Qabul qilindi: 3-oktabr 2026-yil • Ma’qullandi: 8-oktabr 2026-yil • Nashr qilindi: 13-oktabr 2026-yil

Ta’lim muassasalarida kiberxavfsizlikni ta’minlash va shaxsiy ma’lumotlarni himoyalash muammolari

Qo‘qon davlat unversiteti Raqamli texnologiyalar va sun’iy intellekt kafedrasi o‘qituvchisi Pedagogika fanlari bo‘yicha falsafa doktori (PhD)

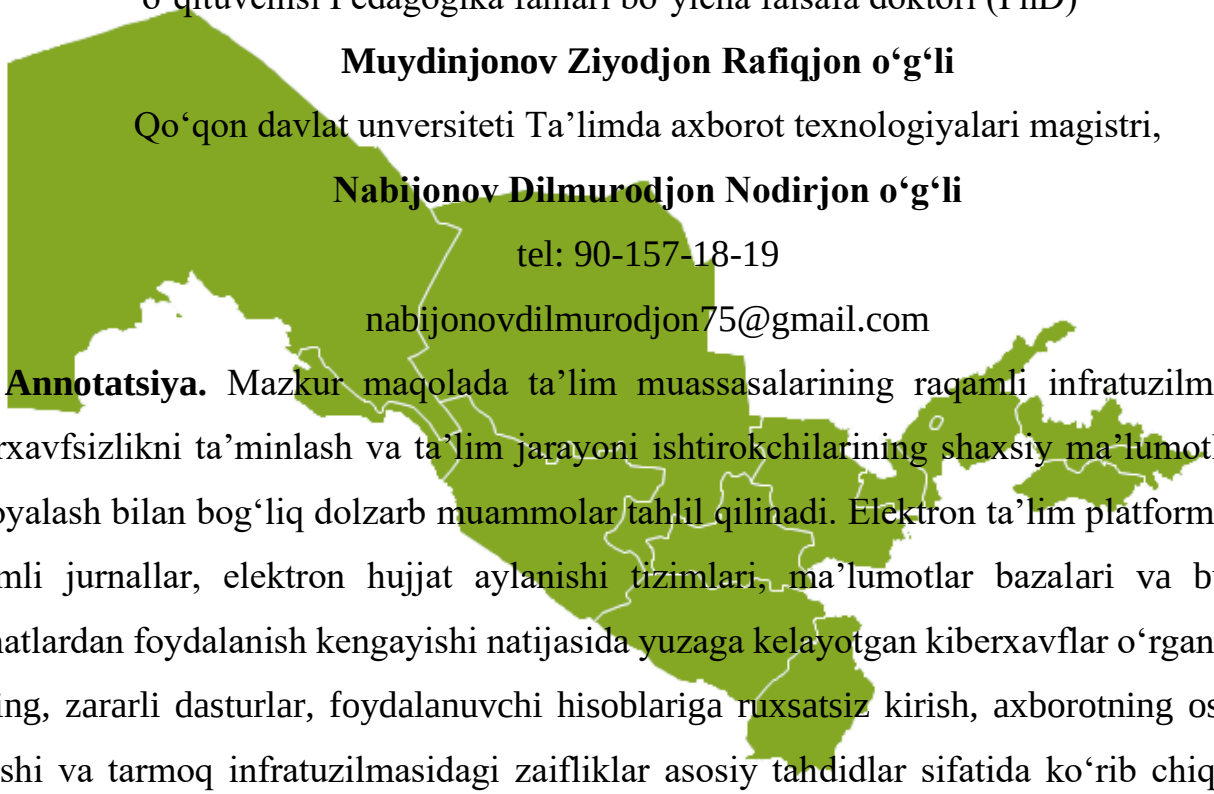
Muydinjonov Ziyodjon Rafiqjon o‘g‘li

Qo‘qon davlat unversiteti Ta’limda axborot texnologiyalari magistri,

Nabijonov Dilmurodjon Nodirjon o‘g‘li

tel: 90-157-18-19

nabijonovdilmurodjon75@gmail.com



Annotatsiya. Mazkur maqolada ta’lim muassasalarining raqamli infratuzilmasida kiberxavfsizlikni ta’minlash va ta’lim jarayoni ishtirokchilarining shaxsiy ma’lumotlarini himoyalash bilan bog‘liq dolzarb muammolar tahlil qilinadi. Elektron ta’lim platformalari, raqamli jurnallar, elektron hujjat aylanishi tizimlari, ma’lumotlar bazalari va bulutli xizmatlardan foydalanish kengayishi natijasida yuzaga kelayotgan kiberxavflar o‘rganiladi. Fishing, zararli dasturlar, foydalanuvchi hisoblariga ruxsatsiz kirish, axborotning oshkor bo‘lishi va tarmoq infratuzilmasidagi zaifliklar asosiy tahdidlar sifatida ko‘rib chiqiladi. Maqolada shaxsiy ma’lumotlarni himoyalashning texnik, tashkiliy va huquqiy mexanizmlari tizimlashtirilib, ta’lim muassasalarida kiberxavfsizlikni kompleks boshqarish bo‘yicha takliflar ishlab chiqiladi. Taklif etilayotgan yondashuv axborot aktivlarini aniqlash, xavflarni baholash, himoya vositalarini joriy etish, foydalanuvchilarni xabardor qilish va kiberhodisalardan keyin tizimlarni tiklash bosqichlarini qamrab oladi.

Kalit so‘zlar: kiberxavfsizlik, ta’lim muassasasi, shaxsiy ma’lumotlar, axborot xavfsizligi, raqamli infratuzilma, fishing, kiberhujum, autentifikatsiya, ma’lumotlarni shifrlash, bulutli texnologiyalar, axborot tizimlari.

