Uzbek Scholar Journal
Volume- 58, November- 2026
www.uzbekscholar.com

XXI ASRDA AXBOROT XAVFSIZLIGINING DOLZARB MUAMMOLARI VA RIVOJLANISH ISTIQBOLLARI

Akramov Xondamir Hotam o‘g‘li
Sharof Rashidov nomidagi Samarqand davlat universiteti
Axborot xavfsizligi yo’nalishi masgistranti

Annotatsiya:
Tezisda XXI asrda axborot xavfsizligiga ta’sir ko‘rsatayotgan texnologik va tashkiliy o‘zgarishlar tahlil qilinadi. Shaxsga doir ma’lumotlarning oshkor bo‘lishi, hisob yozuvlarining egallanishi, raqamli xizmatlarning uzilishi, tashqi yetkazib beruvchilarga bog‘liqlik hamda sun’iy intellekt bilan bog‘liq tahdidlar oliy ta’lim muassasalari faoliyati misolida ko‘rib chiqiladi. Tahdidlar yuzaga kelish ehtimoli, ehtimoliy zarar va xizmatni tiklash imkoniyati bo‘yicha taqqoslanadi. Himoyani rivojlantirish istiqbollari sifatida xavfga asoslangan boshqaruv, minimal kirish huquqlari, ko‘p omilli autentifikatsiya, hodisalarni kuzatish va xizmatlarni tiklashga tayyorgarlik yoritiladi. O‘zbekiston oliy ta’lim muassasalarida ushbu choralarni joriy etishda axborot resurslarining muhimligi, o‘quv jarayoni taqvimi, foydalanuvchilarning til ehtiyojlari va mutaxassislar salohiyatini hisobga olish asoslanadi.

Kalit so‘zlar. Axborot xavfsizligi, kiberxavf, raqamli infratuzilma, shaxsga doir ma’lumotlar, kirishni boshqarish, nol ishonch arxitekturasi, hodisalarga javob berish, raqamli barqarorlik.

Kirish

XXI asrda ta’lim, davlat boshqaruvi, bank xizmatlari va ishlab chiqarish jarayonlarining raqamli platformalarga ko‘chishi axborot xavfsizligining amaliy ahamiyatini oshirdi. Oliy ta’lim muassasalarida abituriyentlarni ro‘yxatga olish, talabalar o‘zlashtirishini qayd etish, o‘quv materiallarini tarqatish va ilmiy ma’lumotlarni saqlash turli axborot tizimlari orqali amalga oshiriladi. Ushbu tizimlar bilan bog‘liq hodisa bir vaqtning o‘zida ma’lumotlar maxfiyligiga ham, xizmat uzluksizligiga ham ta’sir qilishi mumkin. Masalan, elektron jurnalga ruxsatsiz kirish baholar va shaxsga doir ma’lumotlarning oshkor bo‘lishi xavfini tug‘diradi. Baholarning o‘zgartirilishi ma’lumotlar yaxlitligini buzadi, jurnalning ishlamay qolishi esa o‘quv jarayonida kechikishlarga sabab bo‘lishi mumkin.
Raqamli xizmatlarning o‘zaro bog‘lanishi xavfning tarqalish doirasini o‘zgartiradi. Universitetning yagona hisob yozuvi foydalanuvchiga elektron pochta, ta’lim platformasi va ichki hujjatlar tizimiga kirish imkonini berishi mumkin. Bunday tartib kundalik ishni yengillashtiradi, ayni paytda kirish huquqlari to‘g‘ri belgilanmasa, bitta hisob yozuvining egallanishi bir nechta xizmatga ta’sir ko‘rsatadi. Hodisaning oqibati foydalanuvchi vakolatlariga, bog‘langan tizimlar soniga hamda shubhali faoliyatni aniqlash va to‘xtatish tezligiga bog‘liq. Shu sababli universitet xizmatlarini tahlil qilishda ma’lumotning qayerda saqlanishi bilan birga unga kim, qaysi vazifa doirasida va qanday vosita orqali kirishi ham o‘rganiladi.

