RAQAMLI TA'LIM MUHITIDA AI ASOSIDAGI O'QITISH TIZIMLARINING AXBOROT XAVFSIZLIGINI TA'MINLASH

To'xtayeva Shahnoza G'aybulla qizi,
"Cyber university" davlat universiteti
Chet tillari va gumanitar fanlar kafedrasi dotsenti

DOI: https://doi.org/10.5281/zenodo.18501945

Annotatsiya. *Mazkur maqolada raqamli ta'lim muhitida sun'iy intellekt (AI) asosidagi o'qitish tizimlaridan foydalanish jarayonida axborot xavfsizligini ta'minlash masalalari tahlil qilinadi. Tadqiqotda AI texnologiyalariga asoslangan ta'lim platformalarida shaxsiy ma'lumotlarni himoyalash, ma'lumotlar maxfiyligi, yaxlitligi va mavjudligini ta'minlash bilan bog'liq asosiy xavf-xatarlar yoritiladi. Shuningdek, algoritmik shaffoflik, ma'lumotlardan noqonuniy foydalanish va kiberxavfsizlik muammolarining ta'lim jarayoniga ta'siri ko'rib chiqiladi. Maqolada axborot xavfsizligini ta'minlashga qaratilgan texnik va tashkiliy choralar, shuningdek, normativ-huquqiy yondashuvlarning ahamiyati asoslab beriladi. Olingan xulosalar AI asosidagi o'qitish tizimlarini xavfsiz va barqaror joriy etishda ilmiy-amaliy ahamiyatga ega.*

Kalit so'zlar: *raqamli ta'lim muhiti, sun'iy intellekt, axborot xavfsizligi, AI asosidagi o'qitish tizimlari, kiberxavfsizlik, shaxsiy ma'lumotlarni himoyalash.*

Аннотация. *В статье рассматриваются вопросы обеспечения информационной безопасности в цифровой образовательной среде при использовании обучающих систем на основе искусственного интеллекта. Анализируются основные угрозы, связанные с защитой персональных данных, конфиденциальностью, целостностью и доступностью информации в AI-ориентированных образовательных платформах. Особое внимание уделяется проблемам алгоритмической прозрачности, несанкционированного использования данных и киберугроз, влияющих на образовательный процесс. Обосновывается значение технических, организационных и нормативно-правовых мер по обеспечению информационной безопасности. Полученные выводы могут быть использованы при внедрении безопасных и устойчивых AI-систем в сфере образования.*

Ключевые слова: *цифровая образовательная среда, искусственный интеллект, информационная безопасность, обучающие системы на основе AI, кибербезопасность, защита персональных данных.*

Abstract. *This article examines the issue of ensuring information security in digital learning environments through the use of AI-based instructional systems. The study analyzes key risks related to data privacy, confidentiality, integrity, and availability in artificial intelligence–driven educational platforms. Special attention is given to challenges such as algorithmic transparency, unauthorized data use, and cybersecurity threats that may affect the educational process. The paper highlights the importance of technical, organizational, and legal measures for safeguarding information security. The findings contribute to the secure and sustainable implementation of AI-based teaching systems in digital education.*

Keywords: *digital learning environment, artificial intelligence, information security, AI-based teaching systems, cybersecurity, data protection.*

Kirish. Raqamli texnologiyalar va sun'iy intellekt (AI) tizimlarining jadal rivojlanishi ta'lim jarayonining mazmuni, shakllari va boshqaruv mexanizmlarini tubdan o'zgartirmoqda. Bugungi kunda AI asosidagi o'qitish tizimlari adaptiv ta'lim, individual o'quv trajektoriyalarini shakllantirish, o'quv jarayonini tahlil qilish va baholash kabi

imkoniyatlari bilan raqamli ta’lim muhitining muhim tarkibiy qismiga aylanmoqda. Biroq ushbu texnologiyalarning keng joriy etilishi bilan bir qatorda axborot xavfsizligini ta’minlash masalasi ham dolzarb muammolardan biri sifatida yuzaga chiqmoqda.

