Ishonchli foydalanuvchilar, zaif fuqarolar: O‘zbekiston universitet talabalari orasida raqamli kompetensiya va xavfsizlik tafovuti

Akshay Kumar
Muhammad al-Xorazmiy nomidagi TATU
AKTSI kafedrasi katta o‘qituvchisi

Annotatsiya. Maqolada O‘zbekiston universitet talabalari orasida raqamli kompetensiya va raqamli xavfsizlik madaniyati o‘rtasida yuzaga kelayotgan tafovut konseptual-tahliliy yondashuv asosida o‘rganiladi. Talabalar ijtimoiy tarmoqlar, elektron ta’lim platformalari, mobil ilovalar, bulutli xizmatlar va raqamli to‘lov tizimlaridan faol foydalanayotgan bo‘lsa-da, bu faollik har doim ham xavfsiz xulq-atvor bilan mustahkamlanmaydi. Shu sababli maqolaning asosiy g‘oyasi shundan iboratki, raqamli vositalardan erkin foydalanish, tezkor kontent yaratish yoki onlayn muloqot olib borish ko‘nikmasi avtomatik ravishda kiberxavfsizlik immunitetini anglatmaydi. Tadqiqotda “ishonchli foydalanuvchi” va “zaif fuqaro” tushunchalari orqali talabalarning texnik o‘ziga ishonchi bilan real himoyalanganlik darajasi o‘rtasidagi nomutanosiblik izohlanadi.

Kalit so‘zlar: raqamli kompetensiya, raqamli xavfsizlik, kiberxavfsizlik madaniyati, universitet talabalari, O‘zbekiston, raqamli savodxonlik, shaxsiy ma’lumotlar himoyasi.

Kirish

So‘nggi yillarda O‘zbekistonda raqamli iqtisodiyot, elektron davlat xizmatlari, oliy ta’limning raqamli transformatsiyasi va IT sohasiga yo‘naltirilgan ta’lim dasturlari tez sur’atlarda rivojlanmoqda. “Raqamli O‘zbekiston – 2030” strategiyasi doirasida davlat boshqaruvi, ta’lim, sog‘liqni saqlash va boshqa sohalarda zamonaviy axborot-kommunikatsiya texnologiyalarini keng joriy etish ustuvor vazifa sifatida belgilangan [1]. Bunday sharoitda universitet talabalari raqamli muhitning eng faol qatlamlaridan biriga aylanmoqda: ular masofaviy ta’lim platformalaridan foydalanadi, ilmiy axborot izlaydi, ijtimoiy tarmoqlarda shaxsiy brend yaratadi, onlayn to‘lovlar qiladi va sun’iy intellekt vositalaridan o‘quv jarayonida foydalanadi.

Biroq talabalarning raqamli faolligi ularning raqamli xavfsizligi bilan har doim ham mos kelmaydi. Amaliy kuzatuvlar shuni ko‘rsatadiki, ko‘pchilik yoshlar yangi ilovalarni tez o‘zlashtiradi, murakkab interfeyslardan qo‘rqmaydi, bir vaqtning o‘zida bir nechta platformada ishlay oladi, lekin parol gigiyenasi, ikki bosqichli autentifikatsiya, fishing xabarlarini tanish, shaxsiy ma’lumotlarni himoya qilish, soxta havolalarni tekshirish va raqamli izlarni boshqarish bo‘yicha yetarli ehtiyotkorlikka ega emas. Shu jihatdan maqolaning dolzarbligi texnik kompetensiya va xavfsiz fuqarolik madaniyati o‘rtasidagi tafovutni aniqlash zarurati bilan belgilanadi.

Mazkur maqolaning maqsadi O‘zbekiston universitet talabalari misolida raqamli kompetensiya va xavfsizlik tafovuti tushunchasini ilmiy jihatdan izohlash, uning asosiy sabablari va oqibatlarini tahlil qilish hamda oliy ta’lim tizimida raqamli xavfsizlik madaniyatini kuchaytirishga qaratilgan takliflarni ishlab chiqishdan iborat. Tadqiqot savoli quyidagicha qo‘yiladi: nima uchun raqamli vositalardan faol foydalanuvchi talaba real kiberxavflar oldida zaif fuqaro bo‘lib qolmoqda?

Metodologiya

Maqola konseptual-tahliliy tadqiqot sifatida bajarildi. Unda ikkilamchi manbalar tahlili, siyosiy-huquqiy hujjatlar sharhi, xalqaro tashkilotlar materiallari va oliy ta’lim muhitida kuzatiladigan raqamli xatti-harakatlarni mantiqiy modellashtirish usullaridan foydalanildi. Empirik so‘rovnoma natijalari keltirilmaydi; aksincha, mavjud hujjatlar va nazariy yondashuvlar asosida universitet talabalari uchun xos bo‘lgan xavfsizlik tafovuti modeli ishlab chiqiladi.