Kirish

Axborot-kommunikatsiya texnologiyalarining rivojlanishi ta’lim tizimida axborotni yaratish, saqlash, qayta ishlash va uzatish jarayonlarini yangi bosqichga olib chiqdi. Bugungi kunda ta’lim muassasalarida elektron jurnal va kundaliklar, masofaviy ta’lim platformalari, elektron kutubxonalar, talabalar ma’lumotlar bazalari, videokonferensiya xizmatlari hamda elektron hujjat aylanishi tizimlaridan keng foydalanilmoqda. Mazkur texnologiyalar ta’lim xizmatlarining qulayligi va tezkorligini oshirish bilan birga, axborot xavfsizligini ta’minlashga doir yangi vazifalarni ham yuzaga keltirmoqda.

Ta’lim muassasalari o‘quvchilar, talabalar, pedagoglar, ma’muriy xodimlar va ularning qonuniy vakillariga tegishli turli ma’lumotlarni qayta ishlaydi. Ushbu ma’lumotlar tarkibiga shaxsni identifikatsiya qiluvchi axborotlar, aloqa ma’lumotlari, o‘zlashtirish ko‘rsatkichlari, davomat, xizmatga oid hujjatlar va boshqa ma’lumotlar kirishi mumkin. Ularning ruxsatsiz tarqalishi shaxsiy hayot daxlsizligiga zarar yetkazishi, firibgarlik xavfini kuchaytirishi hamda ta’lim muassasasining faoliyatiga salbiy ta’sir ko‘rsatishi ehtimolini oshiradi.

Kiberxavfsizlik masalasi faqat kompyuterlarni zararli dasturlardan himoyalash yoki tarmoqni tashqi hujumlardan saqlash bilan cheklanmaydi. U ma’lumotlardan qonuniy foydalanish, foydalanuvchilar vakolatlarini belgilash, axborot tizimlarining uzluksiz ishlashini ta’minlash, kiberhodisalarni aniqlash va ularning oqibatlarini bartaraf etish kabi ko‘plab vazifalarni qamrab oladi. Shu sababli ta’lim muassasalarida kiberxavfsizlikni kompleks boshqarish, shaxsiy ma’lumotlarni himoyalash mexanizmlarini takomillashtirish va foydalanuvchilarning xavfsiz raqamli xatti-harakatlarini shakllantirish muhim ilmiy-amaliy ahamiyatga ega.

