

Mustafoev Shahzod Mamanazar o'g'li

Buxoro xalqaro universiteti

mustaqil izlanuvchisi

shahzod@buxdpi.uz

0009-0007-8584-1237

TALABANING AXBOROT XAVFSIZLIGI KOMPETENSIYASI PEDAGOGIK TUSHUNCHA SIFATIDA: MOHIYATI, TARKIBI VA SUN'IY INTELLEKT SHAROITIDAGI O'ZIGA XOSLIGI

Annotatsiya. Mazkur maqolada talabanning axborot xavfsizligi kompetensiyasi pedagogik tushuncha sifatida nazariy jihatdan tahlil qilinadi. Uning mohiyati, tarkibiy komponentlari va shakllanishiga ta'sir etuvchi pedagogik omillar yoritiladi. Sun'iy intellekt vositalarining ta'lim jarayoniga keng joriy etilishi sharoitida shaxsiy ma'lumotlarni himoya qilish, axborotning ishonchliligini baholash, kiberxavflarni aniqlash, raqamli etika me'yorlariga rioya qilish hamda sun'iy intellekt yaratgan kontentga tanqidiy yondashish masalalariga alohida e'tibor qaratiladi. Shuningdek, axborot xavfsizligi kompetensiyasining kognitiv, amaliy-faoliyatga oid, qadriyatli-motivatsion va refleksiv komponentlari asoslab beriladi. Kompetensiyani shakllantirishda kompetensiyaviy, tizimli, faoliyatga yo'naltirilgan va shaxsga yo'naltirilgan yondashuvlarning pedagogik imkoniyatlari ochib beriladi.

Kalit so'zlar: axborot xavfsizligi, talaba, kompetensiya, sun'iy intellekt, raqamli ta'lim, kiberxavfsizlik, shaxsiy ma'lumotlar, axborot savodxonligi, raqamli etika, tanqidiy fikrlash.

КОМПЕТЕНЦИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СТУДЕНТА КАК ПЕДАГОГИЧЕСКОЕ ПОНЯТИЕ: СУЩНОСТЬ, СТРУКТУРА И ОСОБЕННОСТИ В УСЛОВИЯХ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Аннотация. В данной статье проводится теоретический анализ компетенции информационной безопасности студента как педагогического понятия. Раскрываются её сущность, структурные компоненты и педагогические факторы, влияющие на её формирование. Особое внимание уделяется вопросам защиты персональных данных, оценки достоверности информации, выявления киберугроз, соблюдения норм цифровой этики и критического отношения к контенту, созданному искусственным интеллектом, в условиях широкого внедрения инструментов искусственного интеллекта в образовательный процесс. Кроме того, обосновываются когнитивный, практико-деятельностный, ценностно-мотивационный и рефлексивный компоненты компетенции информационной безопасности. Раскрываются педагогические возможности компетентностного, системного, деятельностного и личностно ориентированного подходов к формированию данной компетенции.

Ключевые слова: информационная безопасность, студент, компетенция, искусственный интеллект, цифровое образование, кибербезопасность, персональные данные, информационная грамотность, цифровая этика, критическое мышление.

STUDENTS' INFORMATION SECURITY COMPETENCE AS A PEDAGOGICAL CONCEPT: ITS ESSENCE, STRUCTURE, AND SPECIFIC FEATURES IN THE CONTEXT OF ARTIFICIAL INTELLIGENCE

Abstract. This article provides a theoretical analysis of students' information security competence as a pedagogical concept. It examines its essence, structural components, and the

pedagogical factors influencing its development. Particular attention is paid to the protection of personal data, the assessment of information reliability, the identification of cyber threats, compliance with digital ethics standards, and the development of a critical approach to content generated by artificial intelligence in the context of the widespread integration of artificial intelligence tools into the educational process. Furthermore, the cognitive, practical-activity, value-motivational, and reflective components of information security competence are substantiated. The article also explores the pedagogical potential of competency-based, systemic, activity-oriented, and learner-centered approaches to developing this competence.

