnerabilities, and best practices of digital security. Such classes should focus on mastering new information and its practical application in their teaching practice. Classes that provide opportunities for teachers to share their experiences with colleagues contribute to creating a productive learning environment.

Secondly, teachers should be provided access to online resources and communities. This would allow them to stay up-to-date with the latest developments in the field and get support from experts. Creating online forums using existing platforms such as Moodle could facilitate peer-to-peer learning and the sharing of best practices.

Thirdly, mentoring programs will be advisable to combine experienced teachers with those just starting in this field. This will provide an opportunity to learn from professionals and receive personalized recommendations. Mentors can provide support, feedback, and guidance on integrating digital security concepts into teaching practice.

Providing up-to-date digital security knowledge requires collaboration between educational institutions and IT professionals. The ultra-rapid development of digital threats requires partnerships to bridge the gap between academic knowledge and real-world practice *(Spang, 2014)*.

First, the creation of advisory boards can help disseminate information about current digital security challenges and positive practices for their enforcement. Board members can help develop an educational program or its component in compliance with industry needs and standards. Involving IT professionals in developing educational programs can ensure that the skills formed by the academic program are directly applicable to real-life situations.

Second, regular internships and integrated learning opportunities should be provided to provide students with hands-on experience in digital security. This will allow students to deepen and modernize their knowledge of digital security and gain experience under the mentorship of IT industry professionals, which will significantly improve their understanding of the challenges and complexities associated with digital security.

Third, collaborative research projects between educational institutions and industry can lead to the development of innovative teaching materials and resources. A collaborative approach ensures that the academic program remains relevant and in demand, providing future teachers with the knowledge and skills necessary to prepare their students for the challenges of the digital age *(Yuan et al., 2009)*. Additionally, such partnerships can lead to the development of valuable resources, such as online learning modules or interactive simulations, which can be widely used in the educational field.

3. Conclusions

The analysis of scientific sources has shown the relevance and importance of preparing future computer science teachers for the formation of digital security skills in students. The considered studies consistently emphasize the growing need for digital literacy, especially regarding security, in a world increasingly dependent on technology. Generalization of the current training state of future computer science teachers reveals significant gaps in their knowledge and skills in digital security, which in turn poses a substantial threat to the digital safety and well-being of young people, who are increasingly vulnerable to cyber threats and online risks.

The considered sources emphasize the diverse nature of digital security education. It's not just about learning technical skills. It is about awareness of the culture of digital citizenship and the responsible behavior of young people online. Future computer science teachers need training beyond technical security protocols and covering the social, ethical, and legal aspects of digital interaction. Research scientists emphasize the importance of forming interdisciplinary connections within the framework of educational programs for teacher training. This comprehensive approach requires a change in pedagogical strategies - encouraging active learning, developing critical thinking skills, and forming a culture of digital responsibility from the beginning of the student's educational journey. Building confidence and continuously developing teachers' digital competence is essential to counter emerging digital threats, empowering them to create a safe and reliable educational environment for their students.

The results of our research indicate the need to pay attention to developing comprehensive digital security training courses specifically designed for future and practicing computer science teachers. These courses should equip teachers with the technical knowledge to understand and explain safety concepts and provide them with pedagogical tools to integrate these concepts into their professional activities effectively. In addition, curricula should focus on developing critical thinking and problem-solving skills related to digital security, enabling teachers to respond to and adapt to new threats. Such an educational component should include practical exercises and simulations, allowing future teachers to gain practical experience with safety tools and methods.

The lack of a consistent and effective line in digital security in educational programs for the training of computer science teachers can have delayed negative consequences. The integration of digital security courses into computer science teacher training programs should go beyond isolated modules or elective courses and become a regulatory component of the educational program, and academic institutions should develop a culture of continuous learning for professional development in digital security.

References

1. Boer, Kh. M., Juwita, R., & Nurliah (2023). Penggunaan Metode Blanded Learning Untuk Meningkatkan Pengetahuan Literasi Digital Mahasiswa Ilmu Komunikasi Fisip Universitas Mulawarman. Journal of Da'wah and Communication, 3(1), 39-57. https://doi.org/10.28918/iqtida.v3i1.340.

2. Drushliak, M. G., Semenog, O. M., Grona, N. V., Ponomarenko, N. P., & Semenikhina, O. V. (2022). Typology of Internet resources for the development of infomedia literacy of young people. Information Technologies and Teaching Tools, 88(2), 1-22. https://doi.org/10.33407/itlt.v88i2.4786.