Tadqiqotning maqsadi va metodlari

Maqolaning maqsadi ta’lim muassasalarida kiberxavfsizlikni ta’minlashga to‘sqinlik qilayotgan asosiy omillarni tahlil qilish, shaxsiy ma’lumotlarni himoyalashning texnik va tashkiliy vositalarini tizimlashtirish hamda raqamli infratuzilmaning xavfsizligini oshirish bo‘yicha amaliy tavsiyalar ishlab chiqishdan iborat.

Tadqiqotda ilmiy adabiyotlar va me’yoriy hujjatlarni tahlil qilish, taqqoslash,

tasniflash, tizimli yondashuv va umumlashtirish usullaridan foydalanildi. Kiberxavfsizlik bo‘yicha xalqaro tavsiyalar, jumladan, AQSh Milliy standartlar va texnologiyalar instituti tomonidan ishlab chiqilgan Cybersecurity Framework 2.0 doirasi, UNESCOning onlayn ta’limda shaxsiy ma’lumotlar maxfiyligini himoyalashga oid materiallari hamda O‘zbekiston Respublikasining tegishli qonunchiligi tahliliy asos sifatida qaraldi.

Tadqiqot doirasida kiberxavfsizlik tahdidlari texnik, tashkiliy va inson omili bilan bog‘liq guruhlarga ajratildi. Ushbu tasnif ta’lim muassasalarida xavfsizlikka ta’sir ko‘rsatuvchi omillarni o‘zaro bog‘liq holda ko‘rib chiqish va ularni kamaytirishga qaratilgan chora-tadbirlarni shakllantirish imkonini beradi.

Ta’lim muassasalarida kiberxavfsizlikning asosiy muammolari

Axborot xavfsizligining asosiy tamoyillari maxfiylik, yaxlitlik va mavjudlik tushunchalari bilan ifodalanadi. Maxfiylik axborotdan faqat tegishli huquqqa ega shaxslar foydalanishini, yaxlitlik ma’lumotlarning ruxsatsiz o‘zgartirilmasligini, mavjudlik esa zarur vaqtda axborot tizimlaridan foydalanish imkoniyatini anglatadi. Ushbu tamoyillarning buzilishi ta’lim jarayonida turli muammolarni keltirib chiqarishi mumkin. Masalan, elektron jurnaldagi baholarning ruxsatsiz o‘zgartirilishi yaxlitlikka, talabalar hujjatlarining begona shaxslarga oshkor etilishi maxfiylikka, ta’lim platformasining ishdan chiqishi esa mavjudlikka tahdid hisoblanadi.

Ta’lim muassasalarida uchraydigan keng tarqalgan tahdidlardan biri fishing hujumlaridir. Bunda foydalanuvchiga rasmiy tashkilot yoki ta’lim platformasi nomidan soxta elektron xabar yuborilib, uning login va parolini olishga urinish amalga oshiriladi. Foydalanuvchi xabardagi havolaga ishonib, soxta sahifaga ma’lumot kiritganida, uning hisobiga ruxsatsiz kirish imkoniyati yuzaga kelishi mumkin. Bunday xavfni kamaytirish uchun elektron xabarlar manzilini tekshirish, shubhali havolalardan foydalanmaslik, ko‘p bosqichli autentifikatsiyani joriy etish va foydalanuvchilarning xabardorligini oshirish zarur.

Ikkinchi muhim tahdid zararli dasturlar bilan bog‘liq. Ular himoyalanmagan fayllar, noma’lum elektron pochta ilovalari, ishonchsiz dasturlar va tashqi xotira qurilmalari orqali

axborot tizimlariga kirishi mumkin. Ayrim zararli dasturlar ma’lumotlarni o‘g‘irlashga, boshqalari esa fayllarni shifrlash yoki tizim faoliyatini izdan chiqarishga qaratiladi. Ayniqsa, ma’lumotlarni shifrlab, ularni qayta tiklash evaziga to‘lov talab qiluvchi ransomware hujumlari ta’lim muassasalari uchun jiddiy xavf tug‘diradi. Bunday holatlarda elektron hujjatlar va o‘quv ma’lumotlariga kirish cheklanishi, ta’lim jarayonining ayrim qismlari vaqtincha to‘xtashi mumkin.