Keywords: *information security, student, competence, artificial intelligence, digital education, cybersecurity, personal data, information literacy, digital ethics, critical thinking.*

Raqamli texnologiyalar va sun'iy intellekt vositalarining jadal rivojlanishi oliy ta'lim mazmuni, metodlari hamda talabalarga qo'yiladigan kompetensiyaviy talablarning o'zgarishiga olib kelmoqda. Bugungi kunda talabalar ta'limiy topshiriqlarni bajarish, ilmiy ma'lumotlarni izlash, matnlarni tahlil qilish, tarjima qilish va mustaqil ta'limni tashkil etishda turli sun'iy intellekt vositalaridan foydalanmoqda. Ushbu imkoniyatlar ta'lim samaradorligini oshirish bilan birga, shaxsiy ma'lumotlarning oshkor bo'lishi, noto'g'ri axborot tarqalishi, soxta manbalarga tayanish, fishing hujumlari va akademik halollik bilan bog'liq muammolarni ham yuzaga keltirmoqda. Shu sababli talabaning axborot xavfsizligi kompetensiyasini shakllantirish zamonaviy oliy ta'limning muhim pedagogik vazifalaridan biri hisoblanadi.

Yevropa Komissiyasining DigComp 2.2 raqamli kompetensiyalar doirasi raqamli texnologiyalardan ishonchli, tanqidiy va xavfsiz foydalanish uchun zarur bo'lgan bilim, ko'nikma va munosabatlarni qamrab oladi. UNESCO tomonidan ishlab chiqilgan sun'iy intellekt bo'yicha o'quvchilar kompetensiyasi doirasi esa inson manfaatlariga yo'naltirilgan fikrlash, sun'iy intellekt etikasi, texnologik bilimlar va amaliy qo'llash masalalariga e'tibor qaratadi. Mazkur yondashuvlar talabaning axborot xavfsizligini faqat texnik himoya vositalarini bilish bilan cheklamasdan, uni axborot bilan ongli, mas'uliyatli va tanqidiy munosabatda bo'lishni ta'minlaydigan yaxlit kompetensiya sifatida talqin qilish zarurligini ko'rsatadi.

Maqolaning maqsadi talabaning axborot xavfsizligi kompetensiyasini pedagogik tushuncha sifatida nazariy jihatdan asoslash, uning tarkibiy tuzilishini aniqlashtirish hamda sun'iy intellekt vositalaridan foydalanish sharoitidagi o'ziga xos jihatlarini ochib berishdan iborat.

Pedagogik nuqtayi nazardan kompetensiya muayyan faoliyatni samarali amalga oshirish uchun zarur bo'lgan bilim, ko'nikma, malaka, qadriyat va shaxsiy sifatning o'zaro uyg'unligini ifodalaydi. Kompetensiya faqat nazariy bilimlarni o'zlashtirishni emas, balki ularni real vaziyatlarda mustaqil qo'llash, muammolarni aniqlash, maqbul qaror qabul qilish va o'z faoliyati natijalarini baholash qobiliyatini ham nazarda tutadi. Shu ma'noda, axborot xavfsizligi kompetensiyasi talabaning raqamli muhitda axborotni izlash, qabul qilish, qayta ishlash, saqlash va uzatish jarayonlarida xavfsizlik talablariga ongli ravishda amal qilishga tayyorligini ifodalaydi.

Talabaning axborot xavfsizligi kompetensiyasini uning raqamli muhitdagi axborotiy faoliyatini xavfsiz, mas'uliyatli va tanqidiy tashkil etish imkonini beruvchi bilimlar, amaliy ko'nikmalar, qadriyatlar va refleksiv qobiliyatlarning integrativ majmui sifatida ta'riflash mumkin. Ushbu ta'rifda uchta muhim jihat mujassam: xavfsizlikka oid bilimlarni egallash, mazkur bilimlarni amaliy faoliyatda qo'llash va axborot bilan ishlashda mas'uliyatli xulq-atvorni namoyon etish.

