

**SUN’IY INTELLEKT TEXNOLOGIYALARINING OLIY TA’LIMDA
TALABALAR IJODKORLIGINI OSHIRISHDAGI O’RNI VA KIBERXAVFSIZLIK
MUAMMOLARI**

Ro‘ziboyeva Kamola Jaxongir qizi

*TATU, Kiberxavfsizlik fakulteti, Kiberxavfsizlik injiniringi yo‘nalishi 3-kurs talabasi
(733-24 guruh)*

Kalit so‘zlar: *sun’iy intellekt, AIED, generativ sun’iy intellekt, ChatGPT, ijodkorlik, oliy ta’lim, innovatsiyalar diffuziyasi nazariyasi, shaxsga doir ma’lumotlar, prompt injection, kiberxavfsizlik, pedagogik ma’lumotlarga egalik.*

Annotatsiya: *Mazkur maqolada sun’iy intellekt (SI) va ta’limda sun’iy intellekt (AIED – Artificial Intelligence in Education) texnologiyalarining oliy ta’limda, xususan STEM yo‘nalishlarida talabalar ijodkorligini oshirish maqsadida qo‘llanilishi hamda bu jarayonda yuzaga keladigan kiberxavfsizlik muammolari tahlil qilingan. Tahlil L. Tmanovanning Capella universitetida 2025-yilda himoya qilingan doktorlik dissertatsiyasi natijalariga asoslanadi. Unda axborot texnologiyalari, kompyuter fanlari, kiberxavfsizlik va bioinformatika sohalarida 5–30 yillik tajribaga ega professorlarning SI texnologiyalaridan foydalanish tajribasi o‘rganilgan. Maqolada tadqiqotda aniqlangan uchta asosiy mavzu – SI o‘qituvchining yordamchi texnologiyasi sifatida, SI yordamida kuchaytirilgan pedagogik ijodkorlik va “buzuvchi” ta’lim ekotizimi yoritib berilgan. Shuningdek, muallif tomonidan ushbu natijalar kiberxavfsizlik nuqtai nazaridan qayta ko‘rib chiqilib, ta’lim ma’lumotlari maxfiyligi, katta til modellariga qaratilgan hujumlar, intellektual mulk himoyasi va pedagogik ma’lumotlarga egalik masalalari bo‘yicha xavflar va himoya choralari taklif etilgan.*

XXI asrda mehnat bozori oliy ta’lim bitiruvchilaridan nafaqat chuqur nazariy bilim, balki ijodkorlik, tanqidiy fikrlash, hamkorlikda ishlash va murakkab muammolarni nostandart usulda hal qilish ko‘nikmalarini ham talab qilmoqda. Ayniqsa axborot texnologiyalari va kiberxavfsizlik sohasida bu talab yanada yuqori, chunki tajovuzkorlar doimo yangi hujum usullarini o‘ylab topadi, himoyachi mutaxassis esa ulardan bir qadam oldinda yurishi, ya’ni ijodiy fikrlashi lozim. Shu sababli zamonaviy universitetlar o‘quv jarayonini talabalarda ijodiy salohiyatni rivojlantirishga qaratishga intilmoqda.

2022-yil noyabr oyida OpenAI kompaniyasi tomonidan ChatGPT xizmatining ommaga taqdim etilishi oliy ta’lim tarixida burilish nuqtasi bo‘ldi. Qisqa vaqt ichida generativ sun’iy intellekt vositalari talabalar va o‘qituvchilarning kundalik faoliyatiga kirib keldi. Talabalar ulardan referat yozish, dastur kodini tuzish, masalalarni yechish uchun foydalana boshladi, o‘qituvchilar esa bu yangi voqelikka moslashishga, o‘quv topshiriqlari va baholash usullarini qayta ko‘rib chiqishga majbur bo‘ldi. L. Tmanovanning qayd etishicha, SI texnologiyalarining oliy ta’limga yetarli darajada tayyorgarliksiz va tartibga solinmagan holda joriy etilishi

pedagogikada paradigmal o‘zgarishni hamda bir qator axloqiy muammolarni yuzaga keltirdi [1].

Mavzuni to‘g‘ri tushunish uchun asosiy tushunchalarni aniqlashtirib olish zarur. Sun‘iy intellekt deganda odatda inson intellektiga xos bo‘lgan vazifalarni – o‘rganish, mulohaza yuritish, tilni tushunish, qaror qabul qilishni bajara oladigan kompyuter tizimlari tushuniladi [10]. Ta‘limda sun‘iy intellekt (AIED) esa SI usullarini o‘qitish va o‘rganish jarayoniga tatbiq etishga qaratilgan yo‘nalish bo‘lib, unga intellektual repetitor tizimlar, moslashuvchan (adaptiv) o‘qitish platformalari, o‘quv tahlili (learning analytics) vositalari, avtomatik baholash tizimlari kiradi. Generativ SI – katta til modellari (LLM) asosida yangi matn, rasm, kod yoki boshqa kontent yaratuvchi tizimlar bo‘lib, ChatGPT, Google Gemini, Microsoft Copilot kabi vositalar shular jumlasidandir.

Ijodkorlik tushunchasi ta‘lim kontekstida yangi, original va foydali g‘oyalarni yaratish hamda ularni amaliyotga tatbiq etish qobiliyati sifatida talqin qilinadi. STEM fanlarida ijodkorlik yangi algoritm ishlab chiqish, muammoni boshqacha nuqtai nazardan ko‘rish, mavjud yechimlarni yangi sharoitga moslashtirishda namoyon bo‘ladi. Kiberxavfsizlikda esa u tahdid modellarini tuzish, zaifliklarni izlash, noodatiy hujum ssenariylarini oldindan ko‘ra bilish ko‘rinishida aks etadi. Shu bois SI texnologiyalari talabalar ijodkorligiga qanday ta‘sir qilishi – uni rivojlantiradimi yoki aksincha susaytiradimi, degan savol dolzarb ilmiy muammo hisoblanadi.