1-jadval. Oliy ta’lim muassasalarida axborot xavfsizligini ta’minlash yondashuvlarining qiyosiy tavsifi

№	Yondashuv	Qaysi tahdidga qarshi	Asosiy choralar	OTM faoliyatidagi misol	Samaradorlik ko‘rsatkichlari
1	Xavfga asoslangan boshqaruv	Muhim va ikkinchi darajali xizmatlarga bir xil yondashish, resurslarning noto‘g‘ri taqsimlanishi	Har bir tizimning vazifasi, egasi, foydalanuvchilari, ma’lumot turi va bog‘liqligini aniqlash; xavflarni davriy qayta baholash	Elektron jurnalda baholar yaxlitligi muhim, kutubxona katalogida xizmat uzluksizligi muhim	Mutaxassislar va mablag‘ning muhim xizmatlarga yo‘naltirilishi; qayta baholash natijalari
2	Kirish huquqlarini boshqarish	Hisob yozuvlarining egallanishi, ortiqcha vakolatlar	Ko‘p omilli autentifikatsiya; vakolatlarni vazifa bo‘yicha taqsimlash; faoliyat jurnallarini kuzatish; lavozim o‘zgarganda huquqlarni qayta ko‘rish	Talaba hisobi bilan tizim ma’muri hisobi egallanganda oqibatlar har xil bo‘ladi	O‘z vaqtida bekor qilingan ruxsatlar ulushi; shubhali kirishni tekshirish davomiyligi
3	Nol ishonch arxitekturasi	Bitta hisob orqali bog‘langan xizmatlarga xavfning tarqalishi	Kirishni foydalanuvchi, qurilma va resurs ma’lumotlari asosida berish; joriy etishni sezgir xizmatlardan boshlash	Talaba qurilmasi ta’lim platformasiga kira oladi, moliyaviy tizimga esa faqat vakolatli xodim kiradi	Ortiqcha huquqlarning qisqarishi; qonuniy foydalanuvchilar murojaatlari va kirishdagi uzilishlar soni
4	Ma’lumotlarni himoya qilish	Shaxsga doir ma’lumotlarning oshkor bo‘lishi	Ma’lumotni faqat kerakli hajmda yig‘ish; shifrlash; amallar jurnali; bo‘limlar o‘rtasida almashuv qoidalari	Murojaatni ko‘rayotgan xodim faqat kerakli hujjatlarni oladi, talabalar bazasini to‘liq ko‘chira olmaydi	Saqlanadigan ma’lumotlar hajmi; oshkor bo‘lishi mumkin bo‘lgan ma’lumotlar doirasi
5	Xizmat uzluksizligi va tiklashga tayyorgarlik	Xizmat uzilishi, tashqi yetkazib beruvchiga bog‘liqlik	Zaxira nusxalarini tekshirish; tiklash mashqlari; vaqtinchalik ish tartibi; foydalanuvchilarni xabardor qilish; ma’lumotni yetkazib beruvchidan qaytarib olish tartibi	Yakuniy imtihon kuni masofaviy ta’lim portali ishlamay qolishi	Tiklash vaqti; tiklangan yozuvlarning to‘liqligi; xabarning o‘z vaqtida yetib borishi
6	Sun’iy intellekt va avtomatlashtirish	Ko‘p sonli ogohlantirishlar, odatiy tartibdan chetga chiqishlar	Ogohlantirishlarni saralash; noodatiy faoliyatni aniqlash; muhim amallarni mas’ul xodim qaroriga bog‘lash; SI yordamchisining kirish huquqlarini nazorat qilish	Semestr boshida tarmoqqa ko‘plab yangi ulanishlar paydo bo‘lishi	Aniqlash qamrovi; yolg‘on ogohlantirishlar ulushi; hodisani ko‘rib chiqish vaqti
7	Tashkiliy tayyorgarlik va kadrlar salohiyati	Soxta xabarlar orqali aldash, hodisaga kechikib javob berish	Aniq murojaat tartibi; texnik bo‘linma vakolatlari; vaziyatli mashg‘ulotlar; o‘zbek, rus va ingliz tillarida aniq bildirishnomalar	Universitet pochtasiga dekanat nomidan kelgan shubhali xabar bo‘yicha mashg‘ulot	Foydalanuvchi xabari, texnik nazorat va mas’ul bo‘linma javobi o‘rtasidagi bog‘liqlik

Manba: muallif tomonidan tuzilgan.

