

**SUN'IY INTELLEKT VOSITALARIDAN FOYDALANISH
SHAROITIDA TALABALARNING AXBOROT XAVFSIZLIGI
KOMPETENSIYALARINI SHAKLLANTIRISHNING NAZARIY-
METODOLOGIK ASOSLARI****Mustafoyev Shahzod Mamanazar o'g'li**

Buxoro Xalqaro Universiteti

mustaqil izlanuvchisi

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

Annotatsiya. Mazkur maqolada sun'iy intellekt vositalaridan foydalanish sharoitida talabalarning axborot xavfsizligi kompetensiyalarini shakllantirishning nazariy-metodologik asoslari tahlil qilinadi. Raqamli ta'lim muhitida shaxsiy ma'lumotlarni himoya qilish, axborotning ishonchliligini baholash, kiberxavfsizlik tahdidlarini aniqlash va sun'iy intellekt texnologiyalaridan mas'uliyatli foydalanish masalalari yoritiladi. Shuningdek, kompetensiyaviy, tizimli, faoliyatga yo'naltirilgan va shaxsga yo'naltirilgan yondashuvlarning ahamiyati asoslanib, axborot xavfsizligi kompetensiyasining tarkibiy komponentlari hamda uni shakllantirishning pedagogik shart-sharoitlari tavsiflanadi. Taklif etilgan nazariy yondashuvlar oliy ta'lim muassasalarida talabalarning raqamli xavfsizlik madaniyatini rivojlantirishga xizmat qiladi.

Kalit so'zlar: sun'iy intellekt, axborot xavfsizligi, kompetensiya, raqamli ta'lim, kiberxavfsizlik, axborot savodxonligi, shaxsiy ma'lumotlar, raqamli kompetensiya, pedagogik metodologiya, raqamli xavfsizlik madaniyati.

**ТЕОРЕТИКО-МЕТОДОЛОГИЧЕСКИЕ ОСНОВЫ
ФОРМИРОВАНИЯ КОМПЕТЕНЦИЙ ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ СТУДЕНТОВ В УСЛОВИЯХ ИСПОЛЬЗОВАНИЯ
ИНСТРУМЕНТОВ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА**

Аннотация. В данной статье анализируются теоретико-методологические основы формирования компетенций информационной безопасности студентов в условиях использования инструментов искусственного интеллекта. Рассматриваются вопросы защиты персональных данных в цифровой образовательной среде, оценки достоверности информации, выявления угроз кибербезопасности и ответственного использования

технологий искусственного интеллекта. Обосновывается значение компетентностного, системного, деятельностного и личностно ориентированного подходов, а также характеризуются структурные компоненты компетенций информационной безопасности и педагогические условия их формирования. Предложенные теоретические подходы могут служить основой для развития культуры цифровой безопасности студентов в высших образовательных учреждениях.

Ключевые слова: искусственный интеллект, информационная безопасность, компетенция, цифровое образование, кибербезопасность, информационная грамотность, персональные данные, цифровая компетентность, педагогическая методология, культура цифровой безопасности.

THEORETICAL AND METHODOLOGICAL FOUNDATIONS FOR DEVELOPING STUDENTS' INFORMATION SECURITY COMPETENCIES IN THE CONTEXT OF ARTIFICIAL INTELLIGENCE TOOL USE

Abstract. This article examines the theoretical and methodological foundations for developing students' information security competencies in the context of using artificial intelligence tools. It addresses issues related to personal data protection in the digital learning environment, the assessment of information reliability, the identification of cybersecurity threats, and the responsible use of artificial intelligence technologies. Furthermore, the article substantiates the importance of competency-based, systems-based, activity-oriented, and learner-centered approaches, and describes the structural components of information security competencies and the pedagogical conditions required for their development. The proposed theoretical approaches may serve as a foundation for fostering a culture of digital security among students in higher education institutions.

Keywords: artificial intelligence, information security, competency, digital education, cybersecurity, information literacy, personal data, digital competence, pedagogical methodology, digital security culture.

Zamonaviy axborot-kommunikatsiya texnologiyalarining jadal rivojlanishi ta'lim tizimining mazmuni va tashkil etilishiga sezilarli ta'sir ko'rsatmoqda. Ayniqsa, sun'iy intellekt vositalarining ta'lim jarayoniga integratsiyalashuvi talabalarning axborotni izlash, tahlil qilish, qayta ishlash va taqdim etish imkoniyatlarini kengaytirmoqda. Generativ sun'iy intellekt tizimlari matn yaratish, tarjima qilish,

dasturlash va o'quv materiallarini umumlashtirishda keng qo'llanilmoqda. Biroq bu imkoniyatlar bilan bir qatorda, shaxsiy ma'lumotlarning oshkor bo'lishi, noto'g'ri axborot tarqalishi, fishing hujumlari va sun'iy intellekt yaratgan natijalarga tanqidiy yondashmaslik kabi xavflar ham yuzaga kelmoqda. Shu sababli talabalarda axborot xavfsizligi kompetensiyalarini shakllantirish zamonaviy oliy ta'limning dolzarb pedagogik vazifalaridan biri hisoblanadi.