Uchinchi muammo foydalanuvchi hisoblarini himoyalash bilan bog‘liq. Sodda parollar, bir xil parolni turli platformalarda ishlatish, hisob ma’lumotlarini boshqalarga berish va umumiy kompyuterlarda tizimdan chiqishni unutish ruxsatsiz kirish xavfini oshiradi. Ayniqsa, ma’muriy vakolatga ega hisoblarning himoyasizligi katta miqdordagi ma’lumotlarga ta’sir ko‘rsatishi mumkin. Shu sababli foydalanuvchilarga zarur vakolatlarni berish, ortiqcha huquqlarni cheklash va muhim hisoblarda qo‘shimcha autentifikatsiya vositalaridan foydalanish talab etiladi.

Tarmoq infratuzilmasidagi zaifliklar ham axborot xavfsizligiga salbiy ta’sir ko‘rsatadi. Yangilanmagan dasturiy ta’minot, noto‘g‘ri sozlangan tarmoq qurilmalari, himoyasiz simsiz tarmoqlar va ochiq qolgan xizmatlar hujumchilar uchun kirish nuqtasiga aylanishi mumkin. Ta’lim muassasalarida ma’muriy tizimlar, o‘quv kompyuterlari, mehmonlar tarmog‘i va serverlarni alohida segmentlarga ajratish, tarmoqlararo ekranlardan foydalanish va tarmoq faoliyatini monitoring qilish bunday xavflarni kamaytirishga yordam beradi.

Kiberxavfsizlikka ta’sir qiluvchi omillar faqat tashqi hujumlar bilan cheklanmaydi. Xodimlarning ehtiyotsizligi, sobiq xodimlarning hisoblari yopilmasligi, ma’lumotlarni shaxsiy qurilmalarda nazoratsiz saqlash yoki maxfiy hujjatlarni noto‘g‘ri manzilga yuborish ham xavf tug‘diradi. Shuning uchun axborot xavfsizligi siyosatida ichki foydalanuvchilarning huquq va majburiyatlari, ma’lumotlardan foydalanish chegaralari hamda hodisalar haqida xabar berish tartibi aniq belgilanishi kerak.

Shaxsiy ma’lumotlarni himoyalashning o‘ziga xos jihatlari

Shaxsiy ma’lumotlarni himoyalash ta’lim muassasalarining axborot xavfsizligi tizimida alohida o‘rin egallaydi. Bunday ma’lumotlar bilan ishlashda ularni yig‘ish maqsadi,

qayta ishlashning qonuniy asosi, saqlash muddati va ulardan foydalanish huquqiga ega shaxslar oldindan aniqlanishi lozim. Ma’lumotlarni zarur bo‘lmagan hajmda yig‘ish yoki ularni belgilangan maqsaddan tashqari ishlatish himoya tizimining murakkablashishiga va huquqiy xavflarning ortishiga olib kelishi mumkin.

Shaxsiy ma’lumotlarning xavfsizligini ta’minlashda kirish huquqlarini cheklash muhim ahamiyatga ega. Har bir xodim faqat o‘z vazifasini bajarishi uchun zarur bo‘lgan axborotdan foydalanishi kerak. Masalan, muayyan guruhga dars beruvchi pedagogning tegishli talabalar baholarini ko‘rishi asosli bo‘lishi mumkin, biroq boshqa bo‘limlardagi barcha shaxsiy hujjatlarga kirish huquqining berilishi zarur emas. Eng kam vakolat tamoyiliga rioya etish ma’lumotlarning ruxsatsiz tarqalish ehtimolini kamaytiradi. Ma’lumotlarni uzatish va saqlash jarayonida shifrlash texnologiyalaridan foydalanish ham muhim himoya vositasi hisoblanadi. Shifrlangan aloqa kanallari tarmoq orqali yuborilayotgan axborotni himoyalashga yordam beradi, saqlash vositalarini shifrlash esa qurilma yo‘qolgan yoki o‘g‘irlangan holatlarda ma’lumotlardan ruxsatsiz foydalanish xavfini kamaytiradi. Biroq shifrlash kalitlarini xavfsiz boshqarish, zaxira nusxalarini himoyalash va foydalanuvchi huquqlarini nazorat qilish kabi qo‘shimcha choralar ham zarur.