Mazkur maqolaning maqsadi – L. Tmanova tadqiqoti natijalarini tahlil qilish orqali SI texnologiyalarining talabalar ijodkorligini oshirishdagi imkoniyatlari va xavflarini aniqlash hamda ularni kiberxavfsizlik mutaxassisi nuqtai nazaridan baholab, oliy ta‘lim muassasalari uchun amaliy tavsiyalar ishlab chiqishdan iborat.

Tahlil qilingan tadqiqotda umumiy sifat tadqiqoti (generic qualitative inquiry) dizayni qo‘llanilgan. Bu yondashuv ishtirokchilarning shaxsiy tajribasi, qarashlari va mulohazalarini chuqur o‘rganishga imkon beradi [3]. Ishtirokchilarni tanlash jarayonida 365 nafar ko‘ngilli ro‘yxatdan o‘tgan bo‘lsa-da, ulardan faqat 8 nafari qat‘iy mezonlarga javob bergan. Mezonlar quyidagilardan iborat bo‘lgan: AQSh kollej yoki universitetida professor unvoniga ega bo‘lish, kamida 5 yillik pedagogik tajriba hamda STEM bakalavriat dasturlarida talabalar ijodkorligini oshirish uchun SI va AIED texnologiyalaridan foydalanish. Ishtirokchilar haqidagi ma‘lumotlar 1-jadvalda keltirilgan.

1-jadval

Tadqiqot ishtirokchilari tavsifi

Ishtirokchi	Akademik unvon	Tajriba, yil	Fanlar / dasturlar
P1	Professor	25–30	Axborot texnologiyalari
P2	Dotsent (Associate Professor)	20–25	Bioinformatika, biostatistika
P3	Katta o‘qituvchi (Assistant Professor)	5–10	Ta‘lim dizayni va texnologiyalari
P4	Katta o‘qituvchi (Assistant Teaching Professor)	5–10	Axborot texnologiyalari

“O‘ZBEKISTONDA UCHINCHI RENESSANS VA INNOVATSION JARAYONLAR JURNALI”

20-Sentyabr, 2026-yil

P5	Dotsent	5–10	Kompyuter fanlari
P6	Dotsent	5–10	Kompyuter fanlari, bioinformatika
P7	Professor	20–25	Kompyuter fanlari, axborot texnologiyalari, kiberxavfsizlik
P8	O‘qituvchi professor (Teaching Professor)	15–20	Kompyuter fanlari, axborot texnologiyalari

Jadvaldan ko‘rinib turibdiki, ishtirokchilar tarkibi tajriba jihatidan muvozanatlashgan: to‘rt nafari nisbatan yosh (5–10 yil), qolganlari esa katta tajribaga ega (15–30 yil) mutaxassislaridir. Bundan tashqari, ular o‘yin dizayni va dasturlash, geografik axborot tizimlari, statistika, ilmiy tadqiqot usullari, “sun’iy intellekt va san’at” kabi turli kurslarni ham olib boradi. Bu esa natijalarning turli fan yo‘nalishlari tajribasini qamrab olishini ta’minlaydi.

Ma’lumotlar yarim tuzilmali intervyular orqali to‘plangan. Intervyular MS Teams platformasida yozib olinib, avtomatik transkripsiya qilingan, so‘ngra audio bilan solishtirilib tekshirilgan va har bir ishtirokchiga tasdiqlash uchun yuborilgan. Ma’lumotlarni tahlil qilishda induktiv tahlil usuli va NVivo 15 dasturidan foydalanilgan. Dasturning avtomatik kodlash funksiyasi 233 ta kod bergan bo‘lsa, tadqiqotchi matnlarni qayta-qayta o‘qish natijasida 29 ta asosiy kodni ishlab chiqqan. Keyingi bosqichda kodlar naqshlarga (pattern), naqshlar esa umumiy mavzularga birlashtirilgan. Ma’lumotlar to‘yinganlik darajasiga, ya’ni yangi g‘oyalar paydo bo‘lmay, javoblar takrorlana boshlagan bosqichga yetkazilgan [1; 4].

Tadqiqotning nazariy asosi sifatida E. Rogersning innovatsiyalar diffuziyasi nazariyasi (Diffusion of Innovation Theory, DIT) tanlangan [2]. Ushbu nazariyaga ko‘ra, yangi texnologiyaning jamiyatda tarqalish tezligi uning beshta xususiyatiga bog‘liq: nisbiy afzallik, mavjud qadriyat va tajribaga moslik, murakkablik, sinab ko‘rish imkoniyati va natijalarning ko‘zga ko‘rinishi. Shuningdek, nazariya innovatsiyani qabul qiluvchilarni beshta toifaga ajratadi: innovatorlar, erta qabul qiluvchilar, erta ko‘pchilik, kech ko‘pchilik va ortda qoluvchilar. Bu nazariya professorlarning SI texnologiyalarini qanday va nima sababdan qabul qilayotganini tushuntirishga xizmat qilgan.

Tadqiqot natijasida uchta asosiy mavzu aniqlangan. Birinchi mavzu – SI o‘qituvchining yordamchi texnologiyasi sifatida. Ishtirokchilar amaliyotida qo‘llanilayotgan vositalar juda xilma-xil ekani ma’lum bo‘ldi: ChatGPT, Google Gemini, Microsoft Copilot va Perplexity kabi generativ modellar; PyTorch va Python kutubxonalari asosidagi mashinali o‘qitish modullari; Autodesk Fusion 360 kabi bir nechta dizayn variantlarini avtomatik yaratuvchi generativ loyihalash dasturlari; virtual reallik va simulyatsiya vositalari. Shuningdek, Canvas va Moodle kabi o‘quv jarayonini boshqarish tizimlariga (LMS) o‘rnatilgan SI plaginlari, o‘quv tahlili va moslashuvchan o‘qitish modullaridan ham keng foydalanilgan [1].

