



THE RELEVANCE OF FORMING INFORMATION SECURITY COMPETENCE IN THE DIGITAL EDUCATION PROCESS

Mamadaliyeva Sug'diyona Ilxomjon qizi

*Farg'ona ilg'or kasbiy mahorat texnikumi Informatika va axborot texnologiyalari
fani katta o'qituvchisi*

e-mail: ibrohimovasugdiyona98@gmail.com

Muxtarov Farrux Muhammadovich

pedagogika fanlari doktori DSc, Markaziy Osiyo tibbiyot universiteti

Biofizika va axborot texnologiyalar kafedrasi mudiri

e-mail: farruhmukhtarov@gmail.com

Annotatsiya. Mazkur maqolada ta'lim jarayonining raqamlashtirilishi sharoitida ta'lim oluvchilarda axborot xavfsizligi kompetensiyasini shakllantirishning dolzarbligi ko'rib chiqilgan. Raqamli texnologiyalarning keng joriy etilishi ta'lim imkoniyatlarini kengaytirish bilan birga, shaxsiy ma'lumotlar, raqamli identifikatsiya va onlayn xulq-atvor bilan bog'liq yangi xavflarni ham yuzaga keltirmoqda. Shu bois ta'lim oluvchilarda axborotni xavfsiz izlash, baholash, saqlash va mas'uliyatli foydalanish kompetensiyalarini rivojlantirish muhim pedagogik vazifaga aylanmoqda. Maqolada mazkur kompetensiyaning mazmuni, ta'limdagi o'rni va uni shakllantirish zarurati tahlil qilinib, raqamli muhitda xavfsiz xulq-atvor ta'lim sifatining ajralmas qismi ekanligi asoslanadi.

Kalit so'zlar: Raqamli ta'lim, raqamli ta'lim muhiti, axborot xavfsizligi, axborot xavfsizligi kompetensiyasi, raqamli kompetensiya, raqamli savodxonlik, kiberxavfsizlik, axborot madaniyati.

Аннотация. В данной статье рассматривается актуальность формирования компетентности в области информационной безопасности у обучающихся в условиях цифровизации образовательного процесса. Широкое внедрение цифровых технологий, наряду с расширением образовательных



возможностей, порождает новые риски, связанные с персональными данными, цифровой идентификацией и онлайн-поведением. В связи с этим развитие у обучающихся компетенций безопасного поиска, оценки, хранения информации и ответственного её использования становится важной педагогической задачей. В статье анализируются содержание данной компетентности, её роль в образовательном процессе и необходимость её формирования, а также обосновывается, что безопасное поведение в цифровой среде является неотъемлемой составляющей качества образования.

Ключевые слова: цифровое образование, цифровая образовательная среда, информационная безопасность, компетентность в области информационной безопасности, цифровая компетентность, цифровая грамотность, кибербезопасность, информационная культура.

Abstract. This article examines the relevance of forming information security competencies in learners in the context of the digitalization of the educational process. The widespread introduction of digital technologies, along with expanding educational opportunities, also creates new risks associated with personal data, digital identification and online behavior. Therefore, developing competencies in the safe search, evaluation, storage and responsible use of information in learners is becoming an important pedagogical task. The article analyzes the content of this competency, its role in education and the need for its formation, and argues that safe behavior in the digital environment is an integral part of the quality of education.

Keywords: Digital education, digital learning environment, information security, information security competence, digital competence, digital literacy, cybersecurity, information culture.

Introduction: Today, the rapid development of digital technologies has a significant impact on all spheres of social life, in particular, the content, form and organization of the education system. The use of e-learning platforms, digital educational resources, distance learning tools, cloud technologies and various online



services in the educational process creates new opportunities for learning. UNESCO, indicating digital technologies as one of the important factors of modern education, emphasizes that digital transformation is changing existing forms of education. The digitalization of the education system in the Republic of Uzbekistan has been identified as a priority area of state policy within the framework of the "Digital Uzbekistan - 2030" strategy, and systematic reforms aimed at developing e-learning resources, digital infrastructure, and teacher competence are being consistently implemented.

As a result of the transition of the educational process to a digital environment, the learner is becoming not just a simple consumer of information, but an active subject who searches for, analyzes, creates and distributes it. In such conditions, in addition to the technical skills of using digital tools, the learner is also required to understand the requirements of information security, protect personal data, distinguish between reliable and unreliable information sources, prevent various digital threats, and demonstrate responsible behavior in the Internet space. In this regard, the expansion of the digital educational environment requires that the issue of forming information security competencies of learners be viewed not only as a technical, but also as an important pedagogical problem.

Main part : The digital learning environment is a set of interconnected digital technologies, electronic resources, information systems and communication tools in the educational process. Such an environment allows the learner to quickly search for the necessary information, use various educational resources, communicate remotely with the teacher and peers, complete assignments electronically, and monitor learning outcomes using digital tools. However, with the expansion of the capabilities of the digital environment, information security issues are also becoming more complex. When using the Internet, learners may encounter personal information disclosure, malware, phishing, fake news, cyberbullying, social engineering, inappropriate content, and various digital manipulations. According to UNICEF, digital education, while creating great opportunities, also poses new risks



for children and young people. Therefore, it is necessary to pay special attention to online safety and data protection issues in the digital education process. In particular, as a result of the use of various digital platforms in the educational process, the processing of personal and other sensitive data about learners is increasing. The use of digital technologies in education requires strengthening data protection and cybersecurity measures. Therefore, the development of a digital learning environment should not be limited to improving technological infrastructure. The formation of learners who are ready to use the digital environment safely and responsibly is also an important component of this process.