Tahlilda uchta mezon asos qilib olindi. Birinchi mezon – funksional raqamli kompetensiya, ya’ni talabaning qurilma, platforma, ilova va onlayn xizmatlardan foydalana olish darajasi. Ikkinchi mezon – himoyaviy raqamli kompetensiya, ya’ni shaxsiy ma’lumot, akkaunt, moliyaviy operatsiya va

kommunikatsiya xavfsizligini ta’minlashga oid bilim va odatlar. Uchinchi mezon – fuqarolik mas’uliyati, ya’ni raqamli muhitda axloqiy, huquqiy va ijtimoiy javobgarlik bilan harakat qilish qobiliyati. Ushbu mezonlar o‘zaro solishtirilib, “raqamli kompetensiya yuqori, xavfsizlik madaniyati past” bo‘lgan holatlar xavfsizlik tafovuti sifatida talqin qilindi.

Natijalar

Tahlil shuni ko‘rsatadiki, universitet talabalari orasidagi raqamli xavfsizlik tafovuti, avvalo, kompetensiyaning noto‘g‘ri talqin qilinishi bilan bog‘liq. Ko‘p hollarda raqamli kompetensiya deganda texnik foydalanish tezligi tushuniladi: talaba platformaga kira olsa, fayl yuklay olsa, video montaj qila olsa yoki sun’iy intellektdan matn oldira olsa, u “raqamli savodli” deb baholanadi. Ammo xavfsizlik nuqtayi nazaridan bunday yondashuv yetarli emas. Chunki raqamli savodxonlik faqat texnik amaliyot emas, balki xavfni oldindan ko‘ra bilish, ma’lumot manbasini tekshirish, shaxsiy chegaralarni himoya qilish va zararli manipulyatsiyani aniqlash qobiliyatini ham o‘z ichiga oladi.

Ikkinchi muhim natija – talabalarda o‘ziga ortiqcha ishonch fenomeni mavjudligidir. Raqamli muhitda doimiy bo‘lish ularda “men buni bilaman” degan psixologik tasavvurni shakllantiradi. Natijada ular noma’lum havolaga bosish, bir xil paroldan turli platformalarda foydalanish, shaxsiy surat va hujjatlarni ochiq saqlash, umumiy Wi-Fi tarmoqlarida akkauntlarga kirish, tasdiqlanmagan ilovalarni o‘rnatish kabi xatti-harakatlarning oqibatini yetarli baholamaydi. UNODC materiallarida ham raqamli transformatsiya jadallashayotgan sharoitda yoshlar uchun kiberxavfsizlik tahdidlari va raqamli zo‘ravonlik muhim muammo sifatida qayd etilgan [2].

Uchinchi natija shundan iboratki, xavfsizlik tafovuti faqat individual bilim yetishmasligi emas, balki institutsional muhit masalasidir. Agar universitetlarda raqamli xavfsizlik alohida fan yoki amaliy modul sifatida muntazam o‘qitilmasa, talabalar xavfsizlikni shaxsiy mas’uliyat emas, balki texnik mutaxassislar vazifasi deb qabul qiladi. ITU tomonidan O‘zbekistonda bolalar va yoshlarning raqamli savodxonligi hamda onlayn xavfsizligini kuchaytirishga qaratilgan treninglar o‘tkazilgani bu yo‘nalishda tizimli ta’limning ahamiyatini ko‘rsatadi [3]. Demak, oliy ta’lim muassasalari talabalarga nafaqat raqamli vositadan foydalanishni, balki raqamli muhitda himoyalangan, mas’uliyatli va tanqidiy fikrlovchi fuqaro bo‘lishni ham o‘rgatishi kerak.

Quyidagi model tahlil natijalarini umumlashtiradi:

Ko‘rsatkich	Kuchli tomoni	Zaif tomoni
Funksional kompetensiya	Platforma, ilova va qurilmalardan tez foydalanish	Xavfsizlik sozlamalariga befarqlik
Axborot bilan ishlash	Kontent izlash va tarqatish faolligi	Manba va havolani tanqidiy tekshirmaslik
Shaxsiy ma’lumotlar	Onlayn xizmatlardan keng foydalanish	Parol, akkaunt va maxfiylik gigiyenasining sustligi

Munozara

O‘zbekiston sharoitida ushbu muammo kengroq raqamli rivojlanish jarayoni bilan bog‘liq. Bir tomondan, raqamli infratuzilma kengaymoqda, IT ta’lim markazlari soni ortmoqda, elektron xizmatlar ko‘lami kengaymoqda va yoshlarning raqamli iqtisodiyotdagi ishtiroki kuchaymoqda [1]. Boshqa tomondan, UNDPning O‘zbekiston raqamli iqtisodiyotiga oid hisobotida raqamli savodxonlikdagi tafovutlar va malaka yetishmovchiligi inklyuziv raqamli o‘sish uchun muhim cheklovlardan biri sifatida ko‘rsatiladi [4]. Demak, raqamli kompetensiyani faqat “qurilmadan foydalana olish” bilan emas, balki xavfsiz foydalanish va mas’uliyatli fuqarolik ko‘nikmalari bilan birga baholash zarur.