Ushbu vositalar o‘qituvchi faoliyatining deyarli barcha bosqichlarida qo‘llanilgan: dars rejalashtirish, o‘quv resurslarini yaratish, topshiriqlar generatsiya qilish, baholash va talabalarga fikr-mulohaza berish, talabalar faolligi va o‘zlashtirishini kuzatish. Masalan, P8 ishtirokchi talabalarning baholari va faolligi bo‘yicha SI asosidagi tahlil vositalaridan

foydalanadi. U kurs chatboti talabalarining takroriy savollariga javob bergani sababli professorlarga keladigan elektron xatlar soni keskin kamayganini ta’kidlagan. P7 ishtirokchi esa Moodle tizimidagi SI plagini unga Canvas’dagi kabi talabalar faolligi va o’sishi haqida ma’lumot berishini aytgan [1].

Shu bilan birga, SI texnologiyalarini joriy etish tajribasi ishtirokchilar orasida bir xil emas. P2 o‘z tajribasini juda ijobiy deb baholab, hozircha bu vositani ta’limda qanday eng yaxshi qo‘llashni o‘rganishning boshlang‘ich bosqichidamiz, degan fikrni bildirgan. P3 esa joriy etish jarayoni muvaffaqiyatli kechmaganini aytgan. Asosiy to‘siqlar sifatida ChatGPT javoblarining sifatsizligi, SI vositalari kontekst va nozik jihatlarni tushunmasligi, ba’zan vazifani qo‘lda bajarish bilan barobar vaqt talab qilishi ko‘rsatilgan. P2 hatto ChatGPT yordamida o‘zi yozganchalik sifatli test savolini tuzish kutilmaganda qiyin bo‘lganini e’tirof etgan [1].

Ishtirokchilar SI bilan samarali ishlash uchun maxsus ko‘nikma – prompt muhandisligi, ya’ni modelga aniq va to‘g‘ri so‘rov berish mahorati zarurligini alohida ta’kidlagan. P2 ning fikricha, SIning foydaliligi u bilan muloqot qilishni o‘rgangan sari ortib boradi va bu ko‘nikma sinov va xatolar orqali shakllanadi. Professorlar SI ni joriy etishda turli strategiyalarni qo‘llagan: P1 promptlar va sinf muhokamalari orqali talabalarda tanqidiy fikrlashni rivojlantirgan; P2 onlayn darslarda “teskari sinf” (flipped classroom) modelida generativ SI dan foydalangan; boshqa bir ishtirokchi uni hisoblash tafakkurini (computational thinking) shakllantirishga yo‘naltirgan; P6 esa o‘zlashtirishda ortda qolayotgan talabalarga SI ni yordamchi sifatida qo‘llashni tavsiya qilgan [1].

Ikkinchi mavzu – SI yordamida kuchaytirilgan pedagogik ijodkorlik bo‘lib, u tadqiqotning eng muhim ilmiy yangiliklaridan biri hisoblanadi. Uning mohiyati shundaki, SI rutin vazifalarni o‘z zimmasiga olgani sababli o‘qituvchi bo‘shagan vaqtini ijodiy pedagogik izlanishlarga sarflaydi. P7 SI yordamida topshiriqlarni baholashga ketadigan vaqt sezilarli qisqarganini va baholash standartlashganini qayd etgan. P5 SI ni test savollari tuzishda, P3 esa baholash mezonlari (rubrikalar) ishlab chiqishda qo‘llagan. P1 ning ta’kidlashicha, SI oddiy vazifalarni bajarib berishi o‘qituvchiga yuqori darajadagi ta’limga e’tibor qaratish imkonini beradi [1].

Tadqiqotda o‘qituvchi va SI o‘rtasidagi hamkorlikning yangi shakllari aniqlangan. P2 SI bilan maslahatlashishni o‘ziga xos “virtual ustozlik”ka qiyoslab, u o‘zi mustaqil ravishda o‘ylab topa olmaydigan talabalarni jalb qilish usullarini taklif qilishini aytgan. P1 dars ishlanmasini tayyorlashda “yozuvchi to‘sig‘i”ga duch kelganda ChatGPT dan foydalanadi. P4 uchun SI keyinchalik mustaqil rivojlantirish mumkin bo‘lgan g‘oya “bo‘lagi”ni beradi. P5 esa SI chatbotini suhbat vositasi sifatida qo‘llab, talabalarga o‘qituvchidan tashqari boshqa suhbatdosh bilan muloqot qilish va masalaga turli nuqtai nazardan qarash imkonini yaratgan, chunki bitta o‘qituvchi barcha talabalarga bir vaqtda yetarli e’tibor bera olmaydi [1].

Talabalar ijodkorligiga ta’sir masalasida ham qiziqarli misollar keltirilgan. P1 o‘yin dizayni kursida talabalar SI yordamida ancha murakkab o‘quv faoliyatini mustaqil ishlab chiqqanini kuzatgan. P8 har safar ChatGPT orqali yangi topshiriq yaratadi, natijada talabalar doimo yangi vaziyatga duch keladi va muammolarni hal qilish ko‘nikmasi rivojlanadi. P3

SI ni aqliy hujum (brainstorming) mashg‘ulotlarida qo‘llagan va SIDan foydalanmaydigan o‘qituvchilar talabalarni zamonaviy mehnat bozoriga yetarli tayyorlamasligi mumkinligini ta’kidlagan [1].