UNESCO tomonidan ishlab chiqilgan talabalarining sun'iy intellekt bo'yicha kompetensiyalari doirasi inson manfaatlariga yo'naltirilgan tafakkur, sun'iy intellekt etikasi va texnologiyalardan mas'uliyatli foydalanishga alohida e'tibor qaratadi. Yevropa Komissiyasining DigComp 2.2 raqamli kompetensiyalar doirasida esa axborot savodxonligi, raqamli xavfsizlik va muammolarni hal qilish muhim yo'nalishlar sifatida belgilangan. Mazkur yondashuvlar sun'iy intellekt vositalaridan foydalanishda talabalarining nafaqat texnologik bilimlarini, balki axborot xavflarini aniqlash, shaxsiy ma'lumotlarni himoya qilish va asoslangan qarorlar qabul qilish qobiliyatlarini rivojlantirish zarurligini ko'rsatadi.

Maqolaning maqsadi sun'iy intellekt vositalaridan foydalanish sharoitida talabalarining axborot xavfsizligi kompetensiyalarini shakllantirishning nazariy-metodologik asoslarini yoritish, uning tarkibiy komponentlarini aniqlash va pedagogik jarayonni takomillashtirish yo'nalishlarini asoslashdan iborat.

Axborot xavfsizligi kompetensiyasi talabaning raqamli muhitda axborot bilan ishlash jarayonida xavfsizlik talablariga rioya qilishi, ehtimoliy tahdidlarni aniqlashi, xavflarni baholashi va ma'lumotlarni himoya qilishga qaratilgan asosli qarorlar qabul qila olishini ifodalaydi. Sun'iy intellekt vositalaridan foydalanish sharoitida ushbu kompetensiya shaxsiy ma'lumotlarning maxfiyligini ta'minlash, yaratilgan axborotning ishonchliligini tekshirish, algoritmik xatolarni anglash va raqamli etikaga rioya qilish ko'nikmalarini ham qamrab oladi.

Mazkur kompetensiyani shakllantirishning nazariy-metodologik asoslari kompetensiyaviy, tizimli, faoliyatga yo'naltirilgan, shaxsga yo'naltirilgan va xavfga yo'naltirilgan yondashuvlarning o'zaro uyg'unligiga tayanadi. Kompetensiyaviy yondashuv bilimlarni amaliy vaziyatlarda qo'llashga, tizimli yondashuv kompetensiyaning tarkibiy qismlarini yaxlit rivojlantirishga, faoliyatga yo'naltirilgan yondashuv esa amaliy topshiriqlar orqali xavfsizlik ko'nikmalarini shakllantirishga xizmat qiladi. Shaxsga yo'naltirilgan yondashuv talabalarining individual tayyorgarligini hisobga olsa, xavfga yo'naltirilgan yondashuv raqamli tahdidlarni aniqlash, ularning oqibatlarini baholash va tegishli himoya choralarini tanlashga yo'naltiriladi. NIST tomonidan ishlab chiqilgan sun'iy intellekt xavflarini boshqarish

doirasi ham ushbu jarayonda xavfsizlik, ishonchlilik va maxfiylik masalalarini tizimli hisobga olish zarurligini ta'kidlaydi.

Talabalarning axborot xavfsizligi kompetensiyasini axborot-kognitiv, amaliy-faoliyatli, qadriyat-motivatsion va reflektiv-baholash komponentlari orqali tavsiflash mumkin. Axborot-kognitiv komponent axborot xavfsizligi tushunchalari, raqamli tahdidlar va sun'iy intellekt tizimlarining imkoniyatlari hamda cheklovlari haqidagi bilimlarni qamrab oladi. Amaliy-faoliyatli komponent ushbu bilimlarni real vaziyatlarda qo'llash, kuchli parollardan foydalanish, ko'p bosqichli autentifikatsiyani yoqish, shubhali havolalarni aniqlash va maxfiy ma'lumotlarni himoyalash qobiliyatini ifodalaydi. Qadriyat-motivatsion komponent axborot xavfsizligiga ongli munosabat, raqamli etika va mas'uliyatli xulq-atvor bilan belgilanadi. Reflektiv-baholash komponenti esa talabaning o'z faoliyatini tahlil qilish, xatolarni aniqlash va xavfsizlikka oid qarorlarining oqibatlarini baholash qobiliyatini tavsiflaydi. Ushbu komponentlarning o'zaro uyg'unligi bilimlarni barqaror amaliy ko'nikma va mas'uliyatli raqamli xulq-atvorga aylantirish imkonini beradi.

Axborot xavfsizligi kompetensiyalarini shakllantirishda ilmiylik, tizimlilik, izchillik, amaliy yo'naltirilganlik, maxfiylikni ta'minlash, tanqidiy fikrlash va mas'uliyat tamoyillariga amal qilish zarur. Ta'lim jarayonida sun'iy intellekt tomonidan yaratilgan ma'lumotlarni mustaqil manbalar orqali tekshirish, shaxsiy ma'lumotlarni himoya qilish va axborotdan foydalanishning huquqiy hamda axloqiy jihatlarini anglashga alohida e'tibor qaratilishi lozim. Bunda nazariy bilimlarni muammoli vaziyatlar, amaliy mashqlar va mustaqil tahlil bilan uyg'unlashtirish samarali pedagogik yechim hisoblanadi.