Axborot xavfsizligining dolzarb muammolaridan biri foydalanuvchi uchun odatiy bo‘lgan raqamli muloqotdan aldov maqsadida foydalanishdir. Qabul komissiyasi, dekanat yoki texnik yordam xizmati nomidan tarqatilgan soxta xabar odatiy xizmat yozishmasiga o‘xshashi mumkin. Xabar imtihon jadvali, hujjat topshirish muddati yoki hisob yozuvini tiklash kabi dolzarb masalaga taalluqli bo‘lsa, foydalanuvchi shoshilinch qaror qabul qilishi ehtimoli ortadi. Generativ sun’iy intellekt yordamida tabiiy uslubdagi matn va sintetik ovoz yaratilishi xabar manbasini tekshirishga bo‘lgan ehtiyojni kuchaytiradi. Bunday vaziyatlarda xavfsizlikka ta’lim muassasasining rasmiy muloqot tartibi, foydalanuvchilarning xabar berish imkoniyati va texnik himoya vositalari birgalikda ta’sir qiladi.

Bulutli platformalar va tashqi axborot xizmatlaridan foydalanish ham himoya mas’uliyatining taqsimlanishiga ta’sir ko‘rsatadi. Universitet xizmatni tashqi yetkazib beruvchidan olganida, ma’lumotlardan foydalanish qoidalari, kirish huquqlari, hodisa haqida xabar berish va ish faoliyatini tiklash tartibi oldindan belgilanishi muhim. Tashqi xizmatda uzilish sodir bo‘lsa, uning oqibatlari universitetning shu xizmatga qanchalik bog‘liqligi bilan belgilanadi. Masalan, masofaviy ta’lim platformasi imtihon o‘tkaziladigan kuni ishlamay qolsa, texnik muammo baholash jadvaliga ham ta’sir qiladi. Muammoni tahlil qilishda xizmatning muhimligi, vaqtinchalik ish tartibi va universitetda saqlanadigan ma’lumotlar nusxasidan foydalanish imkoniyati e’tiborga olinadi.

O‘zbekiston oliy ta’lim muassasalari uchun axborot xavfsizligining yana bir jihati raqamli xizmatlardan turli foydalanuvchilar foydalanishidir. Talabalar, professor-o‘qituvchilar, ma’muriy xodimlar va tashqi hamkorlarning vazifalari hamda ma’lumotga bo‘lgan ehtiyoji farq qiladi. Talaba o‘z natijalarini ko‘rishi, o‘qituvchi o‘z faniga tegishli baholarni kiritishi, vakolatli xodim esa muayyan hujjatlarni tekshirishi mumkin. Ushbu vazifalarga mos ruxsatlar belgilanganda, foydalanuvchi o‘z ishini bajarish uchun kerakli ma’lumotni oladi va ortiqcha kirish imkoniyatlari kamayadi. O‘zbek, rus va ingliz tillarida muloqot yuritiladigan muhitda xavfsizlik bildirishnomalarining aniqligi ham foydalanuvchining shubhali vaziyatni tushunishi va o‘z vaqtida xabar berishiga ta’sir ko‘rsatadi.

Axborotni himoya qilish istiqbollari raqamli resurslarning muhimligi va ularga tahdid soluvchi hodisalarning oqibatlarini aniqlash bilan bog‘liq. Har bir xizmat uchun xavf darajasi bir xil bo‘lmaydi. Ochiq e’lonlar sahifasidagi vaqtinchalik uzilish bilan talabalar ma’lumotlari saqlanadigan tizimdagi uzilishning tashkiliy oqibatlari farq qiladi. Xuddi shuningdek, ochiq dars jadvalini ko‘rish huquqi bilan yakuniy bahoni o‘zgartirish huquqi turli xavfsizlik talablarini yuzaga keltiradi. Resurslarni shu asosda baholash texnik vositalar, mutaxassislar va ajratilgan mablag‘ni muhim xizmatlarga yo‘naltirish imkonini beradi. Bunda xizmatning ish yuklamasi va uzilishning o‘quv taqvimiga ta’siri ham hisobga olinadi.