Biroq bu borada qarama-qarshi qarashlar ham mavjud. P4 ko‘plab talabalar g‘oyalarni o‘zlari o‘ylab topish o‘rniga SIga tayanishini va bu ularning ijodkorligini susaytirishini kuzatgan. P6 esa ishni algoritmgga topshirib qo‘yish vasvasasi haqida ogohlantirgan. Shu sababli P1 talabalarda SIga nisbatan sog‘lom shubhani (AI skepticism) tarbiyalashni taklif qiladi: SI javoblarini tanqidiy tekshirish, xatolarini topish odatining o‘zi ijodkorlikni rivojlantiradi. P5 ning fikricha, talabalar SIDan to‘g‘ri foydalanishni bilsagina u ularning ijodkorligini oshiradi [1]. Demak, SIning ijobiy ta’siri uning o‘zidan emas, balki pedagogik yondashuvdan kelib chiqadi.

Uchinchi mavzu – “buzuvchi” ta’lim ekotizimi bo‘lib, u SI texnologiyalarining an’anaviy ta’lim muhitiga salbiy ta’sirlarini qamrab oladi. P7 SI ta’limdan inson omilini, ustoz va shogird o‘rtasidagi munosabatni chetga surib qo‘yishidan, shuningdek, tanqidiy va analitik fikrlash hamda ijtimoiy muloqot ko‘nikmalarini zaiflashtirishidan xavotir bildirgan. P5 o‘qituvchilarni SI bilan almashtirishni “halokatli xato” deb baholab, SI bu yechim emas, u har doim inson qo‘lida bo‘lishi kerak bo‘lgan vosita ekanini ta’kidlagan. P6 esa SI o‘qituvchi mehnatining katta qismini inson zarariga almashtirib yuborishi ehtimolini inkor etmagan [1].

Ishtirokchilar tomonidan qayd etilgan axloqiy va xavfsizlik muammolari ro‘yxati ancha keng: SIDan noaxloqiy foydalanish xavfi, shaxsiy ma’lumotlar maxfiyligi, algoritmik xolislik (bias), aholining turli qatlamlari o‘rtasidagi raqamli tengsizlik, akademik halollik va ko‘chirmachilik, modellarning noto‘g‘ri javob berishi, boshqa mualliflar uslubini taqlid qilish. P2 ChatGPTga mualliflik huquqi bilan himoyalangan materiallarni yuklash bilan bog‘liq huquqiy zaiflikni alohida ko‘rsatib o‘tgan. P5 esa SI modellari o‘tmish ma’lumotlari asosida ishlashini, shu sababli ularning natijalari axloqiy ekspertizadan o‘tkazilishi kerakligini ta’kidlagan [1].

Ushbu muammolarni kamaytirish uchun professorlar turli choralarni qo‘llagan: talabalarga SIDan foydalanish chegaralarini aniq belgilab berish, ayrim topshiriqlarda ChatGPTdan foydalanishga ochiq ruxsat berish, talabalarining SI bilan ishlashini nazorat ostida olib borish, generativ SI mavzusida alohida dars o‘tkazish. P1 esa SI ni hech qachon talabalar nimani bilishi kerakligi haqidagi o‘z tushunchasi o‘rniga qo‘ymasligini aytgan [1].

Mavzuning muhim jihatlaridan biri intellektual mulk va egalik masalasidir. P4 fikricha, o‘qituvchilar o‘quv materiallarini SI vositalari yordamida yaratsa, ularga bo‘lgan egalik huquqini yo‘qotishi mumkin. P5 bu holat individual va korporativ intellektual mulk tushunchasini jiddiy qayta ko‘rib chiqishga olib kelishini bashorat qilgan. P2 esa bilimga ochiq kirish tarafdori ekanini bildirgan. O‘qituvchining roli haqida ham fikrlar turlicha: P2 o‘qituvchi roli doimiy o‘zgarib, hatto chetga surilib borayotganini ta’kidlasa, P4 hozircha avtomatlashtirish faqat kichik vazifalar darajasida ekanini qayd etgan [1].

Natijalarni innovatsiyalar diffuziyasi nazariyasi nuqtai nazaridan talqin qilish quyidagi xulosalarga olib keladi. Birinchidan, ChatGPT oliy ta’limga dastlab talabalar, so‘ngra

hamkasb o‘qituvchilar orqali, ya’ni nazorat qilinmagan muhitda tarqalgan va aynan shu holat axloqiy muammolarni keltirib chiqargan. Bu Rogersning fikr yetakchilari innovatsiya tarqalishida hal qiluvchi rol o‘ynashi haqidagi xulosasini tasdiqlaydi [2]. Ikkinchidan, SIn faol qo‘llayotgan professorlar innovatorlar toifasiga, qolganlari esa erta qabul qiluvchilar va erta ko‘pchilik toifalariga mansub. Uchinchidan, SI texnologiyalarining qabul qilinishiga eng kuchli ta’sir ko‘rsatuvchi omillar nisbiy afzallik, sinab ko‘rish imkoniyati va murakkablik ekani aniqlangan [1].

Tmanova DIT nazariyasining murakkab va tarmoqli texnologiyalarni tushuntirishdagi cheklovlarini hisobga olib, uni uchta yangi kategoriya bilan kengaytirishni taklif qilgan. Dinamik o‘quv dasturi – SI texnologiyasini fan bo‘yicha ekspertlikni rivojlantirish maqsadlari bilan mazmunli va axloqiy uyg‘unlashtirish. Ta’limiy bog‘liqlik (educational connectivity) – o‘qitish jarayonida qo‘llaniladigan SI vositalari va ta’lim axloqi o‘rtasidagi muvozanat. Ta’limiy xabardorlik (educational cognizance) – ijodkorlikni oshirish uchun SIn tanlashda axloqiy me’yorlarga ongli ravishda amal qilish [1]. Bu kategoriyalar yangi texnologiyani joriy etishdan oldin uning oqibatlarini baholash va muammolarning oldini olish imkonini beradi.

