Modern American Journal of Linguistics, Education, and Pedagogy
ISSN (E): 3067-7874
Volume 01, Issue 09, December, 2025
Website: usajournals.org

A METHODOLOGICAL MODEL FOR DEVELOPING INFORMATION SECURITY SKILLS IN FUTURE TEACHERS BASED ON ARTIFICIAL INTELLIGENCE TECHNOLOGIES

Mastura Muminova
PhD Student, Fergana State University
E-mail: mastura.muminova.1992@mail.ru
ORCID ID: 0009-0009-1404-8586
Phone: +998 91 110 16 44

Juraev Vokhid
Doctor of Pedagogical Sciences (DSc), Professor of the Department of Applied Mathematics and Informatics of Fergana State University
E-mail: vjurayev1986@gmail.com
ORCID ID: 0000-0003-3732-6242
Phone: +998 90 582 27 07

Mamirjon Turdimatov
Associate Professor of the Department of Software Engineering and Cybersecurity, Fergana State Technical University
E-mail: Turdimatovmamir1958@gmail.com
ORCID ID: 0000-0003-1419-9092
Phone: +998 91 676-22-11

Abstract
In recent years, digital technologies have become an integral component of the educational process. Along with this transformation, issues of information security have gained particular urgency, making it essential for teacher-training programs to equip future educators with the ability to guide students toward safe, responsible, and conscious use of the internet. In the online environment, learners are exposed to various risks such as misinformation, breaches of personal data,

Modern American Journal of Linguistics, Education, and Pedagogy
ISSN (E): 3067-7874
Volume 01, Issue 09, December, 2025
Website: usajournals.org

digital violence, and cybercrime. Therefore, future teachers must possess solid methodological preparation in order to effectively teach students the fundamentals of information security.

Artificial intelligence (AI) technologies open up new opportunities in this regard by enabling the analysis of learning materials, the modelling of educational scenarios, and the development of secure digital behavior among students. However, practical experience demonstrates that many prospective teachers in the region are not yet fully capable of independently utilizing these technologies. Consequently, there is a need to gradually familiarize them with AI tools and to develop a pedagogical methodology for teaching information security.

The purpose of this research is to develop a methodological model for enhancing the information security competencies of future teachers through the integration of artificial intelligence into the teacher-training process, as well as to examine the preliminary effectiveness of this model through experimental testing.

Research Objectives:

1. Study the theoretical foundations of using AI technologies in information security education
2. Determine the initial methodological preparation level of future teachers
3. Develop an AI-based methodological model and identify its components
4. Experimentally test the effectiveness of the model
5. Develop scientific-methodological recommendations for pedagogical practice

The rapid advancement of information technologies has made the integration of digital literacy, information security, and artificial intelligence into educational systems a critical priority. Today's teacher is not only a transmitter of knowledge but also a guide who cultivates students' awareness of digital risks and their ability to handle information responsibly. In this context, preparing future teachers in the field of information security and ensuring their effective use of AI tools represent key priorities of contemporary education.

Modern research demonstrates that teachers' digital competence, analytical thinking, and ethical awareness play decisive roles in shaping students' information security culture. Accordingly, the introduction of AI technologies

Modern American Journal of Linguistics, Education, and Pedagogy
ISSN (E): 3067-7874
Volume 01, Issue 09, December, 2025
Website: usajournals.org

into the educational system is considered a significant factor in structuring teachers' professional readiness in line with contemporary demands.

UNESCO's 2023 report, Artificial Intelligence in Education: Global Guidelines and Teacher Readiness, states that "integrating AI into teacher development is a core direction of future education." Similarly, the OECD's 2023 analytical review AI and the Future of Education Systems identifies the implementation of AI as a major driver of digital competence development among teachers.

The Digital Competence of Educators Framework (DigCompEdu) developed by Redecker (2017) evaluates teacher digital competencies across six domains, one of which is "preparing learners for the digital age," encompassing the formation of information security culture. The NIST (2020) NICE Cybersecurity Workforce Framework is an international standard for identifying cybersecurity competencies. Drawing on these sources, we developed an adapted competence model specifically for teachers. While local research (Muminova, 2023; Zulunov, 2024; Sabirjanov, 2025) highlights the importance of AI in education, the integration of AI technologies into information security pedagogy within teacher-training programs remains insufficiently explored.