Pedagogical content of information security competence

It is inappropriate to understand information security competence as a set of technical knowledge alone. This competence can be viewed as a complex quality that reflects the learner's readiness to understand security requirements, identify risks, make appropriate decisions, and implement safe behavior when working with information. From this point of view, information security competence can be described by the following interrelated components:

1. Cognitive component – knowledge of the basic concepts of information security, digital threats, personal data protection, password security, and rules for safe Internet use.
2. Practical component – skills in applying the acquired knowledge in practical situations, identifying dangerous links, creating secure passwords, protecting confidential information, and using digital resources safely.
3. Value-motivational component – a responsible attitude to information security, respect for personal and other people's data, an internal need to comply with security rules in the digital environment.
4. Reflexive component – the ability to analyze one's digital behavior, realize mistakes made, and make safer decisions in the future. This approach takes information security competency beyond the level of simply “knowing the rules.”



The pedagogical need to form information security competencies in learners

In a context where students' activities in the digital environment are increasingly expanding, the formation of information security competencies is not an additional area of education, but rather one of the important pedagogical tasks that ensures the quality of digital education.

First, a learner's safety in the digital environment is directly related to the protection of their personal data. Careless distribution of personal data or provision to unknown sources can subsequently lead to various risks.

Secondly, it is important for learners to be able to critically evaluate information. The abundance of information in the digital environment does not mean that all of it is reliable. Therefore, it is necessary to teach learners to evaluate the source of information and identify false and manipulative information.

Third, the formation of safe digital behavior is also inextricably linked to the educational aspect of the educational process. In the digital environment, values such as respect, responsibility, confidentiality, compliance with copyright and consideration of the rights of other users should be formed.

Fourth, building information security knowledge and skills should be a continuous process. Cybersecurity and privacy education programs should be linked to awareness, behavior change, and the development of a security culture. Therefore, it is advisable to organize information security education in the educational process, not limited to teaching a separate topic, but in a way that is connected to the daily digital activities of the learner. Approaching the issue of information security only from a technical point of view is not enough to fully form the real digital behavior of the learner. Because even with the presence of technical protection tools, a wrong decision by the user can negatively affect security. In the pedagogical process, it is important to develop such qualities as independent thinking, situation analysis, risk anticipation, and informed decision-making in the learner.



The use of problem situations, practical tasks, cases, interactive exercises, project work, digital simulations and reflexive tasks can increase the learner's readiness for real-life situations related to information security. An important aspect of this approach is that the learner is not limited to memorizing security rules, but also forms safe digital behavior by finding answers to questions such as "why?", "what is the risk?", "how to act?" Thus, the issue of developing information security competencies should be considered as a complex issue that is inextricably linked to the content, methods, and learning outcomes of the pedagogical process.

Conclusion

The digitalization of the educational process, along with creating new opportunities for learners, also creates new pedagogical problems related to their safety in the digital environment. In the process of using digital educational tools, protecting personal data, critically evaluating information sources, understanding digital threats, and demonstrating safe behavior are becoming one of the important competencies of a modern learner. The analysis shows that information security competence is not limited to technical knowledge. It requires a combination of knowledge, practical skills, motivational-value attitudes, and reflexive abilities. Therefore, the role of the pedagogical approach in the formation of this competence is of particular importance.

The development of the digital educational environment requires a deeper study of the scientific and pedagogical foundations of the formation of information security competence in learners. In particular, determining the structural structure of the competence, determining the pedagogical conditions that affect its development, selecting effective teaching methods and developing criteria for evaluating results. Conducting scientific research in this area, and forming information security competence of learners in the context of digitalization of the educational process is not only a need arising from the requirements of the modern digital environment, but also an important pedagogical task that serves to ensure the safety, quality and sustainability of education.



REFERENCES

1. O‘zbekiston Respublikasi Prezidentining 2020-yil 5-oktabrdagi PF-6079-son Farmoni. “Raqamli O‘zbekiston – 2030” strategiyasini tasdiqlash va uni samarali amalga oshirish chora-tadbirlari to‘g‘risida.
2. Mukhtarov, F. . (2023). IMPROVING THE METHODOLOGY OF TEACHING THE SCIENCE OF "CYBERSECURITY FUNDAMENTALS" IN THE CONDITIONS OF
3. Mukhtarov, F. M. (2023). THE POWER OF CYBERSECURITY EDUCATION: DEFENDING AGAINST DIGITAL THREATS. GOLDEN BRAIN, 1(26), 63–66.
4. Retrieved from <https://researchedu.org/index.php/goldenbrain/article/view/4816>
5. Mukhtarov F. Applying the science of cyber security to the educational process of higher education //Евразийский журнал технологий и инноваций. – 2023. – Т. 1. – №. 9. – С. 72-78.
6. Musayev, A.M., Toshmatov, N.R. Raqamli ta'limda axborot xavfsizligi muammolari // Pedagogika va psixologiya. — Toshkent, 2022. — №4. — B. 34–41.
7. UNESCO. Digital learning and transformation of education: What you need to know. UNESCO.
8. Ribble, M. Digital Citizenship in Schools: Nine Elements All Students Should Know. — 3rd ed. — ISTE, 2015.