

METHODS OF DEVELOPING STUDENTS' INFORMATION SECURITY COMPETENCE IN THE CONTEXT OF USING ARTIFICIAL INTELLIGENCE TOOLS

Mustafojev Shahzod

Bukhara International University

E-mail: shahzod@buxdpi.uz

ORCID: <https://orcid.org/0009-0007-8584-1237>

Abstract. The rapid development of artificial intelligence (AI) technologies has significantly transformed the educational environment, creating new opportunities for knowledge acquisition, scientific research, and independent learning. At the same time, the widespread use of AI tools has introduced additional challenges related to information security, personal data protection, digital privacy, cyber threats, academic integrity, and the reliability of AI-generated content. In this context, the development of students' information security competence has become an essential objective of contemporary higher education. This article examines the theoretical and methodological foundations of developing students' information security competence in the context of AI-assisted learning. Particular attention is given to the integration of problem-based learning, project-based learning, case-study analysis, simulation-based training, collaborative learning, and reflective assessment into the educational process. A competency-based methodological approach is proposed that combines technical knowledge, practical cybersecurity skills, critical thinking, ethical responsibility, and the ability to assess AI-related risks. The article argues that the systematic integration of these methods into higher education can contribute to students' ability to use AI tools safely, responsibly, and effectively.

Keywords: artificial intelligence, information security, information security competence, higher education, digital literacy, cybersecurity, personal data protection, AI ethics, pedagogical methods, critical thinking.

Introduction

The digital transformation of higher education has created new conditions for organizing teaching, learning, and scientific research. Artificial intelligence technologies, particularly generative AI systems, are increasingly used to prepare educational materials, explain complex concepts, analyze information, generate computer code, translate texts, and support academic writing. These technologies can improve access to information, facilitate personalized learning, and enhance the efficiency of educational activities. However, their implementation also requires students to develop a comprehensive understanding of information security and responsible digital behavior. The use of AI tools involves several interconnected risks, including the unintended disclosure of personal information, confidential academic materials, research data, and institutional information. Furthermore, AI-generated responses may contain inaccurate information, fabricated references, biased conclusions, or misleading recommendations. Cybercriminals may also exploit AI technologies to produce convincing phishing messages, automate social engineering attacks, and create deceptive digital content. Consequently, students need more than basic digital literacy; they must acquire the knowledge, practical skills, attitudes, and ethical principles necessary to identify information security threats, evaluate the reliability of digital information, protect personal data, and make informed decisions when using AI-based applications. UNESCO's *Guidance for Generative AI in Education and Research* emphasizes the importance of a human-centred approach to generative AI, including data privacy, ethical considerations, and appropriate pedagogical implementation (Miao & Holmes, 2023). Similarly, the National Institute of Standards and Technology (NIST) provides

frameworks for identifying, assessing, and managing cybersecurity and AI-related risks. These approaches provide a relevant conceptual foundation for integrating information security education into AI-supported learning environments. The purpose of this article is to identify and substantiate effective pedagogical methods for developing students' information security competence in the context of using artificial intelligence tools and to propose a methodological framework that integrates theoretical knowledge, practical activities, ethical reflection, and competency-based assessment into the educational process.

