A PEDAGOGICAL MODEL FOR PREPARING FUTURE INFORMATICS TEACHERS IN THE FIELD OF CYBERSECURITY

Khusenov Murodjon Zokhirovich

Associate Professor, Department of Artificial Intelligence and Information Security, Bukhara State University, Bukhara, Uzbekistan

E-mail: m.z.xusenov@buxdu.uz ORCID: 0000-0002-1533-3102

Abstract. The digitalization of general education has turned schools into objects of cyberattacks and made the informatics teacher the first line of defence and the principal translator of a culture of cybersecurity to pupils. International experience shows that pre-service teacher education reacts to this challenge fragmentarily: cybersecurity content appears in individual courses, but is not connected into an integral system of professional preparation. This article substantiates a pedagogical model for preparing future informatics teachers in the field of cybersecurity. On the basis of the analysis of international frameworks (CSEC2017, the NICE Workforce Framework, the UNESCO ICT Competency Framework for Teachers) and the TPACK construct, three clusters of target competences are identified: technical-operational, didactic-methodological and normative-ethical-personal. The model itself comprises four interconnected components — target-methodological, content, procedural-technological and evaluative-diagnostic — and is accompanied by a description of the pedagogical conditions of its realization. The model is intended for implementation in bachelor degree programmes that prepare informatics teachers, including the corresponding programmes of the universities of Uzbekistan; its experimental approbation is defined as the next stage of the research.

Keywords: *cybersecurity education; pre-service teacher preparation; informatics teacher; pedagogical model; TPACK; professional competence; cyber hygiene*

1. Introduction

The mass digitalization of school education — electronic journals and learning management systems, online services, personal devices of pupils and teachers — has substantially expanded the attack surface of educational institutions. Schools accumulate personal data of minors, and incidents ranging from phishing and account takeover to ransomware increasingly affect the general education sector. Under these conditions the informatics teacher occupies a double position: on the one hand, this teacher administers or co-administers school digital resources and must personally observe security requirements; on the other hand, it is precisely in informatics lessons that pupils receive their first systematic ideas about safe behaviour in the digital environment. The quality of school cybersecurity culture is therefore directly determined by the preparation of the informatics teacher.

Educational systems of different countries are responding to this challenge. In the United States, dedicated resources for school teachers have been created at the national level — the NICCS portal of the Cybersecurity and Infrastructure Security Agency aggregates training resources for K-12 teachers [2], and the Teach Cyber initiative provides curriculum guidelines, teaching materials and professional development workshops for secondary-school cybersecurity teachers, using the cloud-based virtual environment of the U.S. Cyber Range for hands-on practice [3, 4]. Researchers analyse theoretical approaches to introducing cybersecurity content into pre-service teacher education; in particular, work performed in the context of new state digital fluency standards, which include cybersecurity among the obligatory strands of school informatics preparation, examines how teacher-education programmes can prepare students to teach this content [1].

In the Republic of Uzbekistan the relevance of the problem is fixed at the level of state policy: the strategy “Digital Uzbekistan — 2030” defines the digitalization of education and the preparation of personnel for the digital economy among national

priorities [5], and the Law “On Cybersecurity” of 15 April 2022, No. LRU-764, establishes the legal foundations of the protection of the national segment of the Internet and the responsibilities of organizations, including educational ones [6]. Informatics is taught as a compulsory school subject, and pedagogical universities, among them Bukhara State University, prepare future informatics teachers. However, the analysis of practice shows that cybersecurity content in teacher-education programmes remains fragmentary: it is concentrated in separate technical courses, weakly connected with the methods of teaching informatics, and does not form the readiness of the future teacher to design lessons and extracurricular activities on cybersecurity.

The aim of this study is to substantiate a pedagogical model for preparing future informatics teachers in the field of cybersecurity. The objectives are: (i) to determine, on the basis of international frameworks, the composition of the cybersecurity-related competences of the informatics teacher; (ii) to construct a model that connects the target, content, procedural and evaluative components of such preparation; (iii) to characterize the pedagogical conditions of the effective realization of the model.

