

**THE PEDAGOGICAL SIGNIFICANCE OF DEVELOPING STUDENTS'
INFORMATION SECURITY COMPETENCE IN THE CONTEXT OF USING
ARTIFICIAL INTELLIGENCE TOOLS****Mustafojev Shahzod**

Bukhara International University

E-mail: shahzod@buxdpi.uzORCID: <https://orcid.org/0009-0007-8584-1237>

Abstract. The widespread integration of artificial intelligence (AI) tools into higher education has significantly transformed the organization of teaching, learning, and scientific research. Although AI technologies provide opportunities for personalized learning, rapid information retrieval, and the development of students' independent learning skills, they also create new challenges associated with information security, personal data protection, digital privacy, academic integrity, and the reliability of generated content. Under these circumstances, developing students' information security competence has acquired considerable pedagogical significance. This article examines the educational importance of developing information security competence in the context of AI-assisted learning, focusing on its role in promoting digital responsibility, critical thinking, ethical decision-making, cybersecurity awareness, and independent learning. Particular attention is given to the pedagogical conditions necessary for integrating information security principles into the educational process, including competency-based instruction, practice-oriented learning, interdisciplinary integration, reflective activities, and formative assessment. The article substantiates the importance of creating an educational environment in which students learn not only to use AI tools effectively but also to assess associated risks, protect sensitive information, verify AI-generated content, and make responsible decisions. It is concluded that the systematic development of information security competence constitutes an important component of contemporary digital education and contributes to the preparation of digitally competent, ethically responsible, and critically thinking professionals.

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

Introduction

The development of artificial intelligence technologies has become one of the significant factors influencing the modernization of contemporary education. AI-based applications are increasingly used by university students to search for information, prepare academic assignments, translate scientific texts, analyze data, generate ideas, and support independent research. These applications can improve the accessibility of educational resources, facilitate individualized learning, and provide additional opportunities for developing professional competencies. However, the expansion of AI use also requires a reconsideration of the pedagogical objectives associated with digital literacy, information security, and responsible technology use.

In the modern educational environment, students interact with large volumes of digital information and various AI-powered platforms, often without fully understanding the potential consequences of sharing personal, academic, or confidential data. Inappropriate use of AI tools may lead to privacy violations, unauthorized disclosure of research materials, exposure to phishing attacks, the dissemination of misinformation, and the uncritical acceptance of inaccurate AI-generated responses. Furthermore, students may encounter fabricated academic references, biased information, manipulated digital content, and other forms of misleading output. These circumstances demonstrate

that the effective use of AI technologies requires not only technical knowledge but also the ability to assess risks, verify information, protect digital resources, and act in accordance with ethical and legal requirements.

From a pedagogical perspective, information security competence should be regarded as an integral component of students' overall digital competence and professional development. Its formation involves the purposeful development of knowledge, practical skills, values, attitudes, and responsible behavioral patterns that enable students to interact safely with digital technologies. UNESCO's Guidance for Generative AI in Education and Research emphasizes the importance of human-centred approaches, data privacy, ethical considerations, and appropriate educational implementation of generative AI (Miao & Holmes, 2023). Accordingly, the development of information security competence should be incorporated into the educational process as a continuous pedagogical objective rather than treated as an isolated technical subject. The purpose of this article is to substantiate the pedagogical significance of developing students' information security competence under conditions of widespread AI use and to identify the educational principles and conditions that support its effective formation.

The Pedagogical Essence of Information Security Competence in AI-Assisted Education

Information security competence represents an integrated personal characteristic that enables individuals to understand information security principles, identify potential digital threats, apply appropriate protective measures, evaluate the reliability of digital information, and demonstrate responsible behavior when interacting with information systems. In the context of AI-assisted education, this competence extends beyond traditional cybersecurity knowledge because students must also understand the specific risks associated with generative AI, automated information processing, algorithmic bias, and the disclosure of information through prompts, uploaded documents, and other forms of user interaction.

The pedagogical essence of developing information security competence lies in preparing students to become conscious and responsible participants in the digital educational environment. This process involves the transformation of theoretical knowledge into practical skills, the development of critical and analytical thinking, the formation of ethical attitudes, and the establishment of sustainable habits of secure digital behavior. Students should understand why certain information must remain confidential, how digital threats emerge, what limitations AI-generated content may have, and which actions can reduce the likelihood of security incidents.