AI asosidagi o‘qitish tizimlari katta hajmdagi ma’lumotlar, jumladan, o‘quvchilarning shaxsiy, akademik va xulq-atvoriga oid axborotlarni qayta ishlaydi. Ushbu ma’lumotlardan foydalanish jarayonida maxfiylik, yaxlitlik va mavjudlik tamoyillarining buzilishi ta’lim jarayonining ishonchliligiga, shuningdek, o‘quvchilarning axborot huquqlari va shaxsiy xavfsizligiga salbiy ta’sir ko‘rsatishi mumkin. Shu sababli raqamli ta’lim muhitida AI tizimlarining xavfsiz ishlashini ta’minlash nafaqat texnik, balki pedagogik va tashkiliy ahamiyatga ega masala hisoblanadi. Zamonaviy tadqiqotlarda ta’kidlanishicha, AI texnologiyalariga asoslangan ta’lim platformalarida axborot xavfsizligi muammolari ko‘pincha kiberxurujlar, ma’lumotlardan noqonuniy foydalanish, algoritmik xatoliklar va shaffoflikning yetishmasligi bilan bog‘liq bo‘ladi. Bu holatlar ta’lim jarayonining barqarorligi va sifatiga putur yetkazib, raqamli ta’lim muhitiga bo‘lgan ishonchni pasaytirishi mumkin. Shu bois, AI asosidagi o‘qitish tizimlarida axborot xavfsizligini ta’minlash masalalarini ilmiy asosda o‘rganish va samarali himoya mexanizmlarini ishlab chiqish zarurati ortib bormoqda.

Pedagogik nuqtai nazardan, axborot xavfsizligi ta’lim jarayonining ajralmas qismi bo‘lib, u o‘quvchilarning raqamli muhitda xavfsiz faoliyat yuritishini ta’minlash bilan birga, mas’uliyatli va ongli axborot madaniyatini shakllantirishga xizmat qiladi. Shu bilan birga, texnologik jihatdan axborot xavfsizligini ta’minlash AI algoritmlarining shaffofligi, ma’lumotlarni himoyalash vositalari va normativ-huquqiy mexanizmlarning uyg‘unlashuvini talab etadi. Mazkur maqolada raqamli ta’lim muhitida AI asosidagi o‘qitish tizimlarining axborot xavfsizligini ta’minlash masalalari tahlil qilinib, mavjud muammolar, xavf-xatarlar hamda ularni bartaraf etishning pedagogik, texnik va tashkiliy yo‘llari ilmiy asosda yoritiladi.

Adabiyotlar tahlili. Raqamli ta’lim muhitining shakllanishi va sun’iy intellekt texnologiyalarining ta’lim jarayoniga jadal joriy etilishi so‘nggi yillarda ilmiy tadqiqotlarning muhim yo‘nalishlaridan biriga aylandi. Ilmiy adabiyotlarda AI asosidagi o‘qitish tizimlari adaptiv ta’lim, o‘quv jarayonini shaxsiylashtirish va ta’lim natijalarini tahlil qilishda samarali vosita sifatida baholanadi. Shu bilan birga, mazkur tizimlar bilan bog‘liq axborot xavfsizligi masalalari alohida ilmiy e’tibor talab etuvchi muammo sifatida ko‘rib chiqilmoqda.

Xorijiy tadqiqotlarda raqamli ta’lim platformalarida axborot xavfsizligini ta’minlash masalasi, avvalo, ma’lumotlarning maxfiyligi, yaxlitligi va mavjudligini kafolatlash tamoyillari asosida tahlil qilinadi. Tadqiqotchilar AI asosidagi tizimlarda katta hajmdagi shaxsiy va akademik ma’lumotlar to‘planishi ularni noqonuniy foydalanish, ma’lumotlar sizib chiqishi va kiberhujumlar xavfiga nisbatan yanada zaif holatga keltirishini ta’kidlaydilar. Shu bois, axborot xavfsizligini ta’minlash masalasi texnik himoya