Mazkur kompetensiyalarni samarali shakllantirish uchun axborot xavfsizligi masalalarini turli fanlar mazmuniga integratsiyalash, xavfsiz raqamli ta'lim muhitini yaratish va pedagoglarning raqamli tayyorgarligini oshirish muhim ahamiyatga ega. Talabalarga sun'iy intellekt tizimlariga maxfiy ma'lumotlarni kiritish bilan bog'liq xavflarni aniqlash, shubhali elektron xabarlarini tahlil qilish, soxta axborotni tekshirish va xavfsiz muqobil yechimlarni tanlashga doir topshiriqlar berilishi mumkin. Bunday faoliyat talabalarning nazariy bilimlarini amaliy vaziyatlarda qo'llash qobiliyatini rivojlantiradi. Shuningdek, o'qituvchilar tomonidan foydalanish qoidalarining aniq belgilanishi, shaxsiy ma'lumotlarni himoya qilish tartiblarining tushuntirilishi va akademik halollik talablariga rioya etilishi zarur.

Talabalarning axborot xavfsizligi kompetensiyalarini baholashda kognitiv, operatsion, motivatsion-aksiologik va reflektiv mezonlardan foydalanish mumkin. Kognitiv mezon xavfsizlikka oid bilimlarni, operatsion mezon amaliy ko'nikmalarni, motivatsion-aksiologik mezon mas'uliyatli munosabatni, reflektiv mezon esa o'z

faoliyatini tahlil qilish va takomillashtirish qobiliyatini ifodalaydi. Baholash jarayonida nazariy testlar bilan bir qatorda vaziyatli topshiriqlar, amaliy mashqlar va refleksiv hisobotlardan foydalanish maqsadga muvofiq. Kompetensiyaning boshlang'ich, o'rta va yuqori darajalarini belgilash uchun har bir mezon bo'yicha aniq indikatorlar ishlab chiqilishi hamda ular amaliy tadqiqotlar orqali tekshirilishi lozim.

Sun'iy intellekt vositalaridan foydalanish sharoitida talabalarning axborot xavfsizligi kompetensiyalarini shakllantirish zamonaviy oliy ta'limning muhim yo'nalishi bo'lib, u texnologik bilimlarni xavfsiz amaliy faoliyat, tanqidiy fikrlash va mas'uliyatli raqamli xulq-atvor bilan uyg'unlashtirishni talab etadi. Nazariy tahlil kompetensiyaviy, tizimli, faoliyatga yo'naltirilgan, shaxsga yo'naltirilgan va xavfga yo'naltirilgan yondashuvlarni birgalikda qo'llash ushbu jarayonni izchil tashkil etishga yordam berishini ko'rsatadi. Axborot-kognitiv, amaliy-faoliyatli, qadriyat-motivatsion va refleksiv-baholash komponentlariga asoslangan konseptual tuzilma talabalarning axborot xavfsizligi kompetensiyalarini yaxlit rivojlantirish uchun nazariy asos bo'lib xizmat qilishi mumkin. Oliy ta'lim amaliyotida xavfsizlik masalalarini o'quv fanlariga integratsiyalash, amaliy topshiriqlardan foydalanish, pedagoglarning tayyorgarligini oshirish va kompetensiyalarni aniq mezonlar asosida baholash zarur. Taklif etilgan yondashuvning samaradorligini aniqlash uchun kelgusida tajriba-sinov tadqiqotlarini o'tkazish va olingan natijalar asosida metodik tavsiyalar ishlab chiqish maqsadga muvofiq.

Foydalanilgan adabiyotlar ro'yxati

1. UNESCO. *AI Competency Framework for Students*. Paris: UNESCO, 2024. <https://www.unesco.org/en/articles/ai-competency-framework-students>
2. Vuorikari, R., Kluzer, S., Punie, Y. *DigComp 2.2: The Digital Competence Framework for Citizens*. Luxembourg: Publications Office of the European Union, 2022. <https://doi.org/10.2760/115376>
3. National Institute of Standards and Technology. *Artificial Intelligence Risk Management Framework (AI RMF 1.0)*. NIST AI 100-1. Gaithersburg, MD: NIST, 2023. <https://doi.org/10.6028/NIST.AI.100-1>
4. National Institute of Standards and Technology. *NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management, Version 1.0*. Gaithersburg, MD: NIST, 2020. <https://doi.org/10.6028/NIST.CSWP.01162020>
5. UNESCO. *Guidance for Generative AI in Education and Research*. Paris: UNESCO, 2023. <https://doi.org/10.54675/EWZM9535>

6. International Organization for Standardization. *ISO/IEC 27001:2022 Information Security, Cybersecurity and Privacy Protection — Information Security Management Systems — Requirements*. Geneva: ISO, 2022.

7. International Organization for Standardization. *ISO/IEC 23894:2023 Information Technology — Artificial Intelligence — Guidance on Risk Management*. Geneva: ISO, 2023.