International Journal on Integrated Education (IJIE)

e-ISSN: 2620 – 3502
p-ISSN: 2615 – 3785

Volume: 9 Issue: 2 | June 2026

https://journals.researchparks.org/index.php/IJIE

Article

The Use of Modern Pedagogical Technologies in Teaching Information Security

Jasur Isroilovich Boymanov*[1]

1. Samarqand Campus, University of Economics and Pedagogy, Department of "Economics and Engineering Sciences"

* Correspondence: jasurboymanov432@gmail.com

Abstract: This work provides an in-depth analysis of the methods for forming fundamental knowledge in the process of teaching information security technologies. In the modern digital society, ensuring the security of information resources and information systems has become one of the most important socio-economic and technological challenges. Therefore, training specialists in the field of information security who possess qualified, profound theoretical knowledge and can adapt to rapidly changing technological environments is one of the pressing issues in the education system. The paper elucidates the concept of educational fundamentalization and its close connection with teaching information security disciplines. Fundamental knowledge includes not only practical skills but also a deep understanding of basic concepts such as cryptography principles, mathematical and logical protection of information, algorithm theory, network technologies, operating system architecture, and security policies. The article systematizes and defines effective approaches to forming fundamental knowledge, which is necessary for successfully teaching information security technologies. This includes, in particular, focusing on interdisciplinary integration of study objectives; problem-based learning and teaching conceptual modeling; alignment of theory with practical application; and a focus on the development of analytical and logical thought. This way they do not only use a tool, but understand the theoretical basis for security processes.

Keywords: Information Security, Information Security Technologies, Fundamental Knowledge, Educational Fundamentalization, Teaching Methodology of Information Security, Pedagogical Technologies, Interdisciplinary Integration, Alignment of Theory and Practice, Professional Competencies, Cybersecurity Education, Educational and Methodological Support, Higher Education, Digital Learning Environment, Problem-Based Learning

Citation: Boymanov J. I. The Use of Modern Pedagogical Technologies in Teaching Information Security. International Journal on Integrated Education (IJIE) 2026, 9(2), 91-94.

Received: 15th Mat 2026
Revised: 05th Apr 2026
Accepted: 20th Apr 2026
Published: 02nd May 2026

Copyright: © 2026 by the authors. Submitted for open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/)

1. Introduction

Today, the rapid development of digital technologies and the deep penetration of information and communication systems into all sectors have made information security a globally pressing issue. Extensive use of information resources in public administration, education, healthcare, banking and finance, industry, and social sectors requires reliable protection of their confidentiality, integrity, and availability. At the same time, the increasing number of cyberattacks and the growing complexity of threats to information systems underscore the need to train highly qualified information security specialists.

Training specialists in information security requires not only teaching modern technologies and practical tools but also systematically and deeply forming the fundamental knowledge that underpins them.[1] An overly practice-oriented educational approach risks being limited to rapidly obsolete knowledge. In contrast, education based

on fundamental knowledge—including mathematical foundations, algorithmic thinking, cryptography theory, network architecture, operating system principles, and theoretical models of information protection—ensures professional stability and adaptability. From this perspective, the concept of educational fundamentalization is considered a priority approach in teaching information security technologies.[2]

Educational fundamentalization aims to develop deep theoretical preparation, ensure coherence and systematic understanding of knowledge, and foster independent thinking and analytical skills. This approach allows students to comprehend not only technological innovations but also the scientific foundations of information security disciplines[3].