The formation of this competence encompasses several interconnected dimensions. The cognitive dimension involves knowledge of cybersecurity principles, data protection, authentication, privacy settings, phishing, social engineering, and AI-related risks. The practical dimension concerns the ability to apply security measures, recognize suspicious digital activities, manage personal information, and respond appropriately to potential incidents. The analytical dimension involves evaluating the accuracy of AI-generated content, comparing information with authoritative sources, identifying misleading claims, and verifying academic references. The ethical dimension includes respect for confidentiality, intellectual property, academic integrity, and the rights of other individuals. The reflective dimension enables students to evaluate their own digital behavior, recognize weaknesses in their security practices, and improve their approaches to using AI tools.

These dimensions demonstrate that information security competence is not formed through the transmission of theoretical knowledge alone. It requires the integration of cognitive, behavioral, practical, and ethical learning outcomes into a coherent pedagogical process. Therefore, teachers should create educational conditions that enable students to apply security principles in realistic situations, critically analyze digital information, and understand the consequences of their decisions.

The Importance of Information Security Competence for Students' Personal and Professional Development

The pedagogical significance of developing information security competence is primarily determined by its contribution to students' personal development and professional readiness. In a digital society, students are expected to use information technologies not only for academic purposes but also in future professional activities that may involve confidential documents, personal data, digital communication, research findings, and organizational information. Insufficient information security awareness can therefore affect both individual users and the institutions in which they study or work.

Developing information security competence helps students understand the relationship between their digital actions and the possible consequences for themselves and others. For example, entering confidential information into an AI system without examining its privacy conditions may expose sensitive material to inappropriate processing or disclosure. Similarly, relying on AI-generated references without verification may undermine the credibility of academic work. Through purposeful instruction, students learn to assess such situations, recognize potential risks, and select safer alternatives.

The formation of information security competence also contributes to professional responsibility. Future teachers, engineers, economists, healthcare professionals, researchers, and other specialists increasingly operate in digital environments where information protection is essential. Their professional effectiveness depends not only on their ability to use digital tools but also on their capacity to safeguard information, respect confidentiality requirements, and apply technology in accordance with relevant ethical and legal standards. Consequently, information security education should be viewed as a cross-disciplinary component of professional training.

Furthermore, information security competence promotes students' independence and self-regulation. Students who understand the principles of secure digital behavior are better prepared to make informed decisions without relying exclusively on external instructions. They can evaluate whether a particular AI tool is appropriate for a given task, identify information that should not be shared, verify the credibility of generated responses, and recognize situations requiring additional guidance. In this respect, information security competence supports lifelong learning by encouraging continuous adaptation to changing digital technologies and emerging threats.

The Role of Critical Thinking and AI Literacy in Developing Information Security Competence

One of the most important pedagogical outcomes of developing information security competence is the enhancement of students' critical thinking. AI systems can generate fluent, persuasive, and well-structured responses that may nevertheless contain factual inaccuracies, unsupported conclusions, fabricated references, or biased interpretations. Students who accept such information without verification may develop misconceptions, produce unreliable academic work, or make inappropriate decisions.

The educational process should therefore encourage students to evaluate AI-generated information systematically. Teachers may ask students to compare AI-generated explanations with scientific publications, official institutional guidance, and other authoritative sources. Students should examine the accuracy of factual claims, the relevance of supporting evidence, the authenticity of cited publications, and the consistency of the generated content with established knowledge. Such activities strengthen analytical reasoning and help students distinguish between plausible language and reliable information.

AI literacy is equally important because students need to understand how AI tools operate at a general level, what limitations they possess, and how their use may affect information security. They should recognize that AI-generated content does not automatically constitute verified knowledge and that different services may apply different data-processing and retention practices. Consequently, students should examine the privacy policies and institutional requirements relevant to the AI tools they use.

From a pedagogical perspective, the integration of AI literacy and information security education creates opportunities for developing informed digital judgment. Students learn to evaluate not only the content generated by AI but also the appropriateness of submitting particular information to a specific platform. This approach strengthens their ability to make independent decisions, question unsupported claims, and maintain responsibility for the accuracy and security of their academic work.

The Role of Teachers and the Educational Environment in Forming Information Security Competence

Teachers play a central role in developing students' information security competence because they organize learning activities, establish expectations for responsible digital behavior, provide feedback, and demonstrate appropriate practices. In the context of AI-assisted education, the teacher's role extends beyond the transmission of subject knowledge to include the development of students' capacity for critical evaluation, ethical reasoning, and secure interaction with digital systems.

An effective pedagogical environment should provide clear explanations of information security principles and opportunities for students to apply them in practice. Teachers can integrate security-related scenarios into lectures, seminars, laboratory sessions, independent assignments, and research activities. For example, students may analyze a hypothetical situation involving the disclosure of confidential research data to an external AI service, identify the associated risks, and propose measures to prevent unauthorized disclosure. They may also evaluate simulated phishing messages, assess the credibility of AI-generated academic references, or develop recommendations for responsible AI use within their academic discipline.