Mazkur kompetensiya axborot savodxonligi, raqamli kompetensiya va kiberxavfsizlik bilan uzviy bog'liq bo'lsa-da, ular bilan aynan bir xil tushuncha emas. Axborot savodxonligi, asosan, axborotga ehtiyojni aniqlash, uni izlash, tahlil qilish va baholash bilan bog'liq. Raqamli kompetensiya raqamli texnologiyalardan samarali foydalanishning kengroq doirasini qamrab oladi. Kiberxavfsizlik esa axborot tizimlari, qurilmalar, tarmoqlar va ma'lumotlarni turli tahdidlardan himoya qilishga qaratilgan texnik hamda tashkiliy choralarni ham o'z ichiga oladi.

Talabaning axborot xavfsizligi kompetensiyasi ushbu yoʻnalishlarni pedagogik jihatdan birlashtirib, ularni shaxsning kundalik taʼlimiy va ilmiy faoliyatida namoyon boʻladigan yaxlit sifat sifatida qarash imkonini beradi.

Shu asosda kompetensiyaning shakllanganlik darajasi talabaning xavfsizlik qoidalarini bilishi bilangina emas, balki xavfli vaziyatlarni aniqlashi, tegishli himoya choralarini tanlashi, axborot manbalarini tekshirishi va oʻz qarorlarining oqibatlarini anglay olishi bilan belgilanadi.

Talabaning axborot xavfsizligi kompetensiyasini pedagogik jihatdan izchil shakllantirish uchun uning ichki tuzilishini aniqlash muhimdir. Mazkur maqolada ushbu kompetensiyaning oʻzaro bogʻliq toʻrtta komponentini ajratish taklif etiladi: kognitiv, amaliy-faoliyatga oid, qadriyatli-motivatsion va refleksiv komponentlar. Bu tasnif muallifning nazariy umumlashtirishi boʻlib, raqamli kompetensiya va masʼuliyatli sunʼiy intellektdan foydalanishga oid xalqaro yondashuvlar bilan uygʻunlashtirilgan.

Kognitiv komponent talabaning axborot xavfsizligi, shaxsiy maʼlumotlarni himoya qilish, maxfiylik, kiberxavflar, raqamli identifikatsiya, axborotning ishonchliligi va sunʼiy intellekt faoliyatining asosiy xususiyatlari haqidagi bilimlarini qamrab oladi. Ushbu komponent doirasida talaba fishing xabarlarining belgilarini, kuchli autentifikatsiya tamoyillarini, xavfsiz parol yaratish qoidalarini, axborot manbalarini tekshirish usullarini hamda raqamli izning mohiyatini bilishi lozim. Shuningdek, sunʼiy intellekt tizimlari notoʻgʻri yoki uydirma maʼlumotlarni ishonchli shaklda taqdim etishi mumkinligini anglash ham mazkur komponentning muhim qismidir.

Amaliy-faoliyatga oid komponent xavfsizlikka doir bilimlarni amalda qoʻllash qobiliyatini ifodalaydi. U shaxsiy hisoblarni himoyalash, koʻp omilli autentifikatsiyadan foydalanish, dasturiy taʼminotni yangilab borish, maxfiy maʼlumotlarni himoyalangan platformalarga kiritmaslik, shubhali havolalarni tekshirish va ishonchli axborot manbalarini tanlash kabi amaliy harakatlarni oʻz ichiga oladi. Sunʼiy intellekt vositalari bilan ishlashda esa soʻrov mazmunini xavfsiz shakllantirish, shaxsni aniqlash imkonini beradigan maʼlumotlarni yashirish, yaratilgan natijalarni boshqa ishonchli manbalar bilan solishtirish va ulardan foydalanishdan oldin aniqligini tekshirish muhim hisoblanadi.

Qadriyatli-motivatsion komponent talabaning axborot xavfsizligiga boʻlgan munosabati, shaxsiy va oʻzgalarning maʼlumotlariga hurmat bilan qarashi, raqamli muhitda masʼuliyatni his etishi hamda xavfsizlik qoidalariga ongli ravishda rioya qilishini anglatadi. Bu komponent tashqi nazorat yoki jazodan qoʻrqish bilan emas, balki xavfsiz xulq-atvorning zarurligini anglash bilan tavsiflanadi. Akademik halollik, mualliflik huquqiga hurmat, axborotni ruxsatsiz tarqatmaslik va sunʼiy intellektdan foydalanishda shaffoflikka rioya etish mazkur komponentning muhim koʻrsatkichlaridir.