2. Research Methodology

The process of educational fundamentalization in teaching information security technologies is implemented based on a systemic-activity approach. This approach considers the educational process as a unified set of interrelated elements. The systemic-activity methodology encompasses defining learning goals and principles, determining educational content, selecting teaching forms, methods, and tools, and evaluating learning outcomes. It relies on scientific and pedagogical research in information security and established theoretical views on teaching organization.[4] To effectively teach information security technologies, it is essential to plan students' preparatory content in computer science, mathematics, and information science education with coherence and interrelation. The unique needs and directions of information security courses must be considered. For example, courses such as "Organizational Information Security," "Protection and Processing of Confidential Documents," "Cryptographic Security of Information," "Hardware-Software Protection of Information," and "Protection of Information Processes in Computer Systems" should be organized not only within a single department but also in collaboration with natural science and specialty departments based on interdisciplinary connections.[5]

Instruction in information security technologies is conducted through traditional and active learning forms, including lectures, seminars, and laboratory work. Lectures play a crucial role in achieving didactic goals and serve several educational functions. They primarily provide informational functions, enabling students to study the scientific foundations of information and information processes, current problems of information security, main principles, threats to information systems, malware, protection methods, methodological foundations of information security theory, concepts of information protection, strategies and tools for information security, and the social significance of information security systems.

The article systematizes and defines effective approaches to forming fundamental knowledge, which is necessary for successfully teaching information security technologies. This includes, in particular, focusing on interdisciplinary integration of study objectives; problem-based learning and teaching conceptual modeling; alignment of theory with practical application; and a focus on the development of analytical and logical thought. This way they do not only use a tool, but understand the theoretical basis for security processes.[6]

3. Results and Discussion

Using a systemic approach in teaching information security technologies encourages students' engagement in research activities and acquisition of necessary skills in applied computer science. The approach organizes the educational process as a holistic system in which goals, content, methods, tools, and outcomes are interrelated[7]. The activity-based approach transforms students from passive recipients of knowledge into active subjects.

The development of the activity-based approach draws on the works of renowned scholars such as L.S. Vygotsky, P.Ya. Galperin, V.V. Davidov, L.V. Zankov, A.N. Leontiev, S.L. Rubinshtein, N.F. Talizina, and D.B. Elkonin. For example, L.S. Vygotsky emphasized that development and knowledge acquisition are inseparable in the learning process, with instruction being a key factor in personal development[8]. P.Ya. Galperin highlighted that the goal of teaching is not simply transmitting ready-made knowledge but forming the ability for conscious action. V.V. Davidov argued that teaching in activity-based education focuses on managing students' acquisition of knowledge, skills, and competencies rather than mere knowledge transfer. This approach underpins developmental education systems characterized by specific pedagogical technologies, through which mechanisms for assimilating culture in various forms are developed[9]. Using a systemic approach in teaching information security allows students to integrate theoretical knowledge with practical activities, develop independent analytical and decision-making skills in the field of information security, and perform practical tasks while deeply understanding information security theory[10]. The fundamentals of developmental education were initially formed by pedagogues such as F.A. Diesterweg and I.G. Pestalozzi and further developed by scholars including Yu.K. Babansky, L.S. Vygotsky, P.Ya. Galperin, V.V. Davidov, L.V. Zankov, L.Ya. Zorina, A.N. Leontiev, N.G. Salmina, A.V. Usova, D.B. Elkonin, and I.Ya. Yakimanskaya[11]. Since the mid-1980s, the systemic-activity approach has rapidly evolved as an independent scientific field. Its application in education has been extensively studied by N.I. Aksenova, A.G. Asmolov, N.S. Buslova, V.A. Dalinger, O.A. Maligina, A.B. Khutorskoy, V.D. Shadrikov, and others. N.I. Aksenova notes that systemic-activity education activates internal potential, creating conditions for developing well-rounded, morally sound, socially active, professionally competent individuals capable of continuous self-improvement. A.G. Asmolov emphasizes that modern education's main task is not to provide ready knowledge but to teach students to learn independently. The study analyzed methods used in teaching information security under the framework of educational fundamentalization, the content and structure of teaching materials, and their impact on students' acquisition of fundamental knowledge, practical skills, and professional competencies[12]. Results indicate that effective teaching requires integrating information security content with fundamental subjects such as computer science, mathematics, cryptography, algorithm theory, and information processes. Such integration enables students to understand information security phenomena and processes scientifically and enhances analytical thinking. Effective course organization requires alignment of lectures, seminars, and laboratory sessions. Lectures present the fundamental principles of information security theory, threats, and protection mechanisms. Seminars involve analysis of problem-based scenarios and justification of security solutions[13]. Laboratory work develops practical skills in cryptographic algorithms, hardware-software protection tools, and information protection technologies. Teaching materials integrate fundamental concepts with modern information security technologies, reinforced through practical examples, modeling, situational tasks, and project work, allowing students to apply knowledge to real-world information security challenges[14].