The educational environment should encourage questions, discussion, experimentation within authorized settings, and reflection on mistakes. Students should be able to explore the consequences of unsafe digital behavior without being exposed to unnecessary risks or being required to disclose their own sensitive information. For this reason, instructors should use fictional or anonymized data, approved educational platforms, and clearly defined rules for practical activities.

Teachers also need sufficient digital and pedagogical competence to guide students effectively. They should understand the general characteristics of AI tools, recognize common information security risks, and be able to explain appropriate preventive measures. Continuous professional development is therefore essential for ensuring that educational practices remain relevant to technological changes.

At the institutional level, universities should establish clear policies concerning acceptable AI use, personal data protection, confidentiality, academic integrity, and incident reporting. These policies should be communicated in accessible language and integrated into academic orientation, course materials, and research procedures. A supportive institutional environment helps ensure that the development of information security competence is not limited to individual classroom activities but becomes a shared educational responsibility.

Pedagogical Conditions for the Effective Formation of Information Security Competence

The successful development of students' information security competence depends on several interrelated pedagogical conditions. One of the most important is the systematic integration of information security topics into the curriculum. Rather than being restricted to specialized computer science courses, information security principles should be incorporated into research methodology, academic writing, professional training, and other disciplines where students use AI tools or process digital information. This interdisciplinary approach enables students to understand how information security principles apply across different academic and professional contexts.

Another essential condition is the use of active and practice-oriented teaching methods. Problem-based learning, project-based learning, case-study analysis, simulation-based exercises, collaborative activities, and reflective assessment enable students to connect theoretical knowledge with practical decision-making. Through these methods, students can identify digital threats, evaluate

alternative solutions, and justify their decisions. Practical activities are particularly valuable when they reproduce realistic situations while maintaining a controlled and safe learning environment.

The development of information security competence also requires the individualization of learning. Students differ in their prior digital experience, technical knowledge, and understanding of AI-related risks. Initial diagnostic assessment can help teachers identify these differences and select appropriate learning tasks. Students with limited knowledge may require additional explanations of basic cybersecurity concepts, while more advanced learners may undertake complex analyses of AI-related risks, information governance, and digital ethics.

A further condition is the integration of continuous feedback and transparent assessment criteria. Students should receive information about the strengths and weaknesses of their performance and understand how their knowledge and behavior are evaluated. Assessment should consider not only theoretical understanding but also practical performance, analytical reasoning, ethical decision-making, and the ability to explain security-related choices. This approach supports the gradual development of competence and helps teachers adjust instructional strategies according to students' learning needs.

Finally, information security education should be supported by a culture of digital responsibility. Students need to understand that secure AI use involves shared responsibilities among individuals, educational institutions, and technology providers. The educational process should therefore promote respect for privacy, careful information sharing, source verification, responsible reporting of security incidents, and continuous improvement of digital practices.

The Relationship Between Information Security Competence, Academic Integrity, and Ethical AI Use

Developing information security competence has a close relationship with academic integrity and the ethical use of artificial intelligence. The availability of AI tools creates opportunities for academic support but also introduces questions concerning authorship, attribution, the reliability of generated information, and the responsible handling of research materials. Students need to understand that the use of AI should be consistent with institutional requirements and the academic expectations applicable to their assignments and research activities.

Academic integrity requires students to take responsibility for the originality, accuracy, and credibility of their work. When AI tools are used to generate explanations, summarize literature, or suggest references, students should verify the information and ensure that the final work meets the relevant academic standards. Fabricated citations, unverified claims, and the inappropriate use of confidential material may compromise the quality and integrity of research.

Ethical AI use also involves respect for privacy and intellectual property. Students should not upload sensitive personal data, confidential institutional documents, unpublished research materials, or information belonging to others unless such use is explicitly authorized and complies with applicable policies and data protection requirements. They should also understand the importance of disclosing AI assistance when required by the relevant institution, publisher, or assignment guidelines.

From a pedagogical perspective, integrating academic integrity with information security education helps students recognize that responsible technology use is not limited to technical protection. It also involves honesty, accountability, respect for others' rights, and an awareness of the consequences of digital actions. These values are essential for preparing professionals who can use AI tools effectively without compromising ethical and academic standards.

Assessment of the Development of Students' Information Security Competence

The pedagogical effectiveness of developing information security competence should be evaluated through a combination of diagnostic, formative, and summative assessment. Diagnostic assessment helps identify students' initial knowledge, digital habits, and ability to recognize common

information security threats. It may involve scenario-based questions, short practical exercises, and assessments of students' understanding of data protection and AI-related risks.