Refleksiv komponent talabaning oʻz axborotiy xatti-harakatlarini tahlil qilish, yoʻl qoʻyilgan xatolarni aniqlash, xavfsizlikka oid qarorlarini baholash va kelgusida faoliyatini takomillashtirish qobiliyatini qamrab oladi. Talaba oʻzi foydalangan sunʼiy intellekt vositasining natijalariga qay darajada tayanganini, qanday maʼlumotlarni taqdim etganini, axborotning toʻgʻriligini qanday tekshirganini va yuzaga kelishi mumkin boʻlgan xavflarni qay darajada hisobga olganini tahlil qila olishi zarur.

Ushbu komponentlar bir-birini toʻldiradi. Bilim amaliy koʻnikmalar bilan mustahkamlanmasa, xavfsizlik qoidalari real vaziyatlarda toʻliq qoʻllanilmaydi. Amaliy koʻnikmalar masʼuliyatli qadriyatlar bilan uygʻunlashmasa, talaba xavfsizlik talablarini faqat zarurat tugʻilganda bajarishi mumkin. Refleksiya esa oʻz faoliyatini tahlil qilish va tajriba asosida takomillashtirish imkonini beradi.

Sunʼiy intellekt vositalarining taʼlim jarayoniga kirib kelishi axborot xavfsizligi kompetensiyasining mazmunini kengaytirmoqda. Anʼanaviy raqamli muhitda talaba, asosan, qurilma, hisob qaydnomasi, tarmoq va maʼlumotlarni himoya qilishga eʼtibor qaratgan boʻlsa, generativ sunʼiy intellekt sharoitida u oʻzi kiritayotgan maʼlumotlar, tizim tomonidan yaratilayotgan kontent, algoritmik cheklovlar va avtomatik tavsiyalarning oqibatlarini ham hisobga olishi kerak.

Birinchidan, shaxsiy ma'lumotlarni himoya qilish talabi yanada dolzarb tus oladi. Talabalar sun'iy intellekt tizimlariga topshiriq matnlari, ilmiy loyihalar, shaxsiy yozishmalar yoki boshqa hujjatlarni kiritishda ularning maxfiylik darajasini baholashi lozim. Ochiq foydalanishga mo'ljallangan vositaga shaxsni aniqlash imkonini beruvchi, moliyaviy yoki boshqa maxfiy ma'lumotlarni kiritish xavf tug'dirishi mumkin. Shu bois talabalarda ma'lumotlarni minimallashtirish, zarur hollarda ularni shaxssizlantirish va foydalanilayotgan platformaning maxfiylik shartlarini o'rganish ko'nikmalarini rivojlantirish zarur.

Ikkinchidan, sun'iy intellekt yaratgan axborotning ishonchliligini baholash alohida ahamiyat kasb etadi. Generativ tizimlar ravon va mantiqan izchil ko'rinadigan, biroq faktik jihatdan xato ma'lumotlar, mavjud bo'lmagan ilmiy manbalar yoki noto'g'ri iqtiboslarni taqdim etishi mumkin. Shu sababli talaba sun'iy intellekt javobini tayyor bilim sifatida qabul qilmasdan, uni ilmiy adabiyotlar, rasmiy hujjatlar va ishonchli manbalar orqali tekshirishi kerak. Bunda manbaning muallifi, nashr sanasi, ilmiy maqomi, dalillarning asoslanganligi va boshqa manbalar bilan muvofiqligi tahlil qilinadi.

Uchinchidan, sun'iy intellektidan foydalanish algoritmik tarafkashlik va axborotning bir tomonlama taqdim etilishi bilan bog'liq xavflarni anglashni talab qiladi. Model yaratgan javoblar o'quv ma'lumotlaridagi cheklovlar, til va madaniy kontekst yoki so'rovning o'ziga xosligi ta'sirida shakllanishi mumkin. Talaba bunday natijalarni mutlaq haqiqat sifatida qabul qilmasligi, muqobil nuqtayi nazarlarni solishtirishi va qarorlarni mustaqil tahlil asosida qabul qilishi zarur. UNESCOning 2024-yilda e'lon qilingan sun'iy intellekt bo'yicha kompetensiya doirasi ham inson manfaatlariga yo'naltirilgan yondashuv, etika va tanqidiy baholashning ahamiyatini ta'kidlaydi.