Kiberxavfsizlik mutaxassisi nuqtai nazaridan qaraganda, ta’lim jarayoniga integratsiya qilingan har bir SI vositasi axborot tizimining bir qismi bo‘lib, u tashkilotning hujum yuzasini (attack surface) kengaytiradi. Tadqiqot ishtirokchilari tilga olgan maxfiylik, akademik halollik, intellektual mulk va manipulyatsiya bilan bog‘liq xavotirlar aslida axborot xavfsizligining klassik uchligi – konfidensiallik, yaxlitlik va foydalanuvchanlik (CIA triadasi) buzilishining turli ko‘rinishlaridir. Shu sababli SIn ta’limga joriy etish faqat pedagogik emas, balki axborot xavfsizligi masalasi sifatida ham ko‘rib chiqilishi lozim.

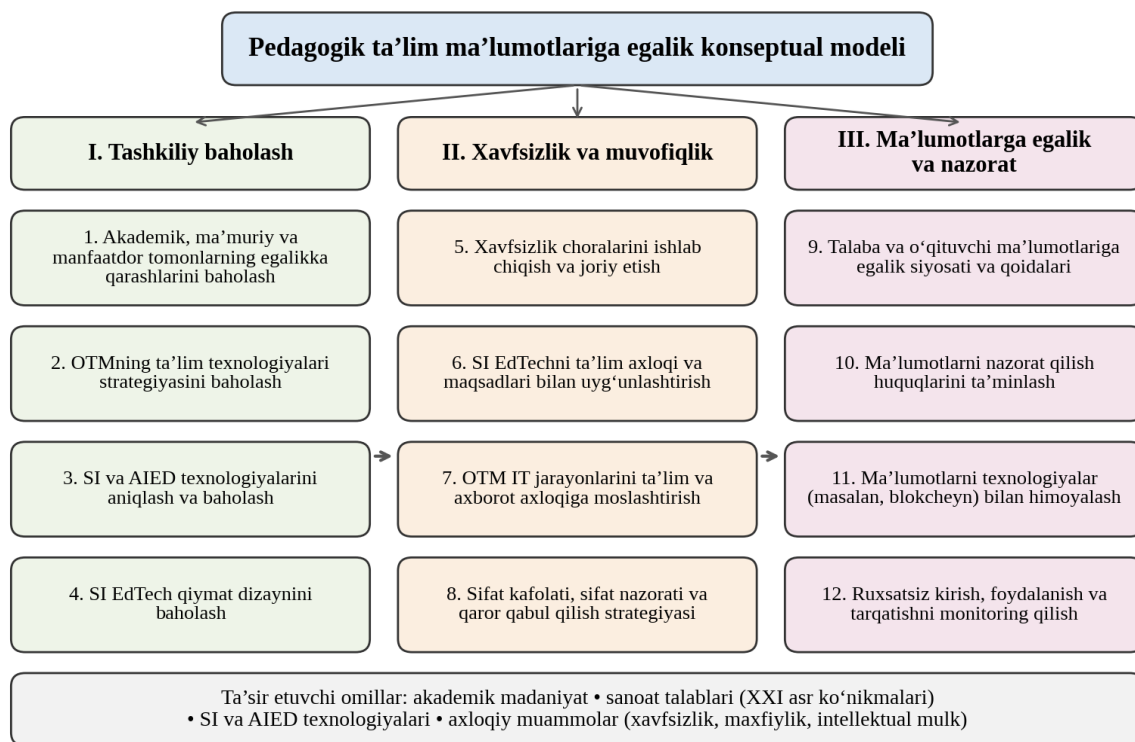
Birinchi va eng muhim xavf – ta’lim ma’lumotlarining maxfiyligi. LMS tizimlariga o‘rnatilgan SI plaginlari va o‘quv tahlili vositalari talabalarning baholari, topshiriqlari, faolligi, hatto xulq-atvor naqshlari haqidagi ma’lumotlarni qayta ishlaydi. Bu ma’lumotlar shaxsga doir ma’lumotlar hisoblanadi. Ko‘pincha ular tashqi SI xizmati provayderining xorijdagi serverlariga uzatiladi va provayder ularni o‘z modelini o‘qitish uchun ishlatishi ham mumkin. O‘zbekiston Respublikasining “Shaxsga doir ma’lumotlar to‘g‘risida”gi Qonuni shaxsga doir ma’lumotlarni qayta ishlashda subyektning roziligini olish, ularni himoya qilish choralari ko‘rishni talab qiladi, fuqarolarning shaxsga doir ma’lumotlarini mamlakat hududidagi ma’lumotlar bazalarida saqlash talabini ham belgilaydi [5]. Yevropa Ittifoqining GDPR reglamenti ham shunga o‘xshash qat’iy talablarni qo‘yadi [11]. Demak, OTM SI xizmatini tanlashda ma’lumotlar qayerda saqlanishi va qanday ishlatilishini aniq bilishi shart.