choralaridan tashqari, tashkiliy va huquqiy mexanizmlarni ham qamrab olishi zarurligi qayd etiladi. Sun'iy intellektga oid ilmiy manbalarda algoritmik shaffoflik va ma'lumotlardan foydalanishning etik jihatlari muhim masala sifatida ko'tariladi. Tadqiqotchilar AI algoritmlarining "qora quti" xususiyati ta'lim jarayonida qarorlar qabul qilishda ishonchlilik va adolatlilik masalalarini keltirib chiqarishini ko'rsatadilar. Bu holat axborot xavfsizligini faqat texnik himoya doirasida emas, balki axborotdan mas'uliyatli foydalanish va algoritmik nazorat kontekstida ko'rib chiqish zaruratini yuzaga keltiradi.

Pedagogik adabiyotlarda raqamli ta'lim muhitida axborot xavfsizligi o'quvchilarning raqamli madaniyati va axborot savodxonligi bilan uzviy bog'liq holda tahlil qilinadi. Olimlar fikricha, AI asosidagi o'qitish tizimlaridan samarali va xavfsiz foydalanish faqatgina texnologik vositalar bilan cheklanmay, balki o'qituvchi va o'quvchilarda axborot xavfsizligi bo'yicha bilim va ko'nikmalarni shakllantirishni ham talab etadi. Shu nuqtai nazardan, axborot xavfsizligi ta'lim jarayonining ajralmas pedagogik komponenti sifatida talqin etiladi. Mahalliy ilmiy manbalarda raqamli ta'lim va axborot xavfsizligi masalalari asosan elektron ta'lim platformalarini himoyalash, shaxsiy ma'lumotlarni saqlash va normativ-huquqiy asoslarni takomillashtirish bilan bog'liq holda yoritilgan. Biroq AI asosidagi o'qitish tizimlarining axborot xavfsizligini pedagogik, texnik va etik jihatlarni integratsiyalashgan holda o'rganishga bag'ishlangan tadqiqotlar yetarli darajada emasligi kuzatiladi. Tahlil qilingan adabiyotlar shuni ko'rsatadiki, raqamli ta'lim muhitida AI asosidagi o'qitish tizimlarining axborot xavfsizligini ta'minlash masalasi ko'p qirrali bo'lib, u texnologik himoya, normativ-huquqiy tartibga solish va pedagogik yondashuvlarning uyg'unligini talab etadi. Aynan ushbu jihatlar mazkur tadqiqotning dolzarbligini belgilab, AI asosidagi o'qitish tizimlarida axborot xavfsizligini ta'minlashning kompleks modelini ishlab chiqish zaruratini yuzaga keltiradi.

Tadqiqot metodologiyasi. Mazkur tadqiqotda riskga asoslangan axborot xavfsizligi tahlili (Risk-Based Security Analysis) metodi qo'llanildi. Ushbu metod raqamli ta'lim muhitida AI asosidagi o'qitish tizimlarida mavjud axborot xavfsizligi xavf-xatarlarini aniqlash, baholash va ustuvorlashtirishga qaratilgan. Metod doirasida shaxsiy ma'lumotlar bilan ishlash, algoritmik qarorlar qabul qilish va ma'lumotlarni saqlash jarayonlarida yuzaga kelishi mumkin bo'lgan xavflar tizimli ravishda tahlil qilindi. Riskga asoslangan tahlil jarayonida axborot xavfsizligining asosiy komponentlari — maxfiylik, yaxlitlik va mavjudlik (CIA triadasi) mezon sifatida olindi. Aniqlangan xavf-xatarlar ehtimollik va ta'sir darajasiga ko'ra baholanib, AI asosidagi o'qitish tizimlarida axborot xavfsizligini ta'minlash bo'yicha ustuvor texnik va tashkiliy choralar belgilandi. Mazkur metod tadqiqotning ilmiy asoslanganligini ta'minlab, AI asosidagi ta'lim tizimlarida axborot xavfsizligini kompleks baholash imkonini berdi.

