pISSN:2349-5707 Volume:13,Issue 2, February -2026 eISSN:2349-5715

CONSIDERATION OF THE SPECIFICS OF TRAINING FUTURE TEACHERS IN INFORMATION SECURITY TRAINING

Imomaliyev Abduhamiyd

2nd year master of Kokand State University

Abstract: The article examines information security as an important pedagogical problem of modern education. The necessity of forming students' culture of safe behavior in the information environment and preparing future educators for teaching the basics of information security is substantiated. The importance of integrating this issue into the educational programs of pedagogical universities is emphasized.

Keywords: information security, information culture, pedagogical problem, digital environment, safe behavior online, training future educators, educational process, information society.

When developing the educational and methodological support for the "Information Security" course, it is necessary to consider the specifics of the target audience - the students of the pedagogical university. Unlike the training of narrow-profile IT specialists in information security, where emphasis is placed on deep technical mastery of the subject, the IT course in a pedagogical university performs a somewhat different function. Future computer science teachers (and, possibly, teachers of other disciplines using ICT) should acquire basic concepts and information protection skills sufficient for: a) ensuring their own digital literacy and security; b) integrating information security issues into their professional activities, primarily in teaching schoolchildren.

The first aspect - ensuring one's own level of IT competence - assumes that the graduate of the pedagogical university knows the main threats to the information environment (viruses, account hacks, phishing, undesirable content, etc.) and can use basic protection tools (antiviral software, confidentiality settings on social networks, strong passwords, data backup, etc.). These skills are necessary for him in his daily work (for example, keeping an electronic journal without letting students' data leak; using internet resources without being in danger). Now there are cases where teachers' lack of knowledge leads to incidents - for example, a school computer was infected with a virus because a teacher opened a non-secure letter; or a teacher accidentally disclosed children's personal data by incorrectly configuring document accessibility. Such situations demonstrate the relevance of training IT teachers at an elementary level.

The second aspect - the teacher's readiness to teach others - is even more specific. A future teacher, especially a computer science teacher, must be able to convey to students the basics of safe behavior in the information environment. In fact, he acts as a conductor of information culture. Children and adolescents, as noted, are highly vulnerable to information threats. A teacher who is in constant interaction with them is able to explain safety rules to them in a timely manner, identify signs of discomfort (for example, if a student is subjected to cyberbullying), and take measures. Therefore, the training program should provide for students to master not only "what to teach" (the content of information technology), but also "how to teach" these issues to schoolchildren. This necessitates the inclusion of methodological elements: familiarizing students with the age-related characteristics of perceiving the topic of safety, the methods of educational work on this topic, and the possibilities of extracurricular activities (cyber-hygiene clubs, thematic class hours).

In addition, the pedagogical university trains specialists who often do not have deep preliminary experience in cybersecurity. Students' initial knowledge of IT is usually limited to

pISSN:2349-5707 Volume:13,Issue 2, February -2026 eISSN:2349-5715

everyday literacy: they know that antivirus is necessary, have heard about computer viruses, and imagine that one should not share an e-mail password with strangers. They may not have targeted IT education at school, except for individual computer science lessons. Therefore, the course at the university is built practically "from scratch" - from the very beginning. On the other hand, educators are humanistically and socially oriented specialists; they may be more interested in the human, applied aspect of the problem than purely technical details. It's important for them to see the meaning: how it will be useful in working with children, what benefit it will bring to school. Therefore, when developing an UMC, it is necessary to emphasize the practical and social significance of the material, avoiding overloading it with theory for the sake of theory.

The specifics of pedagogical training are also manifested in the limited time allocated for technical disciplines. As a rule, future computer science teachers study many pedagogical and methodological subjects, and they have fewer purely technical courses than IT students. The "Information Security" course can only be allocated for one semester, often in the senior year, when the academic load is high. For example, in the curriculum of the Yelabuga Institute of KFU, the IB course takes 11 semesters and, judging by the document, in the correspondence department - only 2 credits, which is equivalent to about 72 class hours. This is not so much, so the content needs to be compressed, the most necessary, and the methodology - the most effective in a short time.

Another feature is the motivation of students. Information security topics may seem secondary to someone (especially if a student, for example, is more of a mathematician than a computer scientist in their field, or if they are far from technology). The teacher's task is to interest them by showing their importance for future work and personal life. A good motivating factor is the demonstration of specific problems that teachers are already facing: the infection of school classroom computers with viruses through flash drives, the spread of dangerous online challenges among students, the leakage of exam test answers into the network, etc. When students see real cases, they realize that having knowledge of information technology distinguishes a teacher as a modern, competent professional, and conversely, ignorance puts their reputation and children's safety at risk.