These sources collectively emphasize the growing role of artificial intelligence in teacher education. In Uzbekistan, however, this area is still in its formative stage: many higher education institutions have limited experience with AI-based tools, and curricula pay inadequate attention to the methodology of teaching information security. Therefore, the significance of this study lies in developing a methodology to enhance information security competencies among future teachers and empirically validating the role of AI technologies in this process. The scientific novelty of the research is reflected in the development of an interactive and analytically oriented model for teaching information security using AI tools.

The theoretical foundation of this work is grounded in modern pedagogy, information technologies, and international frameworks on AI integration in education. Its practical value lies in creating an innovative methodology for teaching information security through AI tools within teacher-training programs, thereby promoting the development of digital culture among students.

Modern American Journal of Linguistics, Education, and Pedagogy
ISSN (E): 3067-7874
Volume 01, Issue 09, December, 2025
Website: usajournals.org

METHODOLOGY

The methodological foundation of this study is based on contemporary pedagogical principles and the integration of digital education with artificial intelligence (AI) technologies. A mixed-method approach was employed, combining quantitative and qualitative analyses to ensure a comprehensive evaluation of the research objectives. Initially, the knowledge level and methodological preparedness of future teachers in the field of information security were assessed through a questionnaire survey. This was followed by an experimental intervention, the results of which were examined using qualitative methods.

Research Design

A controlled experimental design was applied. A total of 68 undergraduate students majoring in pedagogy (3rd and 4th year) were randomly assigned to two groups: an experimental group (n = 34) and a control group (n = 34). The experimental group participated in an eight-week instructional program based on the AI-integrated methodological model, while the control group received traditional instruction.

Throughout the study, participants were introduced to various AI platforms (ChatGPT, Gemini, Copilot, and Firefly) and explored their potential as pedagogical support tools. They analyzed information-security-related instructional content and developed recommendations aimed at enhancing students' information security competencies.

Stages of the Research Process (Aligned with the AI-Integrated Methodological Model). The experimental work was carried out in four stages:

1. **Diagnostic Stage (1 week)** — Determining the initial knowledge level and professional interest of future teachers through questionnaires and interviews.
2. **Experimental Stage (4 weeks)** — Introducing AI tools, demonstrating their pedagogical potential, and conducting hands-on training sessions.
3. **Analytical Stage (1 week)** — Analyzing participants' performance outcomes and identifying effective strategies for developing students' information security skills.

Modern American Journal of Linguistics, Education, and Pedagogy
ISSN (E): 3067-7874
Volume 01, Issue 09, December, 2025
Website: usajournals.org

4. **Synthesis Stage (2 weeks)** — Formulating and presenting the final version of the methodological model based on experimental findings.

Quantitative data were analyzed using statistical methods. Pre- and post-intervention results were compared to determine the magnitude and significance of changes in knowledge and skill development. Qualitative data were derived from student reflections, group discussions, and written analytical responses, enabling the extraction of broader pedagogical insights. All ethical standards were strictly observed during the research. Participants were informed about the purpose of the study, provided written consent, and ensured anonymity. Collected data were used exclusively for academic analysis.

This methodological framework contributes to shaping future teachers' digital awareness, enhancing their readiness to develop students' information security skills, and fostering the conscious application of AI technologies in professional pedagogical practice.

RESULTS AND DISCUSSION

The findings of the study reveal the development of future teachers' preparedness for cultivating students' information security skills, the impact of AI-assisted instruction on their methodological competence, and the shifts observed in their analytical and pedagogical thinking. Initial survey results indicated that students majoring in pedagogy possessed only general and theoretical understanding of information security, while lacking the practical skills and methodological strategies necessary to teach this content effectively. Throughout the experimental intervention, model lessons, scenario-based activities, and analytical tasks involving AI tools significantly enhanced their methodological reasoning and instructional design abilities.