Ikkinchi xavf – katta til modellari qaratilgan maxsus hujumlar. Tadqiqot ishtirokchisi P4 SI chatbotlarini manipulyatsiya qilish juda osonligini va ular foydalanuvchini ko‘proq jalb qilishga mo‘ljallanganini ta’kidlagan [1]. Kiberxavfsizlik nuqtai nazaridan bu OWASP tashkilotining LLM ilovalari uchun eng xavfli 10 ta zaiflik ro‘yxatida birinchi o‘rinda turgan “prompt injection” hujumiga to‘g‘ri keladi [8]. Masalan, talaba kurs chatbotiga maxsus tuzilgan so‘rov yuborib, uning tizimli ko‘rsatmalarini chetlab o‘tishi, test javoblari yoki baholash mezonlarini oshkor qilishga majburlashi mumkin. Agar chatbot LMS ma’lumotlar bazasiga kirish huquqiga ega bo‘lsa, boshqa talabalarning shaxsiy ma’lumotlari yoki baholari

sizib chiqishi ehtimoli paydo bo‘ladi. Bundan tashqari, topshiriq fayliga yashirin ko‘rsatma joylashtirib, SI asosidagi avtomatik baholash tizimini aldash (bilvosita prompt injection) ham real tahdid hisoblanadi.

Uchinchi xavf – ma’lumotlar yaxlitligi va noto‘g‘ri axborot. Ishtirokchilar SI ko‘pincha noto‘g‘ri javob berishini asosiy muammo sifatida ko‘rsatgan [1]. Bu hodisa “gallyutsinatsiya” deb ataladi va OWASP ro‘yxatida ham alohida xavf sifatida qayd etilgan [8]. Agar o‘qituvchi SI yaratgan o‘quv materialini tekshirmasdan ishlatsa, talabalarga noto‘g‘ri bilim uzatiladi. Kiberxavfsizlik fanlarida bu yanada xavfli: noto‘g‘ri sozlangan xavfsizlik konfiguratsiyasi yoki zaif kod namunasi talabalar tomonidan kelajakda real tizimlarda qo‘llanilishi mumkin. Shuningdek, SI yordamida avtomatik baholashda modelning xatosi yoki manipulyatsiyasi baholar yaxlitligini buzadi.

To‘rtinchi xavf – intellektual mulk va ma’lumotlarga egalik. O‘qituvchi o‘z kursining materiallarini, test bazasini yoki ilmiy ishlanmalarini tashqi SI xizmatiga yuklaganda bu ma’lumotlar ustidan nazoratni qisman yo‘qotadi. Bu holat tashkilot uchun maxfiy ma’lumotlarning sizib chiqishi (data leakage) sifatida baholanadi. Tmanova aynan shu muammoga javob sifatida pedagogik ta’lim ma’lumotlariga egalik konseptual modelini taklif qilgan (1-rasm).



1-rasm. Pedagogik ta’lim ma’lumotlariga egalik konseptual modeli (L. Tmanova [1] asosida muallif tomonidan tuzilgan)

Ushbu model 12 bosqichdan iborat bo‘lib, ular mantiqan uch guruhga birlashadi. Birinchi guruh tashkiliy baholashni o‘z ichiga oladi: manfaatdor tomonlarning qarashlarini, OTMning texnologik strategiyasini va SI vositalarining qiymatini baholash. Ikkinchi guruh xavfsizlik va muvofiqlikka bag‘ishlangan: xavfsizlik choralarini ishlab chiqish, SI

“O‘ZBEKISTONDA UCHINCHI RENESSANS VA INNOVATSION JARAYONLAR JURNALI”

20-Sentyabr, 2026-yil

texnologiyalarini ta’lim va axborot axloqi bilan uyg‘unlashtirish, sifat nazorati. Uchinchi guruh esa bevosita ma’lumotlarga egalikni ta’minlashga qaratilgan: talaba va o‘qituvchi ma’lumotlariga egalik siyosatini belgilash, ularning o‘z ma’lumotlarini nazorat qilish huquqini ta’minlash, ma’lumotlarni blokcheyn kabi texnologiyalar bilan himoyalash va ruxsatsiz kirishni monitoring qilish [1]. Model OTM, talaba va o‘qituvchi ma’lumotlarini alohida ajratadi: o‘qituvchi ma’lumotlariga uning pedagogik bilimlari, ta’lim dizayni va o‘qitish usullari ham kiradi.

Kiberxavfsizlik nuqtai nazaridan bu model “ma’lumotlar boshqaruvi” (data governance) va “chuqurlashtirilgan himoya” (defense in depth) tamoyillariga to‘liq mos keladi. Uning 5-bosqichi amalda rollarga asoslangan kirishni boshqarish (RBAC), ma’lumotlarni saqlashda va uzatishda shifrlash, ko‘p faktorli autentifikatsiya kabi texnik choralarni anglatadi. 11-bosqichda tilga olingan blokcheyn texnologiyasi baholar, diplomlar va sertifikatlar yaxlitligini ta’minlashda, ularni soxtalashtirishning oldini olishda samarali qo‘llanilishi mumkin. 12-bosqich esa xavfsizlik hodisalarini jurnallashtirish, SIEM tizimlari orqali monitoring qilish va ma’lumotlar sizib chiqishining oldini olish (DLP) tizimlarini joriy etishni talab qiladi. Tahlil asosida ta’limda SIDan foydalanishdagi asosiy tahdidlar va ularga qarshi himoya choralari 2-jadvalda umumlashtirildi.