Theoretical Foundations of Information Security Competence

Information security competence can be defined as an integrated characteristic of an individual encompassing the knowledge, skills, abilities, attitudes, and ethical principles required to protect information resources, recognize digital threats, manage information security risks, and behave responsibly in digital environments. Within the context of AI-assisted education, this competence acquires an expanded meaning because students must understand not only conventional cybersecurity principles but also the specific characteristics and limitations of AI systems, including the processing of user-provided information, the generation of potentially misleading content, algorithmic bias, and the risks associated with the disclosure of sensitive data. From a pedagogical perspective, information security competence may be conceptualized as a multidimensional construct consisting of cognitive, operational and practical, analytical and critical-thinking, ethical and responsible-use, and self-regulatory components. The cognitive component includes knowledge of cybersecurity principles, personal data protection, authentication, access control, phishing, malware, social engineering, AI-related vulnerabilities, and responsible AI use. Students should understand the basic mechanisms through which digital information is collected, processed, stored, and transmitted. The operational and practical component involves the ability to apply security measures in real or simulated situations, including creating strong passwords, enabling multifactor authentication, recognizing suspicious messages, configuring privacy settings, identifying unsafe links, and selecting appropriate methods for protecting digital files. The analytical and critical-thinking component enables students to evaluate the reliability of AI-generated information, compare AI outputs with authoritative sources, identify fabricated references, recognize possible manipulation, and distinguish verified evidence from unsupported claims. The ethical and responsible-use component encompasses respect for privacy, intellectual property, confidentiality, academic integrity, and the rights of other users. Students should recognize that the availability of an AI tool does not automatically justify the disclosure of information or the unrestricted use of generated content. The self-regulatory component involves the ability to monitor personal digital behavior, identify weaknesses in one's own security practices, respond appropriately to emerging threats, and continuously improve information security knowledge. These components are interdependent, since theoretical knowledge alone cannot ensure safe behavior if students are unable to apply security principles in practice, while technical skills are insufficient when students do not understand the ethical implications of AI use or cannot critically evaluate the information generated by intelligent systems. Therefore, the development of information security competence should be organized as a continuous educational process combining knowledge acquisition, practical application, critical evaluation, ethical reasoning, and reflective learning.

Methodological Approaches to Developing Information Security Competence

The development of students' information security competence requires the application of pedagogical methods that correspond to the complexity and dynamic nature of AI-related threats. Although traditional lecture-based instruction remains useful for introducing fundamental concepts, it should be complemented by active, practice-oriented, and learner-centred methods. The competency-based approach focuses on the practical application of knowledge rather than the memorization of theoretical information. Within this approach, educational objectives should be formulated in terms of observable student performance. Instead of requiring students merely to define personal data protection, for example, an instructor may ask them to evaluate whether a particular

prompt contains sensitive information and propose a safer alternative. Similarly, students may be required to identify security weaknesses in a hypothetical AI-supported learning scenario and justify appropriate protective measures. The implementation of this approach involves establishing clearly defined learning outcomes, selecting corresponding educational activities, and developing assessment criteria that measure actual competence. At the end of the learning process, students should be able to identify common information security risks, apply appropriate protection mechanisms, assess the reliability of AI-generated information, and justify their decisions from technical and ethical perspectives. The competency-based approach therefore provides a foundation for connecting theoretical instruction with practical performance and responsible digital behavior.

Problem-based learning is an effective method for developing students' analytical abilities and decision-making skills because it begins with a problem that requires investigation, discussion, and the development of a justified solution. In the context of AI and information security, students may be presented with a scenario in which a learner enters personal information, unpublished research findings, or confidential institutional documents into a publicly accessible AI service. They are then required to identify potential risks, determine which information should not be disclosed, and propose alternative approaches to completing the task. Another problem may involve an AI-generated explanation containing incorrect cybersecurity recommendations, requiring students to identify inaccuracies, consult reliable sources, and formulate a corrected response. The educational value of this method lies in its capacity to develop independent reasoning and situational awareness, enabling students to analyze threats systematically rather than relying on general rules without understanding their practical significance. Problem-based learning also encourages students to recognize that information security decisions often involve competing considerations, including convenience, confidentiality, accuracy, and ethical responsibility. Project-based learning complements this approach by providing opportunities to apply information security knowledge through the development of tangible educational products. Students may develop an information security guide for university students, design a checklist for the safe use of generative AI, prepare an educational presentation on phishing prevention, or create a prototype of an AI-use policy for an academic course. Another possible project involves developing a decision-making framework that helps students determine whether particular information can be submitted to an AI system. Such a framework may classify information into public, internal, confidential, and sensitive categories, subject to the institution's applicable data protection policies. The project process should include problem identification, information gathering, planning, development, peer review, and presentation, with students explaining the security principles underlying their proposed solutions. This method contributes to practical competence because students must transform abstract security principles into usable recommendations while strengthening communication, collaboration, creativity, and accountability.