Table 1. Initial Knowledge Level of Future Teachers in Information Security (0–10 Scale)

Group	Initial Mean (M±SD)	Final Mean (M±SD)	Growth (%)	t-test (p)
Experimental	5.1 ± 1.2	7.3 ± 1.1	43.1%	$t = 8.42$ $p < 0.001$
Control	5.2 ± 1.3	5.8 ± 1.2	11.5%	$t = 1.87$ $p = 0.07$

Modern American Journal of Linguistics, Education, and Pedagogy
ISSN (E): 3067-7874
Volume 01, Issue 09, December, 2025
Website: usajournals.org

Note: The results demonstrate statistically significant improvement in the experimental group ($p < 0.001$), while the control group did not show meaningful change ($p = 0.07$). This confirms the higher effectiveness of the AI-based methodological model compared to traditional teaching methods.

Table 2. Change in Confidence Levels Regarding the Use of AI Tools (Likert 5 Scale)

Indicator	Initial (M±SD)	Final (M±SD)	Change (%)
Interest in using AI in education	3.1 ± 0.9	4.3 ± 0.6	+38.7%
Readiness to use AI in designing information security materials	2.8 ± 1.0	4.1 ± 0.8	+46.4%
Confidence in AI technologies	2.9 ± 0.8	4.0 ± 0.7	+37.9%

Note: Participants regarded AI as a valuable assistive tool in the teaching–learning process and expressed increased willingness to integrate it into instructional design, although further theoretical and methodological training remains necessary.

Table 3. Effectiveness of Proposed Methods for Developing Students' Information Security Skills (Expert Evaluation)

Methodological Approach	Number of Evaluators	Mean Score (0–10)	Effectiveness (%)
Visual scenarios and situational analysis	6	8.9	93%
Problem-based learning	6	8.5	89%
Textbook analysis with AI assistance	6	8.2	86%
Traditional lecture and test method	6	6.1	61%

Note: Experts concluded that AI-supported methods significantly enhanced visual reasoning and problem-based approaches, contributing to more effective formation of safe online behavior among students.

The results indicate substantial improvement in the methodological preparedness of future teachers regarding information security instruction. Although AI

Modern American Journal of Linguistics, Education, and Pedagogy
ISSN (E): 3067-7874
Volume 01, Issue 09, December, 2025
Website: usajournals.org

technologies were not fully integrated as independent teaching agents, their analytical and visualization capabilities fostered more innovative instructional strategies among participants. Students demonstrated enhanced methodological thinking, increased engagement with interactive teaching formats, and improved ability to explain information security concepts using real-life scenarios.

Focus-group discussions revealed that approximately 74% of participants believed AI tools could ease teachers' workload, although human oversight and responsibility remain essential, particularly in assessment and decision-making processes. According to expert evaluations (n = 6), the primary advantage of the AI-based methodological model lies in its ability to enhance instructional quality and efficiency without replacing the teacher.

To strengthen the formation of information security competencies during pedagogical practice, the study recommends integrating an AI-supported "Methodology of Information Security Education" course into teacher-training curricula, delivering 36–72 hours of practical training each semester, and implementing a mandatory portfolio-based assessment system. Further, the development of AI guides in the Uzbek language, a scenario-based lesson library with over 200 resources, and a long-term online collaborative platform is advisable. The evaluation system should incorporate self-assessment, peer assessment, expert assessment, and practice-based assessment, all supported by detailed rubrics to ensure scientific-methodological rigor. Ensuring technical feasibility—including free access to AI tools, high-quality translation support, and a dedicated technical help center—is crucial for the continuous implementation of the proposed model.

Overall, the experiment demonstrates that the integration of artificial intelligence into teacher training can effectively enhance professional readiness, promote students' information security competencies, and support the formation of digital citizenship and culture.

CONCLUSION

The findings of the study demonstrate that the use of artificial intelligence (AI) technologies is an effective approach for developing future teachers' knowledge, skills, and methodological preparedness in the field of student information

Modern American Journal of Linguistics, Education, and Pedagogy
ISSN (E): 3067-7874
Volume 01, Issue 09, December, 2025
Website: usajournals.org

security. According to the experimental results, AI-enhanced instructional activities significantly improved participants' not only cognitive understanding but also their analytical thinking, reflective engagement, and professional motivation.

Through the integration of AI tools, students developed abilities in independent analysis, modelling problem-based scenarios, and evaluating learners' digital safety behaviors. The study revealed a positive correlation between participants' confidence in using AI and their professional interest in information security ($r = 0.68$, $p < 0.01$). This confirms that AI serves as an important mechanism for fostering innovative competencies within the teaching profession. Expert evaluations identified "situational analysis" and "AI-supported analytical tasks" as the most effective methods, as they enhance students' capacity to reason through real-life digital safety issues. These outcomes align with international studies—particularly UNESCO (2023) and OECD (2023)—which emphasize that the development of teachers' digital and ethical competencies is closely connected to the integration of AI technologies.