2. Materials and Methods

The study employed theoretical methods: the analysis of scientific publications on cybersecurity teacher preparation and of normative-methodological documents, the comparison of international competence frameworks, and pedagogical modelling. The international basis of the analysis was formed by the curricular guidelines CSEC2017, which structure the subject field of cybersecurity into eight knowledge areas and explicitly emphasize its interdisciplinary and applied character [8]; the NICE Workforce Framework for Cybersecurity (NIST Special Publication 800-181, Revision 1), which describes cybersecurity work in terms of task, knowledge and skill statements and includes work roles connected with education and training [9]; and the UNESCO ICT Competency Framework for Teachers (Version 3), which defines the digital

competences of the teacher across the aspects of understanding ICT in education policy, application of digital skills, and organization of learning [10].

The integrating theoretical construct of the model is TPACK — technological pedagogical content knowledge — according to which effective teaching with technology arises at the intersection of content knowledge, pedagogical knowledge and technological knowledge [7]. For the informatics teacher in the field of cybersecurity this means that technical knowledge of threats and protection mechanisms must be integrated with the didactics of the subject and with knowledge of the school informatics curriculum, and not exist alongside them. The construction of the model also relied on the competence-based approach (the result of preparation is described through demonstrable competences), the activity approach (competences are formed in quasi-professional activity) and the contextual approach (learning situations model the future professional context of the school).

The study is theoretical in character: it substantiates the structure and content of the model, while its experimental approbation in the educational process — with the formation of experimental and control groups and the measurement of the levels of competence formation — is planned as the next stage of the research, and no empirical results are reported in this article.

3. Results

3.1. The composition of target competences. The juxtaposition of CSEC2017 [8], the NICE framework [9], the UNESCO ICT CFT [10] and the requirements of school practice allows three clusters of cybersecurity-related competences of the future informatics teacher to be distinguished. The technical-operational cluster covers the foundations of information security: understanding of typical threats (phishing, malicious software, social engineering, account compromise), data and connection protection, secure configuration of operating systems and school services, password and access management, and the basics of incident response at the level of the educational organization. The didactic-methodological cluster comprises the ability to

design lessons and extracurricular activities on cybersecurity for different age groups: to select age-appropriate content, to use active formats — educational games and competitions of the picoCTF type [11], demonstration experiments in virtual laboratories — and to assess pupils' learning outcomes in this area. The normative-ethical-personal cluster includes knowledge of the national legal framework, above all the Law "On Cybersecurity" [6], the rules of processing and protecting pupils' personal data, the ethics of digital behaviour, and the teacher's personal culture of cyber hygiene as a model for pupils.

3.2. The structure of the model. The pedagogical model comprises four interconnected components. The target-methodological component fixes the goal — the formation of the future informatics teacher's readiness for professional activity in the conditions of digital threats and for the development of pupils' cybersecurity culture — and the methodological foundations described above (TPACK, the competence-based, activity and contextual approaches). The content component distributes the material across the stages of the bachelor programme: a propaedeutic module of personal cyber hygiene in the first-year ICT course; a fundamental module (threats, cryptography basics, network and system protection) within the information security course; a special didactic module "Methods of teaching cybersecurity at school" integrated into the course on methods of teaching informatics; and an elective deepening module (virtual laboratories, CTF practice, incident analysis). The procedural-technological component defines four stages of formation — motivational-orienting, knowledge-forming, activity-based and reflexive-professional — realized through lectures and seminars, practical work in virtual laboratory environments, micro-teaching (students conduct fragments of cybersecurity lessons for fellow students), the development of methodological products (lesson plans, scenario tasks, assessment materials) and the conduct of cyber-hygiene lessons during school pedagogical practice. The evaluative-diagnostic component establishes the criteria of formation — cognitive, operational-practical, didactic-design and motivational-value — and three levels (reproductive, productive, creative); the instruments include testing,

the defence of methodological products, observation of micro-teaching and practice lessons, and portfolio assessment.

3.3. Pedagogical conditions. The realization of the model presupposes: (1) the integration of cybersecurity content into the methods-of-teaching-informatics course, and not only into technical disciplines — this is the central condition that distinguishes teacher preparation from the preparation of technical specialists; (2) access to a practice environment — a virtual laboratory or training platforms — in which students can both develop their own skills and rehearse demonstrations for pupils; (3) the connection of preparation with school practice, so that each student conducts at least one cybersecurity lesson or extracurricular event under the guidance of a methodologist; (4) the readiness of university teaching staff, supported by professional development in cybersecurity didactics, by analogy with the workshop model of Teach Cyber [3]; (5) the systematic updating of content following the evolution of threats and of the national normative base [5, 6].