Tezisning maqsadi zamonaviy axborot xavfsizligi muammolarini oliy ta’lim muassasalari faoliyati bilan bog‘liq holda tahlil qilish va himoyani rivojlantirishning ustuvor yo‘nalishlarini asoslashdan iborat. Tahlilda ilmiy adabiyotlarni qiyoslash hamda universitet faoliyatiga xos vaziyatlarni ko‘rib chiqish usullaridan foydalaniladi. Tahdidlar ta’sir qiladigan resurs, hodisaning yuzaga kelish sharoiti, ehtimoliy zarar va tiklanish imkoniyati bo‘yicha tavsiflanadi. Himoya choralari ularning vazifasi, joriy etish sharoiti hamda natijasini kuzatish uchun zarur bo‘lgan ko‘rsatkichlar asosida baholanadi. Bu mezonlar elektron jurnal, qabul tizimi, universitet pochtasi va ma’lumotlar omborining o‘ziga xos xavflarini izchil tahlil qilishga imkon beradi.

Asosiy qism

Axborot xavfsizligini boshqarishda tahlil universitet faoliyati uchun zarur resurslarni aniqlashdan boshlanadi. Har bir axborot tizimi bo‘yicha uning vazifasi, mas’ul bo‘linmasi, foydalanuvchilari, saqlanadigan ma’lumotlar turi va boshqa xizmatlar bilan bog‘liqligi aniqlashtiriladi. Masalan, elektron jurnal himoyasida baholarning maxfiyligi, o‘zgartirishlar tarixining saqlanishi va baholash davrida tizimdan foydalanish imkoniyati birgalikda hisobga olinadi. Kutubxonaning ochiq katalogida esa qidiruv xizmatining uzluksizligi va bibliografik ma’lumotlarning to‘g‘riligi ustuvor bo‘lishi mumkin. Bunday farqlar tahdid oqibatini aniq ifodalashga va barcha tizimlarga bir xil talab qo‘yish oqibatida ortib ketadigan ish yukini kamaytirishga yordam beradi.

Hisob yozuvlarining egallanishi tahdidini tahlil qilishda foydalanuvchi vakolati va hisobdan amalga oshiriladigan amallar muhim o‘rin tutadi. Talaba hisobidan ruxsatsiz foydalanish uning shaxsiy yozishmalari va o‘quv natijalariga ta’sir qilishi mumkin. Tizim ma’muri hisobining egallanishi esa boshqa foydalanuvchilarning huquqlari yoki xizmat sozlamalarini o‘zgartirish imkonini yuzaga keltiradi. Himoya uchun ko‘p omilli autentifikatsiya, vakolatlarni xizmat vazifalari bo‘yicha taqsimlash va faoliyat jurnallarini kuzatish birgalikda qo‘llanadi. Xodim boshqa lavozimga o‘tganda avvalgi huquqlarini qayta ko‘rib chiqish, vaqtinchalik ruxsatlar muddati tugaganda ularni bekor qilish kirishni boshqarishning muntazam jarayoniga aylanishi mumkin. Baholashda o‘z vaqtida bekor qilingan ruxsatlar ulushi va shubhali kirish bo‘yicha tekshiruv davomiyligi kuzatiladi.

Nol ishonch arxitekturasi rivojlanish istiqbollaridan biri sifatida foydalanuvchi, qurilma va murojaat qilinayotgan resursga doir ma’lumotlar asosida kirishni boshqarishga yordam beradi. Universitet tarmog‘iga ulangan qurilma uchun ham ruxsat so‘ralgan xizmat va foydalanuvchi vazifasiga qarab belgilanadi. Masalan, kampus tarmog‘idagi talaba qurilmasiga ta’lim platformasidan foydalanish huquqi berilishi mumkin, moliyaviy hujjatlar tizimiga kirish esa tegishli vakolatga ega xodimlarga cheklanadi. Joriy etishni ma’lumotlari sezgir bo‘lgan yoki keng vakolatli hisoblar ishlatiladigan xizmatlardan boshlash mumkin. Bu jarayonda ortiqcha huquqlarning qisqarishi bilan birga qonuniy foydalanuvchilar murojaatlari va kirishdagi uzilishlar ham kuzatiladi.