However, several limitations of the study must also be noted: restricted access to AI platforms, linguistic barriers, and varying levels of digital literacy among participants. These factors complicate the full-scale implementation of the proposed model. Therefore, future research should focus on further improving AI-integrated methodological models, developing locally contextualized instructional materials, and creating structured professional development programs for teachers.

Overall, the study underscores that integrating AI technologies into teacher-training programs offers a powerful opportunity to cultivate a new generation of educators equipped with innovative, ethical, and information-secure professional competencies.

REFERENCES

1. CYBER.ORG. (2021). K-12 cybersecurity learning standards (Version 1.0). Cyber Innovation Center. Retrieved from https://cyber.org/standards
2. ENISA (European Union Agency for Cybersecurity). (2018). Cybersecurity culture guidelines: Behavioural aspects of cybersecurity. Athens: ENISA.

Modern American Journal of Linguistics, Education, and Pedagogy
ISSN (E): 3067-7874
Volume 01, Issue 09, December, 2025
Website: usajournals.org

Retrieved from https://www.enisa.europa.eu/publications/cybersecurity-culture-guidelines

3. ENISA (European Union Agency for Cybersecurity). (2022). Cybersecurity education initiatives in the EU Member States. Athens: ENISA. Retrieved from https://www.enisa.europa.eu/publications
4. Luckin, R., Holmes, W., Griffiths, M., & Forcier, L. B. (2020). Intelligence unleashed: An argument for AI in education. Pearson Education. Retrieved from https://www.pearson.com/uk/educators/insight/intelligence-unleashed.html
5. Muminova, M. M. (2023). Analysis of current issues and solutions in cybersecurity. In International Scientific and Technical Conference "Application of technical and digital technologies in practice and their innovative solutions" (Part II, Sections III–VI, pp. 635–640). Fergana: TATUFF. Retrieved from https://tatuff.uz/wp-content/uploads/2023/05/2_tom_2.pdf
6. NIST (National Institute of Standards and Technology). (2020). Workforce framework for cybersecurity (NICE framework), NIST Special Publication 800-181 Rev. 1. Gaithersburg, MD: NIST. https://doi.org/10.6028/NIST.SP.800-181r1
7. OECD (Organisation for Economic Co-operation and Development). (2021). OECD digital education outlook 2021: Pushing the frontiers with AI, blockchain and robots. Paris: OECD Publishing. https://doi.org/10.1787/589b283f-en
8. Redecker, C. (2017). European framework for the digital competence of educators (DigCompEdu). Luxembourg: Publications Office of the European Union. https://doi.org/10.2760/159770
9. Sabirjanov, R. A. (2025). Opportunities of using artificial intelligence in the educational process: The case of higher education. Eurasian Journal of Technology and Innovation, 3(2), 38–41. https://doi.org/10.5281/zenodo.14980535
10. UNESCO (United Nations Educational, Scientific and Cultural Organization). (2021). AI and education: Guidance for policy-makers. Paris:

Modern American Journal of Linguistics, Education, and Pedagogy
ISSN (E): 3067-7874
Volume 01, Issue 09, December, 2025
Website: usajournals.org

UNESCO Publishing. Retrieved from https://unesdoc.unesco.org/ark:/48223/pf0000376709

11. UNESCO (United Nations Educational, Scientific and Cultural Organization). (2023). Guidance for generative AI in education and research. Paris: UNESCO Publishing. Retrieved from https://unesdoc.unesco.org/ark:/48223/pf0000386695
12. Zulunov, R. M., & Samatova, Z. N. (2024). Cybersecurity issues and methods for ensuring it. Al-Farghoniy Avlodlari, (2), 322–326. https://doi.org/10.5281/zenodo.11480179
13. Zawacki-Richter, O., Marín, V. I., Bond, M., & Gouverneur, F. (2019). Systematic review of research on artificial intelligence applications in higher education – Where are the educators? International Journal of Educational Technology in Higher Education, 16(1), 39. https://doi.org/10.1186/s41239-019-0171-0