2-jadval

Ta’limda sun’iy intellektdan foydalanishdagi asosiy tahdidlar va himoya choralari

Tahdid	Ta’lim jarayonidagi ko‘rinishi	Himoya choralari
Shaxsga doir ma’lumotlar sizib chiqishi	Talabalar baholari va faolligi haqidagi ma’lumotlar tashqi SI xizmatiga uzatiladi	Ma’lumotlarni anonimlashtirish, shartnomada ma’lumotlardan foydalanish shartlarini belgilash, lokal modellardan foydalanish
Prompt injection	Talaba chatbotni aldab, test javoblari yoki tizim ko‘rsatmalarini oshkor qiladi	Kiruvchi so‘rovlarni filtrlash, chatbot huquqlarini minimal darajada cheklash, tizim ko‘rsatmalarini ma’lumotlardan ajratish
Gallyutsinatsiya va noto‘g‘ri axborot	SI yaratgan o‘quv materialida xato ma’lumot yoki zaif kod namunasi bo‘ladi	Inson tomonidan majburiy tekshiruv, manbalarni solishtirish, talabalarda tanqidiy yondashuvni shakllantirish
Baholash yaxlitligining buzilishi	Avtomatik baholash tizimi manipulyatsiya qilinadi yoki xato baho qo‘yadi	Yakuniy qarorni o‘qituvchi qabul qilishi, baholar jurnalini himoyalash, blokcheyn asosida qayd etish
Intellektual mulk yo‘qotilishi	O‘quv materiallari va ilmiy ishlanmalar tashqi xizmatga yuklanadi	Egalik siyosatini ishlab chiqish, maxfiy materiallarni yuklashni taqiqlash, DLP tizimlari
Akademik halollik buzilishi	Talaba topshiriqni to‘liq SI yordamida bajaradi	SIDan foydalanish qoidalarini aniq belgilash, og‘zaki himoya, jarayonga yo‘naltirilgan topshiriqlar

Jadvaldan ko‘rinib turibdiki, texnik choralarning o‘zi yetarli emas – ularni tashkiliy siyosat va pedagogik yondashuv bilan to‘ldirish zarur. Bu borada AQSh Milliy standartlar va texnologiyalar instituti (NIST) tomonidan ishlab chiqilgan SI xavflarini boshqarish tizimi (AI RMF 1.0) foydali asos bo‘lib xizmat qiladi. Unda SI xavflarini boshqarish to‘rtta funksiya – boshqaruv (Govern), xaritalash (Map), o‘lchash (Measure) va boshqarish (Manage) orqali amalga oshiriladi [7]. Tmanova modelining tashkiliy baholash bosqichlari xaritalash funksiyasiga, xavfsizlik va sifat nazorati bosqichlari o‘lchash va boshqarish funksiyalariga, egalik siyosati esa boshqaruv funksiyasiga mos keladi. YUNESKO ham ta’lim va tadqiqotda generativ SIDan foydalanish bo‘yicha tavsiyalarida ma’lumotlar maxfiyligini himoya qilish, foydalanuvchilar uchun yosh chegarasini belgilash va inson nazoratini saqlab qolishni asosiy talab sifatida ko‘rsatadi [9].

Mavzu kiberxavfsizlik yo‘nalishi talabalarini tayyorlash uchun alohida ahamiyatga ega. Bir tomondan, SI bu sohada o‘qitishni sezilarli boyitishi mumkin: har bir talaba uchun individual CTF (Capture The Flag) topshiriqlarini generatsiya qilish, jurnal fayllarini tahlil qilishni o‘rgatish, tahdid modellarini tuzishda aqliy hujum sherigi sifatida foydalanish, zararli kod namunalarini tushuntirish shular jumlasidandir. Tadqiqotdagi P8 tajribasi – har safar yangi topshiriq yaratish – kiberxavfsizlik laboratoriya mashg‘ulotlari uchun ayniqsa mos keladi, chunki bu talabalar tayyor yechimlarni bir-biridan ko‘chirishining oldini oladi. Ikkinchi tomondan, SI talabalarni tajovuzkorona vositalar yaratishga undashi yoki ular vazifani tushunmasdan tayyor kodni ishlatishiga sabab bo‘lishi mumkin. Shu sababli kiberxavfsizlik ta’limida SIDan faqat izolyatsiya qilingan laboratoriya muhitida, o‘qituvchi nazorati ostida va axloqiy xakerlik qoidalariga qat’iy rioya qilgan holda foydalanish tavsiya etiladi.

O‘zbekiston sharoitida ham sun’iy intellekt texnologiyalarini jadal joriy etish davlat siyosatining ustuvor yo‘nalishlaridan biri hisoblanadi. Bu borada “Raqamli O‘zbekiston – 2030” strategiyasi va sun’iy intellekt texnologiyalarini jadal joriy etish uchun shart-sharoitlar yaratishga oid Prezident qarori qabul qilingan [6; 12]. Tahlil natijalariga asoslanib, oliy ta’lim muassasalari uchun quyidagi tavsiyalarni ilgari surish mumkin: SIDan foydalanish bo‘yicha ichki nizom ishlab chiqish va unda talabalar hamda o‘qituvchilar uchun ruxsat etilgan va taqiqlangan holatlarni aniq belgilash; ta’limda qo‘llaniladigan SI xizmatlarini xavfsizlik va shaxsga doir ma’lumotlar qonunchiligiga muvofiqlik nuqtai nazaridan oldindan ekspertizadan o‘tkazish; imkon qadar mahalliy serverlarda joylashtirilgan ochiq manbali modellardan foydalanish; o‘qituvchilar uchun prompt muhandisligi va SI xavfsizligi bo‘yicha malaka oshirish kurslarini tashkil etish; talabalarga SI savodxonligi va uning cheklavlari haqida alohida mashg‘ulotlar o‘tkazish.