Bulutli xizmatlar va tashqi platformalardan foydalanishda ma’lumotlarning qayerda saqlanishi, kim tomonidan qayta ishlanishi, ularga kirish huquqlari va ma’lumotlarni o‘chirish tartibi hisobga olinishi kerak. Ta’lim muassasasi tashqi xizmatni tanlashda uning xavfsizlik imkoniyatlarini, maxfiylik shartlarini va amaldagi qonunchilik talablariga muvofiqligini tekshirishi lozim. Shaxsiy ma’lumotlarni himoyalash faqat texnik masala emas, balki ma’lumotlarni boshqarish va ulardan qonuniy foydalanishni nazorat qilish jarayoni hamdir.

Kiberxavfsizlikni ta’minlashning texnik va tashkiliy mexanizmlari

Ta’lim muassasalarida kiberxavfsizlikni kuchaytirish uchun bir-birini to‘ldiruvchi himoya vositalaridan foydalanish zarur. Birinchi navbatda, foydalanuvchilarni autentifikatsiya qilish tizimi takomillashtirilishi lozim. Ko‘p bosqichli autentifikatsiya login

va paroldan tashqari qo‘shimcha tasdiqlashni talab qilib, hisobga ruxsatsiz kirish xavfini kamaytiradi. Ushbu mexanizmni, ayniqsa, ma’muriy hisoblar, elektron pochta va muhim ma’lumotlar bazalariga kirishda qo‘llash maqsadga muvofiq.

Ikkinchi yo‘nalish dasturiy ta’minot va tarmoq qurilmalarining xavfsizligini ta’minlashdir. Operatsion tizimlar, server dasturlari, elektron platformalar va tarmoq qurilmalari muntazam yangilanib borishi kerak. Muassasada mavjud axborot aktivlarining ro‘yxatini yuritish, yangilanishlarni nazorat qilish va qo‘llab-quvvatlash muddati tugagan vositalarni almashtirish xavfsizlikdagi zaifliklarni kamaytirishga xizmat qiladi.

Uchinchi yo‘nalish zaxira nusxalarini yaratish va ma’lumotlarni tiklash imkoniyatlarini ta’minlashdan iborat. Muhim hujjatlar va ma’lumotlar bazalarining nusxalari asosiy tizimdan alohida saqlanishi, ularga kirish cheklanishi va tiklash jarayoni muntazam tekshirilishi lozim. Faqat zaxira nusxasining mavjudligi yetarli emas; undan ma’lumotlarni amalda tiklash mumkinligi ham tasdiqlanishi kerak.

To‘rtinchi yo‘nalish xavfsizlik hodisalarini monitoring qilish va qayd etishdir. Tizimga kirish urinishlari, foydalanuvchi huquqlarining o‘zgarishi va shubhali faoliyatlar qayd etilishi kiberhodisalarni aniqlash hamda ularning sabablarini o‘rganishga yordam beradi. Hodisa yuz berganda mas’ul xodimlarni xabardor qilish, zararlangan qurilmalarni ajratish, buzilgan hisoblarni himoyalash va tizimni xavfsiz tiklash bo‘yicha oldindan belgilangan tartib bo‘lishi zarur.

Beshinchi yo‘nalish tashkiliy boshqaruv va foydalanuvchilarni xabardor qilishni qamrab oladi. Ta’lim muassasasida axborot xavfsizligi siyosati ishlab chiqilishi, mas’ul xodimlar tayinlanishi va xodimlar hamda ta’lim oluvchilarga muntazam tushuntirish ishlari olib borilishi lozim. Fishing xabarlarini aniqlash, parollarni himoyalash, umumiy kompyuterlardan xavfsiz foydalanish va shaxsiy ma’lumotlarni ulashishdan oldin tekshirish kabi amaliy masalalarga alohida e’tibor qaratish zarur. Tahlil natijalariga asoslanib, ta’lim muassasalarida kiberxavfsizlikni kompleks boshqarishning besh bosqichli modelini taklif etish mumkin. Birinchi bosqichda muassasaning axborot aktivlari ro‘yxatga olinadi va ular bilan bog‘liq xavflar aniqlanadi. Ikkinchi bosqichda xavf darajasiga muvofiq texnik himoya