Formative assessment provides continuous feedback during the learning process. Teachers may evaluate students' responses to simulated incidents, their ability to identify suspicious messages, the quality of their source verification, and their reasoning when determining whether particular information can be shared with an AI system. Reflective journals, peer assessment, group discussions, and short analytical reports can provide additional evidence of students' progress.

Summative assessment may include practical tasks, case-study analyses, project presentations, and structured examinations. Students should be required to demonstrate not only knowledge of information security principles but also the ability to apply them in realistic educational situations. For instance, they may be asked to analyze an AI-use scenario, identify possible privacy risks, verify generated information, and recommend appropriate protective measures.

The assessment process can be organized around cognitive, practical, analytical, and ethical-reflective criteria. The cognitive criterion concerns understanding of information security principles and AI-related risks. The practical criterion assesses the ability to apply protective measures and respond to simulated incidents. The analytical criterion examines the capacity to verify information, recognize misleading content, and justify decisions using credible evidence. The ethical-reflective criterion evaluates respect for confidentiality, academic integrity, responsible AI use, and the ability to recognize weaknesses in personal digital practices.

For practical implementation, these criteria may be measured using initial, developing, proficient, and advanced performance levels. Clear indicators should be established for each level so that assessment remains transparent and consistent. Importantly, students' self-reported confidence should be supplemented by observable performance because awareness of information security principles does not necessarily demonstrate the ability to apply them correctly.

Discussion

The pedagogical significance of developing students' information security competence is determined by the interaction of educational, technological, ethical, and professional factors. The increasing availability of AI tools makes it necessary to reconsider the content of digital education and to expand the traditional understanding of digital literacy. Students must not only know how to operate digital applications but also understand the implications of their use, evaluate the reliability of generated information, and protect the information they process.

The integration of information security competence into higher education can support the development of independent learning, critical thinking, professional responsibility, and ethical decision-making. Practice-oriented educational activities help students transform abstract knowledge into practical skills, while reflective learning encourages them to evaluate their own digital behavior and identify areas for improvement. Institutional policies and teacher guidance provide the conditions necessary for applying these skills consistently across academic contexts.

These considerations are consistent with UNESCO's emphasis on human-centred and ethically informed approaches to generative AI in education (Miao & Holmes, 2023), as well as the risk-management principles outlined in the NIST AI Risk Management Framework (Tabassi, 2023). The NIST Cybersecurity Framework 2.0 also provides a structured approach to understanding, prioritizing, and communicating cybersecurity risks (Pascoe et al., 2024). Although these frameworks were not designed exclusively for pedagogical purposes, their principles can inform the development of educational content and institutional practices related to secure AI use.

Nevertheless, the proposed pedagogical considerations should be understood as a theoretically grounded analysis rather than evidence of experimentally verified effectiveness. Further empirical research is needed to determine which combinations of teaching methods produce the most substantial improvements in students' information security competence. Such research may involve pre- and post-assessment, observation of practical performance, analysis of student projects, and comparisons

across different educational contexts. Particular attention should be given to measuring students' ability to protect sensitive information, recognize AI-assisted phishing attempts, verify AI-generated content, and make ethically justified decisions.

Conclusion

The development of students' information security competence in the context of using artificial intelligence tools represents an important pedagogical priority in contemporary higher education. The widespread use of AI technologies creates opportunities for improving learning and research, but it also introduces risks associated with personal data protection, information reliability, cybersecurity, academic integrity, and responsible digital behavior. These challenges require an educational approach that combines theoretical knowledge, practical skills, critical thinking, ethical awareness, and self-regulation.

The pedagogical significance of information security competence lies in its contribution to students' personal development, academic responsibility, professional readiness, and ability to participate safely in digital environments. Its effective formation depends on the integration of information security principles into the curriculum, the use of active and practice-oriented teaching methods, the development of teachers' digital competence, the establishment of clear institutional policies, and the application of transparent assessment procedures.

Particular importance should be assigned to AI literacy, the verification of generated information, the protection of confidential materials, and the development of responsible information-sharing practices. Students should be encouraged to use AI as a supportive educational resource while retaining responsibility for their decisions, academic work, and the security of information.

In conclusion, developing information security competence should be regarded as a continuous, interdisciplinary, practice-oriented, and ethically informed pedagogical process. Its systematic implementation can contribute to preparing digitally competent professionals who are capable of using artificial intelligence tools critically, safely, and responsibly. Further empirical research is necessary to evaluate the effectiveness of specific pedagogical approaches and to refine educational models that respond to the changing demands of AI-supported higher education.

References

1. 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>
2. 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>
3. 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>
4. UNESCO. Recommendation on the Ethics of Artificial Intelligence. United Nations Educational, Scientific and Cultural Organization. 2021. <https://unesdoc.unesco.org/ark:/48223/pf0000381137>