To'rtinchidan, akademik halollik va intellektual mulk masalalari axborot xavfsizligi bilan uzviy bog'lanadi. Sun'iy intellekt yordamida tayyorlangan matn yoki tahlildan foydalanishda oliy ta'lim muassasasining talablariga amal qilish, zarur hollarda vositadan foydalanilganini ko'rsatish, manbalarni to'g'ri rasmiylashtirish va o'z hissasini aniq belgilash talab etiladi. Sun'iy intellekt yaratgan matnni tekshirmasdan o'z ishi sifatida taqdim etish nafaqat akademik halollikka, balki ilmiy axborotning ishonchliligiga ham salbiy ta'sir ko'rsatadi.

Beshinchidan, sun'iy intellekt bilan ishlash jarayonida raqamli xavfsizlikka oid yangi tahdidlarni tanib olish ko'nikmasi zarur. Bunday tahdidlarga sun'iy intellekt yordamida tayyorlangan soxta xabarlar, ovoz yoki tasvirni taqlid qilish, ishonchli shaxs nomidan yuborilgan firibgar murojaatlar va zararli havolalar kirishi mumkin. Talaba shubhali axborotning manbasini tekshirishi, favqulodda talablar yoki maxfiy ma'lumotlarni so'rashga ehtiyotkor munosabatda bo'lishi va zarur vaziyatlarda tegishli mutaxassisga murojaat qilishi lozim.

Shunday qilib, sun'iy intellekt sharoitida axborot xavfsizligi kompetensiyasi texnik himoya ko'nikmalaridan tashqari, axborotni tanqidiy baholash, ma'lumotlarni mas'uliyatli boshqarish, algoritmik natijalarni tushunish va raqamli etika me'yorlariga rioya qilishni ham qamrab oladi. Bu kompetensiya statik bilimlar majmui emas, balki texnologiyalar va tahdidlar o'zgarishi bilan muntazam rivojlantirib borilishi zarur bo'lgan integrativ shaxsiy sifatdir.

Talabalarda axborot xavfsizligi kompetensiyasini shakllantirish jarayoni maqsadli tashkil etilgan pedagogik faoliyatni talab qiladi. Bunda kompetensiyaviy yondashuv ta'lim natijalarini talabning real vaziyatlarda xavfsiz va mas'uliyatli harakat qila olish qobiliyati bilan bog'lash imkonini beradi. Tizimli yondashuv esa axborot xavfsizligi mavzularini alohida fan doirasida cheklab qo'ymasdan, turli o'quv fanlari va mustaqil ta'lim faoliyatiga integratsiyalashni nazarda tutadi. Faoliyatga yo'naltirilgan yondashuv amaliy topshiriqlar, vaziyatli tahlillar va muammoli vazifalar orqali xavfsiz xulq-atvor ko'nikmalarini rivojlantiradi. Shaxsga yo'naltirilgan yondashuv talabalarning raqamli tajribasi, ehtiyojlari va tayyorgarlik darajasini hisobga olishga yordam beradi.

Pedagogik jarayonda real hayotga yaqin vaziyatlardan foydalanish samarali vosita bo'lishi mumkin. Masalan, talabalarga shubhali elektron xatni tahlil qilish, sun'iy intellekt yaratgan ilmiy manbaning mavjudligini tekshirish, ochiq platformaga yuborishdan oldin hujjatdagi maxfiy ma'lumotlarni aniqlash yoki raqamli xizmatning maxfiylik siyosatini baholash

topshiriqlari beriladi. Bunday vazifalar nazariy bilimlarni amaliy faoliyat bilan bog'laydi va talabani mustaqil qaror qabul qilish qobiliyatini rivojlantiradi.