choralari tanlanadi va joriy etiladi. Uchinchi bosqichda tashkiliy qoidalar, foydalanuvchilar vakolatlari va shaxsiy ma’lumotlar bilan ishlash tartibi belgilanadi. To‘rtinchi bosqichda foydalanuvchilarning xabardorligi oshiriladi va xavfsizlik qoidalariga rioya etilishi nazorat qilinadi. Beshinchi bosqichda xavfsizlik hodisalari monitoring qilinadi, zarur hollarda tizimlar tiklanadi va aniqlangan kamchiliklar asosida himoya choralari takomillashtiriladi.

Mazkur model mualliflik taklifi sifatida shakllantirilgan bo‘lib, uning samaradorligi muayyan ta’lim muassasasida amaliy tekshiruvlar orqali baholanishi lozim. Baholashda muhim hisoblarda ko‘p bosqichli autentifikatsiya joriy etilganligi, kirish huquqlarining muntazam tekshirilishi, zaxira nusxalarini tiklash sinovlari, dasturiy ta’minot yangilanishlarining bajarilishi va kiberhodisalar haqida xabar berish tartibining mavjudligi kabi ko‘rsatkichlardan foydalanish mumkin. Ushbu yondashuv kiberxavfsizlikni bir martalik texnik tadbir sifatida emas, balki muntazam nazorat va takomillashtirishni talab qiladigan boshqaruv jarayoni sifatida tashkil etishga yordam beradi. Modelni joriy etishda ta’lim muassasasining hajmi, texnik imkoniyatlari, axborot tizimlarining xususiyatlari va mavjud xavflar darajasi hisobga olinishi zarur.

O‘zbekiston Respublikasida kiberxavfsizlik va shaxsiy ma’lumotlarni himoyalashning huquqiy asoslari

O‘zbekistonda shaxsiy ma’lumotlarni himoyalash va kiberxavfsizlikni ta’minlash tegishli qonunchilik hujjatlari bilan tartibga solinadi. Jumladan, 2019-yil 2-iyuldagi O‘RQ-547-sonli “Shaxsga doir ma’lumotlar to‘g‘risida”gi Qonun hamda 2022-yil 15-apreldagi O‘RQ-764-sonli “Kiberxavfsizlik to‘g‘risida”gi Qonun ushbu sohaning muhim huquqiy asoslari hisoblanadi.

Ta’lim muassasalari shaxsiy ma’lumotlarni yig‘ish, saqlash, qayta ishlash va uzatishda qonunchilikda belgilangan talablarni hisobga olishi zarur. Buning uchun ma’lumotlarni qayta ishlash maqsadlarini belgilash, ulardan foydalanish huquqlarini cheklash, axborot tizimlarining himoyasini ta’minlash va ma’lumotlarni saqlash tartibini belgilash talab etiladi. Shaxsiy ma’lumotlarni qayta ishlash bilan bog‘liq ichki hujjatlar amaldagi qonunchilikka muvofiq ishlab chiqilishi va muntazam qayta ko‘rib chiqilishi lozim.

Huquqiy talablarni amaliyotga tatbiq etish texnik himoya vositalari bilan uyg‘unlikda olib borilishi kerak. Masalan, ma’lumotlarni shifrlash yoki kirish huquqlarini cheklash texnik himoyani ta’minlasa, ma’lumotlarni qonuniy maqsadda yig‘ish, ulardan foydalanish asoslarini belgilash va saqlash muddatlariga rioya etish tashkiliy-huquqiy boshqaruv bilan bog‘liq. Ushbu yo‘nalishlarning birgalikda amalga oshirilishi axborot xavfsizligini mustahkamlashga yordam beradi.