4. Conclusion

Teaching information security technologies under educational fundamentalization is a priority in modern education. In the context of fast-paced digital transformation, rapid adoption of AI technologies and volume increasing information flows, it is essential to cultivate in the younger generation an information security culture. These include learning the basics, studying the theory, and putting it into practice. This includes studying core information security concepts, the theoretical foundations of cryptography, cyber attack defenses, network safety protocols, etc. Fundamental knowledge helps students grow to be independent analytical thinkers, threat analysts and decision-makers who can make optimal security decisions. The study of information security has adopted many

innovative pedagogical methods, including simulation technologies and virtual laboratories, interactive platforms, project-based learning, case studies and problem-based learning (PBL) that bring education closer to practice by means of gamification. Such methods encourage analytical thinking, creativity, teamwork and quick response to real-life cyber attacks. Lastly, curriculum should be current and one that conforms to international paradigms; with practical illustrative examples from the world of security. Thus, educational fundamentalization provides an opportunity for scientific, systematic and practical development of teaching information security technologies that will improve the culture of safe activity of future specialists in digital environments.[15].

REFERENCES

[1] J. Andress, The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice. Oxford, U.K.: Syngress, 2019.

[2] T. A. Jumaniyozova, "Enhancing cybersecurity culture in higher education institutions: Developing competencies of teachers, staff, and students," Journal of Academic Research and Trends in Educational Sciences, no. 6, p. 1027, 2024.

[3] M. A. Mustaffaqulov, Z. S. Eshturdiyeva, and R. B. Abduraximova, "Ensuring cybersecurity in the educational process," Journal of Academic Research and Trends in Educational Sciences, p. 1007, 2024.

[4] A. Normoʻminov, D. Kendjaeva, and A. Primbetov, "The role of cybersecurity in the educational process," Eurasian Journal of Academic Research, no. 6, pp. 881–886, 2024.

[5] G. I. Qosimova, "Cybersecurity: Modern transformation of education," Modern Transformation of Education, no. 6, pp. 881–886, 2024.

[6] I. R. Mirzoev, Fundamentals of Information Security. Tashkent, Uzbekistan: Fan va Texnologiya, 2020.

[7] I. Abdullaev and A. Karimov, Information Culture and Information Security. Tashkent, Uzbekistan: Iqtisod-Moliya, 2018.

[8] C. Curricula, "Curriculum guidelines for post-secondary degree programs in cybersecurity," no. 3, pp. 40–50, 2017.

[9] Oʻ. Q. Tolipov and M. Usmonboyeva, Pedagogik texnologiyalar: nazariya va amaliyot. Tashkent, Uzbekistan: Fan va Texnologiya, 2012.

[10] R. Ishmuhamedov, A. Abduqodirov, and A. Pardaev, Ta'limda innovatsion texnologiyalar. Tashkent, Uzbekistan: Iste'dod, 2010.

[11] J. Gʻ. Yoʻldoshev and S. A. Usmonov, Pedagogik texnologiya asoslari. Tashkent, Uzbekistan: Oʻqituvchi, 2004.

[12] N. N. Azizxoʻjayeva, Pedagogik mahorat. Tashkent, Uzbekistan: Nizomiy nomidagi TDPU nashriyoti, 2006.

[13] J. H. Flavell, "Metacognition and cognitive monitoring: A new area of cognitive–developmental inquiry," American Psychologist, 1979.

[14] B. J. Zimmerman, "Becoming a self-regulated learner: An overview," Theory Into Practice, 2002.

[15] G. Schraw and R. S. Dennison, "Assessing metacognitive awareness," Contemporary Educational Psychology, 1994.