Kompetensiyani shakllantirishda muammoli ta'lim, keys-stadi, loyiha metodi, guruhli muhokama va refleksiv topshiriqlardan foydalanish mumkin. Masalan, "Sun'iy intellekt yaratgan javobni ilmiy ishda qo'llash mumkinmi?" mavzusidagi keys orqali talabalar manbalarni tekshirish, mualliflik huquqi, akademik halollik va axborotning ishonchliligi masalalarini birgalikda tahlil qiladilar. Bunda o'qituvchining vazifasi faqat qoidalarni tushuntirishdan iborat bo'lmay, balki talabalarning dalillarga asoslangan qaror qabul qilishiga yo'naltirishdan iborat bo'ladi.

Axborot xavfsizligi kompetensiyasini baholashda faqat test natijalariga tayanish yetarli emas. Bilimlarni tekshiruvchi savollar bilan bir qatorda amaliy vazifalarni bajarish, xavfli vaziyatlarni aniqlash, xavfsiz yechim tanlash va o'z qarorlarini asoslash qobiliyati ham baholanishi kerak. Shu maqsadda quyidagi mezonlardan foydalanish mumkin: axborot xavfsizligi bo'yicha bilimlarning to'liqligi; xavfsiz amaliy harakatlarni to'g'ri bajarish; shaxsiy ma'lumotlar va intellektual mulkka mas'uliyatli munosabat; sun'iy intellekt yaratgan axborotni tanqidiy tekshirish; o'z faoliyatini tahlil qilish va xatolarni tuzatish qobiliyati. Quyidagi 1-jadvalda Talabani axborot xavfsizligi kompetensiyasining tarkibiy qismlari va ularning tavsifi keltirib o'tilgan.

1-jadval

№	Tarkibiy qism	Mazmuni	Asosiy ko'nikma va qobiliyatlar	Sun'iy intellekt sharoitidagi namoyon bo'lishi
1	Kognitiv komponent	Axborot xavfsizligi, kiberxavfsizlik va raqamli muhitga oid bilimlar majmui	Axborot tahdidlarini bilish, ma'lumotlarning ishonchliligini baholash, xavfsizlik qoidalarini tushunish	Sun'iy intellekt yaratgan ma'lumotlarning aniqligini tekshirish, soxta axborot va algoritmik tarafdashlikni aniqlash
2	Amaliy-faoliyat komponenti	Axborotni himoya qilishga qaratilgan amaliy harakatlar va ko'nikmalar	Kuchli parollardan foydalanish, ikki bosqichli autentifikatsiyani qo'llash, xavfsiz internetdan foydalanish	Shaxsiy ma'lumotlarni AI vositalariga kiritishda ehtiyotkorlik, xavfsiz raqamli xizmatlardan foydalanish
3	Qadriyat-motivatsion komponent	Axborot xavfsizligiga mas'uliyatli munosabat va xavfsiz xulq-atvoriga ichki ehtiyoj	Raqamli etika me'yorlariga rioya qilish, boshqalarning shaxsiy hayotini hurmat qilish, mas'uliyatli qaror qabul qilish	AI vositalaridan halol foydalanish, mualliflik huquqini hurmat qilish va shaxsiy ma'lumotlar daxlsizligini saqlash
4	Refleksiv komponent	O'z faoliyatini tahlil qilish, xatolarni aniqlash va xavfsizlik xulq-atvorini takomillashtirish	Xavflarni tahlil qilish, o'z harakatlarini baholash, xatolardan xulosa chiqarish	AI tomonidan berilgan javoblarni tanqidiy tahlil qilish, raqamli izni baholash va xavfsizlik choralarini takomillashtirish

Mazkur mezonlar asosida kompetensiyaning boshlang'ich, o'rta va yuqori darajalarini belgilash mumkin. Boshlang'ich darajada talaba asosiy xavflarni biladi, biroq murakkab vaziyatlarda o'qituvchi ko'magiga muhtoj bo'ladi. O'rta darajada u odatiy raqamli vaziyatlarda

xavflarni aniqlab, tegishli himoya choralarini mustaqil qo'llaydi. Yuqori darajada esa talaba turli manbalarni solishtiradi, murakkab xavflarni tahlil qiladi, sun'iy intellekt natijalarini tekshiradi va xavfsiz qarorlarini dalillar bilan asoslay oladi. Bu darajalar taklif etilayotgan pedagogik modelning amaliy mezonlari bo'lib, ularni ta'lim muassasasi sharoiti va o'quv natijalariga mos ravishda aniqlashtirish talab etiladi.