Case-study analysis involves examining specific situations that illustrate information security problems and the consequences of inappropriate digital behavior. Relevant cases may include phishing emails generated with AI assistance, the accidental disclosure of personal information through chatbots, fabricated academic references, the unauthorized use of confidential research data, and the manipulation of AI-generated images or documents. During the analysis, students should identify the main security problem, determine the information assets at risk, examine the actions that contributed to the incident, and propose preventive and corrective measures. For example, a case may describe a student who receives an email apparently sent by a university administrator requesting account credentials through an unfamiliar link. Students must examine the sender's address, the wording of the message, the destination of the link, and the urgency of the request, explaining how AI-generated language may make fraudulent communications more convincing. Case studies are particularly valuable because they connect theoretical knowledge with realistic situations without requiring students to expose their own accounts or confidential information. Instructors should

therefore use fictionalized or anonymized cases to avoid unnecessary disclosure of personal data. Simulation-based learning further enables students to practise security-related decisions in controlled educational environments and is especially useful for developing procedural skills and appropriate responses to potential incidents. Practical activities may include identifying simulated phishing messages, evaluating password strength using approved educational tools, configuring privacy settings in demonstration accounts, classifying information according to sensitivity, and practising incident reporting procedures. AI-related simulations may involve comparing different prompts to determine whether they request sensitive information, evaluating generated content for misleading statements, or identifying attempts to manipulate an AI system into producing inappropriate disclosures. Such activities should be conducted in authorized environments using fictional data and controlled scenarios. Students should not be encouraged to test security mechanisms on real systems without permission or submit actual confidential information to external AI services. The effectiveness of simulation-based training depends on structured feedback, through which students explain their decisions, identify mistakes, and formulate strategies for preventing similar incidents.

Collaborative learning creates conditions for exchanging knowledge, discussing alternative solutions, and developing collective responsibility for information security. Students may work in small groups to analyze an AI-related security incident, assess the reliability of generated content, or prepare recommendations for the responsible use of AI in academic activities. Peer assessment can be organized through structured evaluation criteria, enabling students to determine whether another group's proposed AI-use policy addresses data confidentiality, authentication, information verification, citation practices, and incident reporting. This method encourages students to articulate their reasoning, consider alternative perspectives, and identify weaknesses in proposed solutions. It also demonstrates that information security is not exclusively an individual responsibility but a shared concern involving students, teachers, researchers, and educational institutions. Reflective learning and digital self-assessment further help students evaluate their own digital behavior and recognize the relationship between personal decisions and information security outcomes. Students may maintain a learning journal in which they record the security principles learned, analyze hypothetical or anonymized incidents, and reflect on changes in their approach to using AI tools. Self-assessment questionnaires can be used to evaluate students' awareness of password management, data protection, source verification, phishing recognition, and ethical AI use. However, self-reported confidence should not be treated as sufficient evidence of competence. A more reliable assessment combines reflection with practical tasks, scenario-based questions, and instructor feedback, enabling educators to determine whether students can translate awareness into appropriate action.

The Role of AI Literacy and Critical Evaluation

An essential condition for developing information security competence is the integration of AI literacy into the curriculum. Students should understand the basic capabilities and limitations of AI systems and recognize that generated responses may be incomplete, inaccurate, biased, or unsupported by reliable evidence. One important educational method is the comparative evaluation of AI-generated information. Students can ask an AI system to explain a cybersecurity concept and then compare the response with official guidelines, academic publications, and recognized institutional resources. The comparison should focus on factual accuracy, the relevance of references, the currency of recommendations, and the consistency of the information with established security principles. Another important method is citation verification. Students should be trained to check whether cited publications exist, whether their bibliographic details are correct, and whether the cited source actually supports the claim being made. This is particularly important because generative AI systems can produce plausible-looking but nonexistent references. AI literacy should also include an understanding of the risks associated with prompts and uploaded materials. Students need to recognize that information entered into an AI service may be processed according to the service provider's terms, technical architecture, and data retention policies. The precise handling of submitted

data varies between systems and configurations; therefore, students should consult the relevant privacy documentation rather than assume that all AI interactions are confidential. The educational objective is not to discourage the use of AI tools but to develop the capacity to evaluate their appropriateness, limitations, and security implications. Such an approach supports informed decision-making and promotes responsible participation in digital academic environments.