Taking all this into account, in our educational and methodological support for the "Information Security" course, special attention is paid to:

Selection of content relevant to pedagogical activity. In addition to the general foundations of information security, sections on information protection specifically in the educational context are included: protection of students' personal data, rules for using devices in school, ethical aspects (for example, the inadmissibility of copying others' work - a connection with academic honesty), and ways to teach schoolchildren safe internet.

Methodological insertions into technical topics. For example, after studying the topic "Social Engineering," students are asked to discuss how to teach teenagers to recognize fraudulent methods. Or while studying "Content Filtering," we consider how to set up filters in a school library and how to explain to children the reasons for blocking harmful websites.

Simplicity and clarity of the material. Educational materials contain minimal complex formulas, but there are many schemes, tables, analogies (for example, comparing encryption with locks and keys - for the humanities to be more understandable). Special terms are introduced gradually and reinforced through a glossary. If English terminology is used (which is abundant in IT: firewall, phishing, backup), explanation in Russian and examples are provided.

Practical orientation and interactivity of lessons. Considering the small number of hours, the theory is maximally integrated with practice. Each lecture contains a demonstration or a small

pISSN:2349-5707 Volume:13,Issue 2, February -2026 eISSN:2349-5715

practical exercise. In seminars, students perform roles and situations close to school practice - for example, one portrays a "hacker," the other a school system administrator, and they analyze an educational incident.

Using pedagogical concepts familiar to students. For example, you can rely on their knowledge of age-related psychology: when discussing threats to children, we rely on how different ages perceive information. Or to attract knowledge on the methodology of educational work: when planning an AC activity at school, students apply the general principles of planning educational activities that they are familiar with.

Accounting for various training profiles. If the course is attended not only by future computer science teachers, but also, let's say, by methodologists in vocational education or other specialties, then the tasks vary. But usually, of course, the target group is students related to ICT, particularly computer science.

It is also worth noting the specifics of the material and technical base of pedagogical universities. They are not always equipped with advanced cybersecurity laboratories (unlike technical universities). There may be no specialized software (sniffers, virtual virus debugging machines, etc.). Therefore, we are creating such practical tasks in the UMO that can be performed on standard computers and with free software. For example, using free antivirus software, online password verification services, Windows folders encryption utilities, and trial versions of products. That is, we do not require expensive funds, which is important for the implementation of the course in a typical pedagogical university with limited funding in the IT direction.

Finally, an important specific point: the formation of general pedagogical culture and responsibility. Future teachers should be aware that information security issues are part of their professional responsibility for the life and health of students (in modern conditions, digital "health" is also significant). Therefore, the content constantly emphasizes the value component: the confidentiality of students' information is the ethical norm of the teacher; protecting children from harmful content is the moral obligation of the school and the teacher; instilling a culture of working with information is a component of the educational process. Such axiological filling advantageously distinguishes our course from purely technical ones - and makes it closer to teachers.

Thus, considering the pedagogical specifics of designing the "Information Security" course manifests itself in selecting relevant, applied content, adapting methodological techniques to the initial level and the needs of future teachers, and integrating professionally oriented tasks and value aspects into the educational process. All this will make the training more effective and meaningful for students, and ultimately - prepare graduates who are truly ready to ensure information security in their future educational institution.

References

1. Law of the Republic of Uzbekistan "On Informatization." - Tashkent.
2. Law of the Republic of Uzbekistan "On the Principles and Guarantees of Freedom of Information." - Tashkent.
3. Law of the Republic of Uzbekistan "On Cybersecurity." - Tashkent.
4. Bogatyrova Yu.I. Information security of the individual in the educational environment. - Moscow: Prosveshchenie, 2020.
5. Kozlova O.A. Formation of Information Security Culture in Schoolchildren. - St. Petersburg: Piter, 2019.

pISSN:2349-5707 Volume:13,Issue 2, February -2026 eISSN:2349-5715

6. Pulat E.S. Modern Pedagogical and Information Technologies in the Education System. - Moscow: Academy, 2021.
7. Smirnov A.V. Information Security: A Textbook for Universities. - Moscow: Yurait, 2022.