Ma’lumotlarni himoya qilish ularni yig‘ish, saqlash, uzatish va foydalanishdan chiqarish jarayonlarini qamrab oladi. Qabul tizimidagi shaxsga doir ma’lumotlar xizmat vazifasi uchun zarur hajmda olinishi va foydalanish maqsadiga mos tartibda saqlanishi lozim. Bo‘limlar o‘rtasidagi almashuvda qaysi ma’lumot kimga va nima sababdan berilishi aniqlashtiriladi. Shifrlash ma’lumotni himoya qilishda qo‘llanadi, kirish huquqlari va amallar jurnali esa undan foydalanish ustidan nazoratni ta’minlaydi. Masalan, talabaning murojaatini ko‘rib chiqayotgan xodim ish uchun kerakli hujjatlarni olishi mumkin. Mazkur vazifa sababli talabalar bazasini to‘liq ko‘chirishga ruxsat berish oqilona bo‘lmaydi. Saqlanadigan ma’lumot hajmining cheklanishi hodisa yuz berganda oshkor bo‘lishi mumkin bo‘lgan ma’lumotlar doirasini ham qisqartiradi.

Xizmat uzilishiga qarshi himoya hodisani aniqlash, uning ta’sirini cheklash va ishni tiklashga tayyorgarlikni birlashtiradi. Zaxira nusxasi yaratilganini qayd etish bilan birga undan kerakli ma’lumotni tiklash imkoniyati va tiklash davomiyligini tekshirish xizmatning amaliy tayyorgarligini baholashga yordam beradi. Qabul tizimi hamda o‘quv portaliga qo‘yiladigan tiklanish talablari ularning ish yuklamasi va taqvimiga qarab farqlanadi. Masalan, yakuniy imtihon paytida portalga kirish uzilsa, vaqtinchalik ish tartibi, mas’ullar o‘rtasida aloqa va foydalanuvchilarga tezkor xabar berish ham texnik tiklash qadar muhim bo‘lishi mumkin. Tashqi platformalar bilan ishlashda hodisa haqida xabarnoma olish va ma’lumotlarni qaytarib olish tartibi shu jarayonga kiritiladi.

Sun'iy intellekt va avtomatlashtirish xavfsizlik hodisalari haqidagi ko'p sonli xabarlarni saralash, odatiy ish tartibidan chetga chiqishlarni aniqlash va mutaxassisga dastlabki ma'lumotni taqdim etishda qo'llanishi mumkin. Universitet tarmog'ida semestr boshida ko'plab yangi ulanishlar kuzatilishi tabiiy. Bunday vaziyatda modelning ogohlantirishlari hodisaning mazmuni, foydalanuvchi roli va tegishli xizmatning ish tartibi bilan birga tekshiriladi. Natijani baholashda aniqlangan tahdidlar qamrovi, yolg'on ogohlantirishlar ulushi va mutaxassisning hodisani ko'rib chiqish vaqti hisobga olinadi. Sun'iy intellektga asoslangan yordamchi ichki hujjatlarni qayta ishlaganda, unga berilgan kirish huquqlari hamda ma'lumotni kimga taqdim etishi mumkinligi alohida nazorat qilinadi.

Tashkiliy tayyorgarlik himoya choralarining kundalik faoliyatda qanday ishlashini belgilaydi. Shubhali yozishma olgan xodimga qaerga murojaat qilishni bilish, texnik bo'linmaga esa voqeani tekshirish va tegishli bo'limga yetkazish vakolati kerak. O'quv mashg'ulotlarida universitet pochtasiga kelgan shubhali xabar, baholash tizimida kuzatilgan noodatiy o'zgarish yoki qabul portalining vaqtincha uzilishi kabi vaziyatlardan foydalanish mumkin. Har bir vaziyatda himoyaning sifati foydalanuvchi harakati, texnik nazorat va mas'ul bo'linmaning javobi o'rtasidagi bog'liqlik orqali baholanadi. Axborot xavfsizligi yo'nalishida tahsil olayotgan talabalar bunday misollar orqali tahdid tavsifini himoya chorasi hamda uni baholash mezoni bilan bog'lashni o'rganadilar.