Integrating Information Security Education into the Curriculum

The development of information security competence should not be limited to a single lecture or specialized course; instead, it should be integrated into different academic subjects and supported by institutional policies. In computer science courses, students may study authentication, encryption, access control, secure software practices, and the technical characteristics of AI systems. In research methodology courses, they may examine research data protection, source verification, academic integrity, and the responsible use of AI in scholarly writing. In language and humanities courses, students may analyze misinformation, AI-generated texts, manipulated media, and the ethical implications of automated content production. Instructors should explain the distinction between publicly available information and confidential material. Before using AI tools for academic tasks, students should determine whether the intended information can be shared under institutional rules, applicable law, and the service provider's data policies. At the institutional level, universities should establish clear guidelines concerning acceptable AI use, the protection of student and research data, disclosure of AI assistance, and procedures for reporting information security incidents. UNESCO's guidance supports the development of human-centred educational policies that consider privacy, ethics, and pedagogical appropriateness when implementing generative AI (Miao & Holmes, 2023). In addition, NIST's Cybersecurity Framework 2.0 provides a structured approach to understanding, prioritizing, and communicating cybersecurity risks (Pascoe et al., 2024). These frameworks can inform institutional planning, although they should be adapted to the educational context, local legal requirements, and the specific needs of students and teachers.

A Proposed Methodological Model for Developing Students' Information Security Competence

Based on the pedagogical approaches discussed above, a methodological model can be proposed that integrates diagnostic, motivational, instructional, practical, and evaluative stages. The diagnostic stage identifies students' existing knowledge, digital habits, and ability to recognize common security threats. Initial assessment may include scenario-based questions, short practical tasks, and an evaluation of students' understanding of personal data protection and AI-related risks. The motivational stage develops students' awareness of the importance of information security. Teachers can use realistic case studies, discussions of digital incidents, and demonstrations of the consequences of unsafe information-sharing practices to establish the relevance of the subject. The instructional stage provides systematic knowledge of cybersecurity, data privacy, AI literacy, ethical digital behavior, and information verification. The content should progress from fundamental concepts to more complex situations involving AI-assisted learning and research. The practical stage enables students to apply acquired knowledge through projects, simulations, collaborative problem-solving, and case-study analysis. Activities should reflect realistic educational situations while avoiding exposure to actual sensitive data. The evaluative stage measures the development of competence through practical performance, analytical tasks, reflective reports, and structured feedback. Assessment should determine not only whether students can identify a threat but also whether they can justify and implement an appropriate response. The proposed model is based on the principle of continuity: assessment results should inform subsequent instruction, allowing teachers to identify weaknesses and adapt learning activities to students' needs.

To evaluate the development of competence systematically, four principal criteria may be applied: cognitive, practical, analytical, and ethical-reflective. The cognitive criterion assesses students' understanding of information security principles, AI-related risks, data protection, and

responsible digital behavior. The practical criterion measures their ability to apply security measures, recognize suspicious activities, manage information appropriately, and respond to simulated incidents. The analytical criterion evaluates their capacity to verify AI-generated content, distinguish reliable information from misleading claims, and justify decisions using credible sources. The ethical and reflective criterion examines their respect for privacy, confidentiality, academic integrity, and responsible AI use, as well as their ability to evaluate and improve their own digital practices. For practical implementation, these criteria may be assessed using a four-level scale consisting of initial, developing, proficient, and advanced levels. The assessment rubric should define observable indicators for each level and be applied consistently across learning activities. For example, a student at the initial level may recognize an obvious phishing message but struggle to explain its characteristics. A student at the proficient level should be able to identify several warning signs, justify the assessment, and recommend appropriate protective actions. An advanced student should additionally be able to compare alternative responses, evaluate contextual risks, and explain the limitations of the chosen solution. The use of a transparent assessment framework makes the development of information security competence more measurable and supports the alignment of educational objectives, instructional methods, and learning outcomes.