Talabalar orasida xavfsizlik tafovutini kamaytirish uchun oliy ta’lim muassasalarida uch bosqichli yondashuv maqsadga muvofiq. Birinchi bosqichda barcha ta’lim yo‘nalishlari uchun “raqamli gigiyena” bo‘yicha qisqa majburiy modul joriy etilishi kerak. Bu modul parol siyosati, fishing, ikki bosqichli autentifikatsiya, ijtimoiy tarmoqlarda maxfiylik, shaxsiy ma’lumotlar va akademik halollik masalalarini qamrab oladi. Ikkinchi bosqichda fanlararo integratsiya zarur: iqtisodiyot, pedagogika, jurnalistika, tibbiyot, muhandislik yoki huquq yo‘nalishida tahsil olayotgan talaba o‘z kasbiy sohasiga

xos raqamli xavflarni tushunishi kerak. Uchinchi bosqichda universitetlarda real holatlarga asoslangan simulyatsiya, keys va mikrotreninglar yo‘lga qo‘yilishi lozim. Chunki xavfsizlik madaniyati faqat ma’ruza bilan emas, balki takroriy amaliy mashqlar orqali shakllanadi.

Shuningdek, raqamli xavfsizlik masalasini faqat texnik muammo sifatida emas, balki fuqarolik madaniyati masalasi sifatida talqin qilish muhim. Talaba nafaqat o‘z akkauntini himoya qilishi, balki boshqalarning shaxsiy ma’lumotiga hurmat bilan qarashi, yolg‘on axborotni tarqatmasligi, raqamli zo‘ravonlikka befarq bo‘lmasligi va onlayn muloqotda huquqiy-axloqiy chegaralarni bilishi kerak. O‘zbekistonning kiberxavfsizlik sohasidagi huquqiy bazasi va 2026-yilda qabul qilingan kiberxavfsizlik strategiyasi ham bu masalaning davlat siyosati darajasida ahamiyatli ekanini ko‘rsatadi [1].

Amaliy tavsiyalar

Universitetlar uchun birinchi amaliy tavsiya – raqamli xavfsizlikni barcha yo‘nalishlar kesimida umumkasbiy kompetensiya sifatida belgilashdir. Bugungi sharoitda kiberxavfsizlik faqat axborot texnologiyalari fakulteti talabalariga tegishli bilim emas. Iqtisodchi onlayn to‘lov va mijoz ma’lumotlari bilan, jurnalist axborot manbasi va raqamli obro‘ bilan, pedagog o‘quvchi ma’lumotlari va elektron platformalar bilan, tibbiyot yo‘nalishidagi talaba esa shaxsiy tibbiy ma’lumotlar maxfiyligi bilan ishlaydi. Shuning uchun raqamli xavfsizlik moduli barcha ta’lim yo‘nalishlarida kasbiy etikaga bog‘langan holda berilishi maqsadga muvofiq.

Ikkinchi tavsiya – nazariy ogohlantirishdan amaliy mashq modeliga o‘tishdir. Talabalarga “fishingdan ehtiyot bo‘ling” deyishning o‘zi yetarli emas; ular soxta xat, qalbaki havola, klonlangan sayt, ijtimoiy muhandislik savoli, QR-kod orqali tuzoq, bepul Wi-Fi xavfi yoki sun’iy intellekt yordamida yaratilgan yolg‘on kontentni amaliy vaziyatda ajrata olishi kerak. Buning uchun universitet axborot-resurs markazlari, tyutorlar, professor-o‘qituvchilar va IT bo‘limlari hamkorligida qisqa, ammo muntazam mikrotreninglar tashkil etilishi mumkin. Har semestr boshida 20–30 daqiqalik raqamli gigiyena mashg‘uloti ham talabaning kundalik xatti-harakatiga sezilarli ta’sir ko‘rsatadi.

Uchinchi tavsiya – xavfsizlik madaniyatini baholash indikatorlarini joriy etishdir. Talabaning raqamli kompetensiyasini faqat elektron platformadan foydalanish yoki topshiriqni onlayn yuborish bilan o‘lchash yetarli emas. Baholash mezonlariga parol xavfsizligi, ma’lumot manbasini tekshirish, havola ishonchliligini aniqlash, shaxsiy ma’lumotni oshkor qilmaslik, ijtimoiy tarmoqlarda axloqiy muloqot yuritish va raqamli huquqlarni bilish kabi ko‘rsatkichlar ham kiritilishi lozim. Bunday yondashuv raqamli kompetensiyani texnik ko‘nikmadan fuqarolik mas’uliyatiga olib chiqadi.