Tahlillar va natijalar. Tadqiqot doirasida raqamli ta'lim muhitida AI asosidagi o'qitish tizimlarining axborot xavfsizligi holati Cyber University talabalari misolida tahlil qilindi. Tadqiqotda 63 nafar talaba ishtirok etdi. Tahlil jarayoni riskga asoslangan axborot

xavfsizligi tahlili metodi asosida olib borildi hamda AI texnologiyalaridan foydalaniladigan ta’lim tizimlarida mavjud xavf-xatarlar aniqlash va baholashga yo‘naltirildi. Tahlil davomida axborot xavfsizligining asosiy komponentlari — maxfiylik, yaxlitlik va mavjudlik mezonlari asosida talabalar foydalanayotgan raqamli ta’lim platformalaridagi xavfsizlik holati o‘rganildi. Tadqiqot natijalari shuni ko‘rsatdiki, talabalar tomonidan sun’iy intellektga asoslangan o‘qitish tizimlaridan foydalanishda shaxsiy ma’lumotlarni himoyalashga oid bilimlar yetarli darajada shakllanmagan bo‘lib, bu holat axborot xavfsizligi bilan bog‘liq xavflarning ortishiga olib kelishi mumkin. Risklarni baholash natijasida aniqlanganki, yuqori darajadagi xavf-xatarlar asosan shaxsiy ma’lumotlarni qayta ishlash jarayonida, ma’lumotlardan uchinchi tomonlar tomonidan foydalanish ehtimoli hamda AI algoritmlarining shaffof emasligi bilan bog‘liqdir. O‘rtacha darajadagi xavflar foydalanuvchi autentifikatsiyasi, parollarni boshqarish va kirish huquqlarini nazorat qilish bilan bog‘liq bo‘lsa, past darajadagi xavflar asosan texnik infratuzilmaning barqaror ishlashi bilan izohlandi.

1) Umumiy risk darajasi bo‘yicha natijalar

1-jadval. Umumiy axborot xavfsizligi riski (n=63)

Risk darajasi	Talabalar soni	Ulushi (%)
Yuqori	24	38.1
O‘rtacha	27	42.9
Past	12	19.0
Jami	**63**	**100**

2) CIA triadasi bo‘yicha (maxfiylik–yaxlitlik–mavjudlik) risklar

2-jadval. CIA kesimida risk darajalari (n=63)

Ko‘rsatkich (CIA)	Yuqori (son / %)	O‘rtacha (son / %)	Past (son / %)
Maxfiylik (Confidentiality)	30 / 47.6	23 / 36.5	10 / 15.9
Yaxlitlik (Integrity)	18 / 28.6	29 / 46.0	16 / 25.4
Mavjudlik (Availability)	12 / 19.0	26 / 41.3	25 / 39.7

Tahlil natijalari shuni ko‘rsatadiki, AI asosidagi o‘qitish tizimlarida axborot xavfsizligini ta’minlash faqat texnik himoya choralarini joriy etish bilan cheklanmasligi lozim. Talabalarning axborot xavfsizligi bo‘yicha bilim va ko‘nikmalarini oshirish, ularni raqamli muhitda mas’uliyatli xatti-harakatlarga yo‘naltirish muhim ahamiyat kasb etadi. Shu bilan birga, AI algoritmlarining shaffofligini ta’minlash va ma’lumotlardan foydalanish jarayonini qat’iy nazorat qilish xavfsizlik darajasini oshirishga xizmat qiladi. Olingan natijalar asosida aytish mumkinki, Cyber University talabalari misolida olib borilgan tadqiqot raqamli ta’lim muhitida AI asosidagi o‘qitish tizimlarining axborot xavfsizligini ta’minlash masalasi kompleks yondashuvni talab etishini tasdiqlaydi. Ushbu

yondashuv texnologik, tashkiliy va pedagogik choralarni uyg‘unlashtirish orqali ta’lim jarayonining xavfsizligi va barqarorligini ta’minlash imkonini beradi.