Shuni ham ta’kidlash kerakki, tahlil qilingan tadqiqot ayrim cheklavlarga ega. Namuna bor-yo‘g‘i 8 nafar AQSh professoridan iborat va faqat STEM yo‘nalishlarini qamrab oladi. Sifat tadqiqoti bo‘lgani sababli natijalar ishtirokchilarning subyektiv tajribasini aks ettiradi va ularni boshqa mamlakatlar, jumladan O‘zbekiston oliy ta’lim tizimiga to‘g‘ridan-to‘g‘ri ko‘chirib bo‘lmaydi. Tadqiqotchining o‘zi ham kelgusida ijtimoiy, gumanitar va san’at fanlari o‘qituvchilari tajribasini o‘rganishni tavsiya qilgan [1]. Bizning fikrimizcha, kelajakdagi

tadqiqotlarda ta’limda qo’llaniladigan SI tizimlarining xavfsizligini amaliy tekshirish, masalan, OTM chatbotlariga nisbatan prompt injection hujumlariga chidamlilik testlarini o’tkazish ham muhim yo’nalish bo’ladi.

Xulosa qilib aytganda, sun’iy intellekt texnologiyalari oliy ta’limda o’qituvchining kuchli yordamchisiga aylanmoqda. Ular baholash, dars rejalashtirish va topshiriqlar tuzish kabi rutin vazifalarni yengillashtirib, o’qituvchiga ijodiy pedagogik izlanishlar uchun vaqt ajratish imkonini beradi, o’qituvchi va SI hamkorligi esa yangi o’qitish usullarining paydo bo’lishiga olib keladi. Shu bilan birga, SIga haddan tashqari tayanish talabalarning mustaqil fikrlashi va ijodkorligini susaytirishi, ta’limdagi inson muloqotini kamaytirishi mumkin. Kiberxavfsizlik nuqtai nazaridan esa SI tizimlari yangi tahdidlar manbai bo’lib, ular ta’lim ma’lumotlari maxfiyligi, baholash yaxlitligi va intellektual mulk himoyasiga tahdid soladi.

XULOSA

Tadqiqot natijalari shuni ko’rsatdiki, sun’iy intellekt va AIED texnologiyalari oliy ta’limda talabalar ijodkorligini oshirishda katta salohiyatga ega, biroq bu salohiyat faqat to’g’ri pedagogik yondashuv va ishonchli axborot xavfsizligi choralari mavjud bo’lgandagina ro’yobga chiqadi. L. Tmanova tadqiqotida aniqlangan uchta mavzu – SI o’qituvchining yordamchisi sifatida, SI yordamida kuchaytirilgan pedagogik ijodkorlik va buzuvchi ta’lim ekotizimi – SIning ta’limga ta’siri bir tomonlama emasligini yaqqol ko’rsatadi. Innovatsiyalar diffuziyasi nazariyasini dinamik o’quv dasturi, ta’limiy bog’liqlik va ta’limiy xabardorlik kategoriyalari bilan kengaytirish hamda pedagogik ma’lumotlarga egalik modeli SIni ongli va xavfsiz joriy etish uchun muhim nazariy asos yaratadi. Kiberxavfsizlik nuqtai nazaridan tahlil ta’limda SIDan foydalanishning asosiy tahdidlari sifatida shaxsga doir ma’lumotlarning sizib chiqishi, prompt injection hujumlari, noto’g’ri axborot, baholash yaxlitligining buzilishi va intellektual mulk yo’qotilishini ko’rsatdi. Ularga qarshi texnik choralar (kirishni boshqarish, shifrlash, monitoring, blokcheyn), tashkiliy choralar (ichki nizom, xizmatlarni ekspertizadan o’tkazish, NIST AI RMF asosida xavflarni boshqarish) va pedagogik choralar (SI savodxonligi, sog’lom shubha, inson nazorati) kompleks tarzda qo’llanilishi lozim. Shu sababli sun’iy intellekt o’qituvchining o’rnini bosuvchi emas, balki inson nazorati ostida ishlaydigan, xavfsizligi ta’minlangan yordamchi vosita sifatida oliy ta’lim tizimiga joriy etilishi maqsadga muvofiqdir.

FOYDALANILGAN ADABIYOTLAR:

1. Tmanova L. Professors’ Use of Artificial Intelligence Technology for Student Creativity Enhancement: Doctoral dissertation. – Capella University, 2025. – 224 p.
2. Rogers E.M. Diffusion of Innovations. 5th Edition. – New York: Free Press, 2003.
3. Percy W.H., Kostere K., Kostere S. Generic qualitative research in psychology // The Qualitative Report. – 2015. – Vol. 20, No. 2. – P. 76–85.
4. Hennink M., Kaiser B.N. Sample sizes for saturation in qualitative research: A systematic review of empirical tests // Social Science & Medicine. – 2022. – Vol. 292. – 114523.

20-Sentyabr, 2026-yil

5. O‘zbekiston Respublikasining “Shaxsga doir ma’lumotlar to‘g‘risida”gi Qonuni. O‘RQ-547-son, 2019-yil 2-iyul.
6. O‘zbekiston Respublikasi Prezidentining “Sun’iy intellekt texnologiyalarini jadal joriy etish uchun shart-sharoitlar yaratish chora-tadbirlari to‘g‘risida”gi PQ-4996-son qarori. 2021-yil 17-fevral.
7. NIST. Artificial Intelligence Risk Management Framework (AI RMF 1.0). NIST AI 100-1. – National Institute of Standards and Technology, 2023.
8. OWASP. Top 10 for Large Language Model Applications. – OWASP Foundation, 2025.
9. UNESCO. Guidance for Generative AI in Education and Research. – Paris: UNESCO, 2023.
10. Russell S., Norvig P. Artificial Intelligence: A Modern Approach. 4th Edition. – Pearson, 2021.
11. Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation). – 2016.
12. O‘zbekiston Respublikasi Prezidentining “«Raqamli O‘zbekiston – 2030» strategiyasini tasdiqlash va uni samarali amalga oshirish chora-tadbirlari to‘g‘risida”gi PF-6079-son Farmoni. 2020-yil 5-oktabr.