Results and Discussion

The theoretical analysis indicates that the development of students' information security competence in AI-supported educational environments requires a comprehensive combination of pedagogical methods rather than reliance on isolated instructional activities. The competency-based approach establishes a direct relationship between educational objectives and practical security behavior, enabling instructors to evaluate students' ability to apply knowledge instead of measuring only their theoretical understanding. Problem-based and case-based learning encourage students to recognize the contextual nature of information security risks and understand that appropriate decisions depend on the type of information involved, the purpose of AI use, the characteristics of the platform, and the possible consequences of disclosure. Project-based and collaborative learning provide opportunities to develop practical solutions, communicate security recommendations, and share responsibility for digital safety, while also supporting research skills and professional competencies. Simulation-based training and reflective assessment strengthen the connection between knowledge and behavior. By practising responses in controlled environments and reviewing their decisions, students can develop more consistent security habits. AI literacy and critical evaluation are equally indispensable because secure AI use involves both technical protection and epistemic judgment. Students must determine whether generated information is reliable and whether the information they submit is appropriate for the intended platform. These conclusions are consistent with the general principles of risk management described in the NIST AI Risk Management Framework, which emphasizes the importance of identifying, assessing, and managing risks associated with AI systems (Tabassi, 2023). The framework can complement educational approaches by providing a structured vocabulary for discussing trustworthiness, privacy, security, accountability, and risk mitigation. Nevertheless, the proposed methodological model should be regarded as a theoretically grounded framework rather than a set of experimentally validated findings. Its effectiveness should be examined through empirical research involving clearly defined learning outcomes, appropriate comparison procedures, and pre- and post-intervention assessments. Future research could investigate the extent to which different combinations of pedagogical methods improve students' ability to identify phishing attempts, protect personal data, verify AI-generated information, and make responsible decisions in academic settings. Such research would provide a stronger empirical basis for selecting instructional methods and evaluating their effectiveness across different educational contexts.

Conclusion

The development of students' information security competence has become an important pedagogical objective in the context of the expanding use of artificial intelligence tools in higher education. The growing integration of AI into learning and research requires students to possess not only digital skills but also the ability to recognize information security threats, protect personal data, evaluate the reliability of generated content, and use digital technologies ethically and responsibly. The analysis presented in this article demonstrates the pedagogical relevance of competency-based instruction, problem-based learning, project-based learning, case-study analysis, simulation-based training, collaborative learning, and reflective assessment. The integration of these methods can support the development of cognitive, practical, analytical, ethical, and self-regulatory dimensions of information security competence. A systematic methodological model should combine diagnostic assessment, motivation, theoretical instruction, practical activities, and outcome evaluation. Its implementation requires coordinated efforts by educators, students, and educational institutions, together with clear policies governing AI use, privacy protection, and academic integrity. Particular importance should be assigned to AI literacy, source verification, safe information-sharing practices, and the ability to recognize the limitations of AI-generated outputs. Students should be encouraged to use AI as a supportive educational resource while retaining responsibility for their decisions, academic work, and the protection of information. In conclusion, the effective development of information security competence requires a continuous, practice-oriented, and ethically informed educational process. The proposed framework provides a theoretical and methodological basis for further empirical research and for designing educational interventions aimed at promoting the safe, responsible, and informed use of artificial intelligence in higher education.

References

1. Miao, F., & Holmes, W. *Guidance for generative AI in education and research*. UNESCO.2023. <https://doi.org/10.54675/EWZM9535>
2. Pascoe, C., Quinn, S., & Scarfone, K. *The NIST Cybersecurity Framework (CSF) 2.0*. National Institute of Standards and Technology. 2024. <https://doi.org/10.6028/NIST.CSWP.29>
3. Tabassi, E. *Artificial Intelligence Risk Management Framework (AI RMF 1.0)*. National Institute of Standards and Technology.2023. <https://doi.org/10.6028/NIST.AI.100-1>
4. National Institute of Standards and Technology. *NIST Cybersecurity Framework 2.0: Resource and Overview Guide (NIST SP 1299)*. 2024. <https://doi.org/10.6028/NIST.SP.1299>
5. UNESCO. *Recommendation on the Ethics of Artificial Intelligence*. United Nations Educational, Scientific and Cultural Organization. 2021. <https://unesdoc.unesco.org/ark:/48223/pf0000381137>