To‘rtinchi tavsiya – universitetlarda raqamli xavfsizlik bo‘yicha ichki kommunikatsiyani kuchaytirishdir. Talaba ko‘pincha xavfga uchraganidan keyin kimga murojaat qilishni bilmaydi. Shu sababli har bir oliy ta’lim muassasasida qisqa yo‘riqnoma, ishonchli aloqa kanali, favqulodda holatlarda murojaat qilish tartibi va profilaktik eslatmalar bo‘lishi zarur. Raqamli xavfsizlik madaniyati shaxsiy ehtiyotkorlik, institutsional yordam va huquqiy ong birlashgan taqdirdagina barqaror shakllanadi.

Tadqiqot cheklovlari va kelgusi yo‘nalishlar

Mazkur maqola konseptual-tahliliy xarakterga ega bo‘lgani sababli unda talabalar o‘rtasida o‘tkazilgan maxsus so‘rovnoma yoki statistik eksperiment natijalari da’vo qilinmaydi. Bu yondashuv maqolaning ilmiy halolligini saqlaydi: unda mavjud siyosiy-huquqiy hujjatlar, xalqaro tashkilotlar materiallari va oliy ta’lim muhitiga xos raqamli xatti-harakatlar asosida muammo modeli ishlab chiqildi. Shuning uchun keltirilgan xulosalar keyingi empirik tadqiqotlar uchun nazariy asos va metodologik yo‘nalish sifatida qabul qilinishi mumkin.

Kelgusi tadqiqotlarda O‘zbekistonning turli hududlaridagi universitetlar, ta’lim yo‘nalishlari va kurslar kesimida talabalarning raqamli xavfsizlik darajasini anketa, fokus-guruh va amaliy testlar orqali o‘lchash maqsadga muvofiq. Ayniqsa, talabalar o‘zini qanchalik “raqamli bilimdon” deb baholashi bilan real xavfsizlik amaliyoti o‘rtasidagi farqni aniqlash muhim. Bunday empirik tahlil oliy ta’lim muassasalari uchun aniq o‘quv modullari, profilaktik kampaniyalar va xavfsizlik indikatorlarini ishlab chiqishga xizmat qiladi.

Xulosa

Maqola natijalari shuni ko‘rsatadiki, O‘zbekiston universitet talabalari orasida raqamli kompetensiya va raqamli xavfsizlik madaniyati o‘rtasida sezilarli tafovut shakllanishi mumkin. Talabalar raqamli vositalardan faol foydalanishi, turli platformalarda tez harakat qilishi va onlayn muhitda o‘zini ishonchli his qilishi ularning kiberxavflardan yetarli himoyalanganligini anglatmaydi. Aksincha, ortiqcha ishonch, xavfni past baholash, shaxsiy ma’lumotlar himoyasiga befarqlik va institutsional o‘quv mexanizmlarining yetarli emasligi ularni zaif raqamli fuqaroga aylantiradi.

Xavfsizlik tafovutini kamaytirish uchun oliy ta’lim tizimida raqamli kompetensiya tushunchasini qayta ko‘rib chiqish, uni himoyaviy ko‘nikmalar, tanqidiy fikrlash va raqamli fuqarolik mas’uliyati bilan boyitish zarur. Universitetlarda majburiy raqamli gigiyena modullari, sohaviy kiberxavfsizlik keyslar, simulyatsion mashg‘ulotlar va muntazam profilaktik treninglar joriy etilsa, talabalar nafaqat ishonchli foydalanuvchi, balki himoyalangan va mas’uliyatli raqamli fuqaro sifatida shakllanadi.

Foydalanilgan adabiyotlar

1. Government portal of the Republic of Uzbekistan. Digital technologies and Transport: “Digital Uzbekistan – 2030” Strategy, cybersecurity legislation and digital development indicators. 2026.
2. UNODC Regional Office for Central Asia. Empowering the Digital Generation: Youth-Led Policy on Cyber Safety in Uzbekistan. 2025.
3. International Telecommunication Union. Implementing Child Online Protection in Uzbekistan. 2023.
4. UNDP Uzbekistan. Digital Economy of Uzbekistan: The State of Digital Entrepreneurship and Artificial Intelligence. 2025.
5. UNESCO. ICT skills development in the Republic of Uzbekistan. 2025.
6. Law of the Republic of Uzbekistan “On Personal Data”, No. ZRU-547, 2 July 2019; Law “On Cybersecurity” and related policy documents.