3. Fang, F. (2024). University Data Security Practice Under the Background of Digital Transformation. 2024 3rd International Conference on Artificial Intelligence and Computer Information Technology (AICIT), Yichang, China, 1-4. https://doi.org/10.1109/AICIT62434.2024.10730168.
4. Feng, L., Li, T., Yu, L., & Dong, Z. (2022). Application of OpenIPMP and Network Teaching Resources in Graduate Student Training. 2022 3rd International Conference on Education, Knowledge and Information Management (ICEKIM), Harbin, China, 50-53. https://doi.org/10.1109/ICEKIM55072.2022.00019.
5. Kozhukhova, K., & Proshkin, V. (2021). The content of the selective discipline "digital technologies in education" as a means of building digital competences in future teachers of the humanities. Collection of Scientific Papers of Uman State Pedagogical University, 3, 81–91. https://doi.org/10.31499/2307-4906.3.2021.241576.
6. Martin, F., Ceviker, E., & Gezer, T. (2024). From digital divide to digital equity: Systematic review of two decades of research on educational digital divide factors, dimensions, and interventions. Journal of Research on Technology in Education, 1-25. https://doi.org/10.1080/15391523.2024.2425442.
7. Mostaghimi, A, Olszewski, A, Bell, S, Roberts, D, & Crotty, B. (2017). Erosion of Digital Professionalism During Medical Students' Core Clinical Clerkships. JMIR Med Educ, 3(1), e9. https://doi.org/10.2196/mededu.6879.
8. Ng, D.T.K., Leung, J.K.L., & Su, J. (2023). Teachers' AI digital competencies and twenty-first century skills in the post-pandemic world. Education Tech Research Dev, 71, 137–161. https://doi.org/10.1007/s11423-023-10203-6.
9. Port, D., & Kessler, G. C. (2014). Introduction to IS Education and Training Minitrack. 2014 47th Hawaii International Conference on System Sciences, Waikoloa, HI, USA, 4921-4921. https://doi.org/10.1109/HICSS.2014.603.
10. Rahmatullah, A. S., Mulyasa, E., Syahrani, S., Pongpalilu, F., & Putri, R. E. (2022). Digital era 4.0: The contribution to education and student psychology. Linguistics and Culture Review, 6(S3), 89-107. https://doi.org/10.21744/lingcure.v6nS3.2064.
11. Rudenko, Y. O., Drushlyak, M. G., Shamonia, V. G., Ostroha, M. M., & Semenikhina, O. V. (2023a). Development of student's ability to resist information influences. Information Technologies and Learning Tools, 94(2), 54-71. https://doi.org/10.33407/itlt.v94i2.5162.
12. Rudenko, Y., Ahadzhanov-Honsales, K., Ahadzhanova, S., Batalova, A., Bieliaieva, O., Yurchenko, A., & Semenikhina, O. (2024). Modeling the choice of an online course for information hygiene skills using the saaty method. Informatyka, Automatyka, Pomiary W Gospodarce I Ochronie Środowiska, 14(2), 127–132. https://doi.org/10.35784/iapgos.5691.
13. Rudenko, Yu., Proshkin, V., Naboka, O., Yurchenko, A., & Semenikhina, O. (2023b). Using Bloom's taxonomy to assess information hygiene skills. In E. Smyrnova-Trybulska (ed.). E-learning & Artificial Intelligence (AI). „E-learning" Series, 15, Katowice–Cieszyn, 137–148. https://doi.org/10.34916/el.2023.15.12.
14. Spang, D. I. (2014). Curriculum Design and Assessment to Address the Industry Skills Gap. Paper presented at 2014 ASEE Annual Conference & Exposition, Indianapolis, Indiana. https://doi.org/10.18260/1-2--20236.
15. Tang, Y., & Fan, J. (2024). Challenges, Opportunities and Countermeasures of Education and Teaching Management in the Digital Age. Research and Commentary on Humanities and Arts, 1, 122-124. http://dx.doi.org/10.18686/rcha.v2i6.4722.
16. Yousif Yaseen, K. A. (2022). Importance of Cybersecurity in The Higher Education Sector 2022. Asian Journal of Computer Science and Technology, 11(2), 20–24. https://doi.org/10.51983/ajcst-2022.11.2.3448.

17. Yu, L., Harrison, L., Lu, A., Li, Z., & Wang, W. (2011). 3D Digital Legos for Teaching Security Protocols. IEEE Transactions on Learning Technologies,4(2), 125–137. https://doi.org/10.1109/TLT.2010.19.

18. Yuan, X., Malki, H., Song, G., & Waight, C. (2009). Introducing Advanced Wireless Sensor Networks Into Undergraduate Research. Paper presented at 2009 Annual Conference & Exposition, Austin, Texas. https://doi.org/10.18260/1-2—5023.

19. Yurchenko, A., Drushlyak, M., Sapozhnykov, S., Teplytska, S., Koroliova, L., & Semenikhina, O. (2021). Using online IT-industry courses in the computer sciences specialists' training. International Journal of Computer Science and Network Security, 21(11), 97–104. https://doi.org/10.22937/IJCSNS.2021.21.11.13.

20. Yurchenko, A., Rozumenko, A., Rozumenko, A., Momot, R., & Semenikhina, O. (2023). Cloud technologies in education: the bibliographic review. Informatyka, Automatyka, Pomiary W Gospodarce I Ochronie Środowiska, 13(4), 79–84. https://doi.org/10.35784/iapgos.4421.