Shuningdek, axborot xavfsizligi kompetensiyasini shakllantirish faqat talabanning individual mas'uliyati bilan cheklanmasligi lozim. Oliy ta'lim muassasasi xavfsiz raqamli infratuzilmani ta'minlashi, sun'iy intellekt vositalaridan foydalanish bo'yicha aniq qoidalarni ishlab chiqishi, pedagoglarning raqamli kompetensiyasini rivojlantirishi va talabalar uchun maslahat hamda yordam mexanizmlarini yaratishi zarur. Bunday muhit xavfsiz xulq-atvorni kundalik ta'lim amaliyotining ajralmas qismiga aylantirishga xizmat qiladi.

Talabanning axborot xavfsizligi kompetensiyasi zamonaviy pedagogikada raqamli muhitda xavfsiz, ongli, tanqidiy va mas'uliyatli faoliyat yuritishni ta'minlaydigan integrativ shaxsiy sifat sifatida qaralishi lozim. Uning mohiyati axborot xavfsizligiga oid bilimlarni egallash, ularni amaliy vaziyatlarda qo'llash, raqamli etika me'yorlariga rioya qilish va o'z faoliyatini tahlil qilish qobiliyatlarining birligida namoyon bo'ladi. Maqolada ushbu kompetensiyaning kognitiv, amaliy-faoliyatga oid, qadriyatli-motivatsion va refleksiv komponentlari ajratib ko'rsatildi. Ularning o'zaro uyg'unligi talabanning nafaqat xavfsizlik qoidalarini bilishi, balki ularni real ta'limiy va ilmiy faoliyatda ongli ravishda qo'llashi uchun asos yaratadi. Sun'iy intellekt sharoitida mazkur kompetensiyaning mazmuni shaxsiy ma'lumotlarni himoya qilish, generativ tizimlar yaratgan axborotning ishonchliligini tekshirish, algoritmik tarfakshlikni anglash, soxta kontent va kiberxavflarni aniqlash hamda akademik halollikka rioya qilish bilan boyib bormoqda. Shu bois oliy ta'limda axborot xavfsizligini o'qitish texnik qoidalarni bayon qilish bilan cheklanmasdan, tanqidiy fikrlash, mas'uliyatli qaror qabul qilish va refleksiv faoliyatni rivojlantirishga yo'naltirilishi kerak.

Xulosa qilib aytganda, talabanning axborot xavfsizligi kompetensiyasini shakllantirish uzluksiz, tizimli va amaliyotga yo'naltirilgan pedagogik jarayon bo'lib, unda ta'lim mazmuni, o'qitish metodlari, baholash mezonlari va institutsional xavfsizlik siyosati o'zaro uyg'unlashishi zarur. Mazkur yo'nalishda taklif etilgan nazariy yondashuvlar kelgusida kompetensiyani shakllantirish metodikasini ishlab chiqish va uning samaradorligini empirik tadqiqotlar orqali baholash uchun asos bo'lib xizmat qilishi mumkin.

Foydalanilgan adabiyotlar

1. Miao, F., Shiohira, K., Lao, N. 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. 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>
4. UNESCO. Guidance for Generative AI in Education and Research. Paris: UNESCO, 2023. <https://doi.org/10.54675/EWZM9535>
5. National Institute of Standards and Technology. NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management, Version 1.0. 2020. <https://doi.org/10.6028/NIST.CSWP.01162020>
6. ISO/IEC 27001:2022. Information Security, Cybersecurity and Privacy Protection — Information Security Management Systems — Requirements. Geneva: International Organization for Standardization, 2022.
7. ISO/IEC 23894:2023. Information Technology — Artificial Intelligence — Guidance on Risk Management. Geneva: International Organization for Standardization, 2023.