Xulosa. O‘tkazilgan tadqiqot natijalari raqamli ta’lim muhitida AI asosidagi o‘qitish tizimlarining axborot xavfsizligini ta’minlash masalasi dolzarb va ko‘p qirrali muammo ekanligini ko‘rsatdi. **Cyber University** talabalari misolida 63 nafar ishtirokchi asosida amalga oshirilgan riskga asoslangan tahlil AI texnologiyalaridan foydalaniladigan ta’lim tizimlarida axborot xavfsizligiga oid xavf-xatarlar mavjudligini ilmiy jihatdan tasdiqladi. Statistik tahlil natijalariga ko‘ra, umumiy risk darajasida o‘rtacha va yuqori ko‘rsatkichlar ustun bo‘lib, bu holat AI asosidagi o‘qitish tizimlarida shaxsiy ma’lumotlarni himoyalash, foydalanuvchi autentifikatsiyasi hamda ma’lumotlardan foydalanish jarayonlarini kuchaytirishni talab etadi. Ayniqsa, CIA triadasi kesimida **maxfiylik** yo‘nalishida yuqori risk darajasining ustunligi aniqlanib, bu shaxsiy va akademik ma’lumotlar bilan ishlash jarayonida qo‘shimcha himoya mexanizmlarini joriy etish zarurligini ko‘rsatadi. Pedagogik nuqtai nazardan, axborot xavfsizligini ta’minlash nafaqat texnik vositalar bilan cheklanmasligi, balki talabalar va o‘qituvchilarda axborot xavfsizligi madaniyatini shakllantirish bilan ham uzviy bog‘liq ekanligi aniqlandi. AI asosidagi o‘qitish tizimlaridan xavfsiz foydalanish uchun raqamli savodxonlik, mas’uliyatli axborot muomalasi va algoritmik shaffoflikka oid bilimlarni ta’lim jarayoniga integratsiyalash muhim ahamiyat kasb etadi.

Xulosa qilib aytganda, raqamli ta’lim muhitida AI asosidagi o‘qitish tizimlarining axborot xavfsizligini ta’minlash kompleks yondashuvni talab etadi. Ushbu yondashuv texnologik himoya choralarini pedagogik va tashkiliy mexanizmlar bilan uyg‘unlashtirish orqali ta’lim jarayonining barqarorligi, ishonchliligi va samaradorligini oshirish imkonini beradi. Tadqiqot natijalari AI asosidagi ta’lim tizimlarini joriy etishda axborot xavfsizligini ta’minlashga qaratilgan ilmiy-amaliy tavsiyalar ishlab chiqish uchun muhim asos bo‘lib xizmat qiladi.

Foydalanilgan adabiyotlar ro‘yxati:

1. Russell S., Norvig P. Artificial Intelligence: A Modern Approach. – 4th ed. – Boston: Pearson, 2021. – 1136 p.
2. Floridi L. The Ethics of Artificial Intelligence for Education // *AI & Society*. – 2020. – Vol. 35, №3. – P. 617–628.
3. Holmes W., Bialik M., Fadel C. Artificial Intelligence in Education: Promises and Implications for Teaching and Learning. – Boston: Center for Curriculum Redesign, 2019. – 257 p.
4. OECD. Artificial Intelligence in Education: Challenges and Opportunities for Sustainable Development. – Paris: OECD Publishing, 2021. – 162 p.
5. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection – Information security management systems – Requirements. – Geneva: ISO, 2022.
6. NIST. AI Risk Management Framework (AI RMF 1.0). – Gaithersburg, MD: National Institute of Standards and Technology, 2023. – 56 p.
7. Zimnyaya I. A. Информационная безопасность личности в условиях цифрового общества. – Москва: Юрайт, 2019. – 192 с.

8. Khutorskoy A. V. Цифровая образовательная среда и проблемы безопасности данных // *Педагогика*. – 2020. – №7. – С. 32–38.
9. European Commission. Ethics Guidelines for Trustworthy AI. – Brussels: EC Publications, 2019. – 41 p.
10. Shmatko A. D. Кибербезопасность в цифровой образовательной среде. – Санкт-Петербург: Питер, 2020. – 224 с.