O‘rganilgan masalalar ta’lim muassasalarida kiberxavfsizlikni ta’minlash bir nechta o‘zaro bog‘liq omillarga bog‘liqligini ko‘rsatadi. Texnik himoya vositalari ruxsatsiz kirish, zararli dasturlar va tarmoq hujumlari xavfini kamaytirishga yordam beradi, biroq ular noto‘g‘ri boshqaruv yoki foydalanuvchilarning ehtiyotsizligi sababli yuzaga keladigan barcha muammolarni mustaqil ravishda bartaraf eta olmaydi. Shu sababli axborot xavfsizligini ta’minlashda texnik, tashkiliy va huquqiy choralarni uyg‘unlashtirish zarur. Taklif etilayotgan kompleks modelning amaliy ahamiyati xavfsizlik choralarini bosqichma-bosqich rejalashtirish va ularning bajarilishini baholash imkoniyati bilan belgilanadi. Biroq modelning samaradorligi hozircha empirik natijalar bilan tasdiqlanmagan. Uni turli ta’lim muassasalarida sinovdan o‘tkazish, xavflarni baholash ko‘rsatkichlarini aniqlashtirish va joriy etishdan oldingi hamda keyingi holatlarni taqqoslash kelgusidagi tadqiqotlarning muhim yo‘nalishi hisoblanadi.

Xulosa

Ta’lim muassasalarining raqamli infratuzilmasi kengayishi kiberxavfsizlik va shaxsiy ma’lumotlarni himoyalash masalalarining ahamiyatini oshirmoqda. Elektron ta’lim platformalari, ma’lumotlar bazalari va bulutli xizmatlardan foydalanish qulaylik yaratishi bilan birga, ruxsatsiz kirish, fishing, zararli dasturlar, ma’lumotlarning oshkor bo‘lishi va xizmatlar faoliyatining buzilishi kabi xavflarni ham yuzaga keltiradi. Tahlil natijalari ta’lim muassasalarida xavfsizlikni ta’minlash uchun ko‘p bosqichli autentifikatsiya, ma’lumotlarni shifrlash, kirish huquqlarini cheklash, tarmoq infratuzilmasini himoyalash, dasturiy ta’minotni yangilash, zaxira nusxalarini yaratish va xavfsizlik hodisalarini monitoring qilish kabi mexanizmlardan kompleks foydalanish zarurligini ko‘rsatadi. Shaxsiy ma’lumotlar

bilan ishlashda ularni zarur hajmda yig‘ish, qonuniy maqsadlarda qayta ishlash, saqlash muddatlarini belgilash va ruxsatsiz foydalanishdan himoyalash alohida ahamiyatga ega.

Maqolada taklif etilgan besh bosqichli model axborot aktivlarini aniqlash, texnik himoya choralarini joriy etish, tashkiliy-huquqiy boshqaruvni yo‘lga qo‘yish, foydalanuvchilarni xabardor qilish hamda monitoring va tiklash jarayonlarini o‘zaro bog‘lashga asoslanadi. Uning samaradorligini amaliy tadqiqotlar orqali tekshirish va olingan natijalarga muvofiq takomillashtirish lozim. Mazkur yondashuv ta’lim muassasalarining raqamli infratuzilmasini ishonchli boshqarish, shaxsiy ma’lumotlar daxlsizligini saqlash va axborot tizimlarining barqaror faoliyatini ta’minlashga xizmat qilishi mumkin.

Foydalanilgan adabiyotlar

1. O‘zbekiston Respublikasining 2019-yil 2-iyuldagi O‘RQ-547-sonli “Shaxsga doir ma’lumotlar to‘g‘risida”gi Qonuni. — https://lex.uz/

2. O‘zbekiston Respublikasining 2022-yil 15-apreldagi O‘RQ-764-sonli “Kiberxavfsizlik to‘g‘risida”gi Qonuni. — https://lex.uz/

3. National Institute of Standards and Technology. The NIST Cybersecurity Framework (CSF) 2.0. NIST CSWP 29, 2024. — https://doi.org/10.6028/NIST.CSWP.29

4. UNESCO Institute for Information Technologies in Education. Personal Data and Privacy Protection in Online Learning: Guidance for Students, Teachers and Parents. — https://iite.unesco.org/

5. Cybersecurity and Infrastructure Security Agency. #StopRansomware Guide. — https://www.cisa.gov/stopransomware/ransomware-guide

6. National Institute of Standards and Technology. Cybersecurity Framework. — https://www.nist.gov/cyberframework