4. Discussion

The proposed model differs from existing approaches by the explicit integration of pedagogical and security frameworks. International curricular documents — CSEC2017 [8] and the NICE framework [9] — describe the subject field and professional roles of cybersecurity, but do not address the didactics of school teaching; the UNESCO ICT CFT [10] describes the digital competences of the teacher, but treats security only as one aspect of digital citizenship. The juxtaposition of these frameworks through the TPACK construct [7] makes it possible to describe precisely the position of the informatics teacher, whose professional task is double: to be a competent user-administrator and, simultaneously, a methodologist capable of transforming the technical content into age-appropriate learning activity. The studies of teacher-education responses to new digital fluency standards lead to a consonant conclusion: the introduction of cybersecurity into school standards is realizable only insofar as teacher-education programmes purposefully prepare students to teach this content [1].

The practical significance of the model for Uzbekistan consists in the fact that it can be realized within the existing structure of bachelor programmes by the redistribution and enrichment of the content of already taught courses, without the introduction of a separate discipline as an obligatory condition. The principal constraint is the capacity of university staff: the didactic module requires teachers who combine competence in security with competence in school methods, which justifies the condition of professional development formulated above and cooperation with practising specialists. The limitation of the study is its theoretical character: the model is substantiated analytically, and its effectiveness has not yet been verified experimentally. A quasi-experimental approbation in the preparation of future informatics teachers at Bukhara State University — with diagnostics of the levels of competence formation according to the criteria of the evaluative-diagnostic component — is planned as the continuation of this work.

5. Conclusion

The preparation of future informatics teachers in the field of cybersecurity is a necessary condition of the safe digitalization of school education and of the formation of pupils' cybersecurity culture. The contribution of this article is a pedagogical model that defines three clusters of target competences (technical-operational, didactic-methodological, normative-ethical-personal) and connects four components of preparation — target-methodological, content, procedural-technological and evaluative-diagnostic — with the pedagogical conditions of their realization. The distinctive feature of the model is the integration of cybersecurity content into the methodological preparation of the teacher on the basis of the TPACK construct and international frameworks, which transforms cybersecurity from an isolated technical course into a through line of professional formation. The directions of further research are the experimental approbation of the model, the development of an assessment toolkit for the identified criteria, and the creation of a methodological bank of school cybersecurity lessons shared between pedagogical universities.

References

1. Navarrete C. C. et al. Preparing preservice teachers to teach cyber security education: Examining theoretical approaches // IATED Conference Proceedings. 2023. [Online]. Available: https://library.iated.org/view/NAVARRETE2023PRE

2. Cybersecurity for K-12 Teachers // NICCS — National Initiative for Cybersecurity Careers and Studies, Cybersecurity and Infrastructure Security Agency (CISA). [Online]. Available: https://niccs.cisa.gov/education-training/cybersecurity-teachers

3. Teach Cyber: Resources and Professional Development for High School Cybersecurity Teachers. [Online]. Available: https://teachcyber.org/

4. Teach Cyber. Cybersecurity Curriculum Guidelines. [Online]. Available: https://teachcyber.org/cybersecurity-teaching-resources/curriculum-guidelines/

5. Decree of the President of the Republic of Uzbekistan No. UP-6079 “On Approval of the Strategy ‘Digital Uzbekistan — 2030’ and Measures for Its Effective Implementation”. October 5, 2020.

6. Law of the Republic of Uzbekistan “On Cybersecurity” No. LRU-764. April 15, 2022.

7. Mishra P., Koehler M. J. Technological Pedagogical Content Knowledge: A Framework for Teacher Knowledge // Teachers College Record. 2006. Vol. 108, No. 6. P. 1017–1054.

8. Joint Task Force on Cybersecurity Education. Cybersecurity Curricula 2017: Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity. ACM / IEEE-CS / AIS SIGSEC / IFIP WG 11.8, 2017. DOI: 10.1145/3184594.

9. Petersen R., Santos D., Smith M. C., Wetzel K. A., Witte G. Workforce Framework for Cybersecurity (NICE Framework). NIST Special Publication 800-181, Revision 1. Gaithersburg: National Institute of Standards and Technology, 2020.

10. UNESCO ICT Competency Framework for Teachers. Version 3. Paris: UNESCO, 2018.

11. picoCTF. Carnegie Mellon University. [Online]. Available: https://picoctf.org

12. ISC2. 2024 ISC2 Cybersecurity Workforce Study. International Information System Security Certification Consortium, 2024.