Xulosa

XXI asrda axborot xavfsizligining rivojlanishi raqamli xizmatlarning o'zaro bog'liqligi, ma'lumot almashuvining tezlashishi va yangi texnologiyalarning kundalik faoliyatga kirib borishi bilan belgilanadi. Oliy ta'lim tizimida xavfsizlik hodisasi talabalar ma'lumotlarining oshkor bo'lishi, akademik yozuvlarning o'zgarishi yoki ta'lim xizmatining uzilishi shaklida namoyon bo'lishi mumkin. Tahlil shuni ko'rsatadiki, himoya choralarini tanlashda resursning vazifasi va hodisaning oqibati asosiy mezon bo'lib xizmat qiladi. Elektron jurnal uchun baholar yaxlitligi ustuvor bo'lsa, masofaviy imtihon platformasida xizmatning belgilangan vaqtda ishlashi alohida ahamiyat kasb etadi. Qabul tizimida esa ma'lumotlar maxfiyligi va murojaatlarni o'z vaqtida ko'rib chiqish imkoniyati birgalikda muhofaza qilinadi.

O'zbekiston oliy ta'lim muassasalarida himoyani rivojlantirish uchun avvalo asosiy raqamli xizmatlar, ularning egalari va o'zaro bog'liqligi belgilanishi maqsadga muvofiq. Bu ma'lumot har bir hodisa qaysi bo'limlar faoliyatiga ta'sir qilishini, qanday ma'lumotlar xavf ostida qolishini va xizmatni tiklashda qaysi ishlar avval bajarilishini aniqlashga yordam beradi. Qabul, sessiya va yakuniy attestatsiya davrlarida ayrim xizmatlarning ustuvorligi o'zgaradi. Himoya rejasi o'quv taqvimi bilan bog'langanda, texnik xizmat ko'rsatish, yangilash va zaxiradan tiklash mashqlari uchun qulay vaqtni belgilash osonlashadi. Shu tartib xavfsizlikni universitet faoliyatining umumiy boshqaruvi bilan bog'laydi.

Kirish huquqlarini boshqarish yuqori ta'sirga ega tahdidlarni kamaytirishning asosiy yo'nalishlaridan biridir. Xizmat vazifasiga mos vakolatlar, ko'p omilli autentifikatsiya va ruxsatlarni davriy ko'rib chiqish birgalikda qo'llanganda, shubhali hisob yozuvi orqali bajarilishi mumkin bo'lgan harakatlar doirasi cheklanadi. Nol ishonch arxitekturasi ushbu tamoyillarni bog'langan xizmatlar bo'yicha izchil tatbiq etishga yordam beradi. Universitetda buning amaliy ifodasi qabul ma'lumotlariga, baholarni o'zgartirish amallariga va tizim sozlamalariga kirishni vazifa bo'yicha ajratishdir. Davriy nazorat foydalanuvchining amaldagi vazifasi bilan unga biriktirilgan ruxsatlar o'rtasidagi moslikni tekshirishga xizmat qiladi. Vakolat o'zgarishining qayd etilishi esa hodisa yuz berganda mas'ul shaxslarga holatni tushunishga yordam beradi.

Xizmat uzluksizligi uchun tayyorgarlik zaxira nusxalarini boshqarish, tiklash amallarini mashq qilish va foydalanuvchilarga xabar berish tartibini qamrab olishi zarur. Tiklash vaqti ta'lim jarayoni talablariga mos belgilanganda, universitet qaysi xizmat darhol ishga qaytarilishi va qaysi jarayon vaqtincha boshqa tartibda olib borilishini oldindan aniqlay oladi. Tashqi yetkazib beruvchilarga bog'liq xizmatlarda ma'lumotlarni qaytarib olish va uzilish to'g'risida xabar olish tartibi ham tayyorgarlikning bir qismi hisoblanadi. Mazkur jarayonning sifati xizmatni tiklash uchun sarflangan vaqt, qayta tiklangan yozuvlarning to'liqligi va foydalanuvchilarga berilgan axborotning o'z vaqtida yetib borganligi orqali baholanadi.

Sun'iy intellekt vositalarining rivojlanishi universitet xavfsizlik xizmatlari uchun hodisalarni tezroq saralash va katta hajmdagi faoliyat yozuvlarini tahlil qilish imkoniyatini kengaytiradi. Bu imkoniyatlar ogohlantirishni tekshirish, hodisaga ustuvorlik berish va mas'ul xodimga tushunarli ma'lumot uzatish kabi aniq vazifalar bilan bog'langanda amaliy ahamiyat kasb etadi. Vositaning ishlashi aniqlash qamrovi, yolg'on ogohlantirishlar ulushi va tekshiruvga ketgan vaqt bilan birga baholanadi. Universitet xabarlarida o'zbek, rus va ingliz tillarining qo'llanishi tahlil natijalarini til kesimida ko'rib chiqish uchun asos bo'ladi. Shaxsga doir ma'lumotlarni berish, akademik yozuvni o'zgartirish yoki foydalanuvchi hisobini cheklash kabi amallar mas'ul xodimning qarori bilan bog'lanishi lozim.

Axborot xavfsizligi yo'nalishida kadrlar tayyorlashda texnik bilimni oliy ta'lim muassasasining haqiqiy ish jarayonlari bilan bog'lash muhim. Talaba hodisani tavsiflash, ta'sir ko'rgan resursni aniqlash va bir nechta himoya chorasini oqibatlari bo'yicha taqqoslashni o'rganishi kerak. Masalan, ta'lim portalida shubhali kirish aniqlanganda, hisobni cheklash, bog'liq xizmatlarni tekshirish va o'quv jarayonini davom ettirish imkonini saqlash bo'yicha qarorlar birgalikda ko'rib chiqiladi. Bunday mashg'ulotlarda hodisa haqida tushunarli xabar yozish, mutaxassislar o'rtasida vazifalarni taqsimlash va bajarilgan amallarni hujjatlashtirish ko'nikmalari ham rivojlantiriladi. Bu kompetensiyalar texnik tayyorgarlikni jamoaviy ish va mas'uliyatli qaror qabul qilish bilan uyg'unlashtiradi.

Oliy ta'limda axborot xavfsizligining rivojlanish istiqboli himoyani hodisalarga va xizmatlar ehtiyojiga qarab muntazam takomillashtirish bilan bog'liq. O'z vaqtida bekor qilingan kirish huquqlari, tiklash mashqlarida qayd etilgan vaqt va tekshirilgan ogohlantirishlar ulushi kabi ko'rsatkichlar qaysi jarayon qo'shimcha e'tibor talab qilishini aniqlashga yordam beradi. Xavflarni davriy qayta baholashda yangi platformaning ishga tushirilishi, ma'lumot almashuvining kengayishi va foydalanuvchilar vazifalaridagi o'zgarishlar hisobga olinadi. Shu asosda universitet texnik vositalarni, tashkiliy tartiblarni va xodimlar tayyorgarligini muhim xizmatlar atrofida muvofiqlashtirishi mumkin. Bunday yondashuv ma'lumotlarni himoya qilish, akademik yozuvlar yaxlitligini saqlash va raqamli ta'lim xizmatlarining uzluksizligini ta'minlashga xizmat qiladi.

Foydalanilgan adabiyotlar

1. G'aniyev, S., Karimov, M., & Tashev, K. (2008). Axborot xavfsizligi (Axborot-kommunikatsion tizimlar xavfsizligi). Aloqachi.
2. Admass, W. S., Munaye, Y. Y., & Diro, A. A. (2024). Cyber security: State of the art, challenges and future directions. Cyber Security and Applications, 2, 100031.
3. Sampson, P., Sheehan, B., Shannon, D., Cartwright, A., Seifert, J., Cartwright, E., & Meurs, T. (2026). Bridging the gaps in cyber risk assessment: A comprehensive systematic review of standards, frameworks and quantification methods. The Geneva Papers on Risk and Insurance – Issues and Practice, 51(4).
4. Gambo, M. L., & Almulhem, A. (2026). Zero trust architecture: A systematic literature review. Journal of Network and Systems Management, 34, 25.