O‘ZBEKISTON RESPUBLIKASI OLIY TA’LIM, FAN VA INNOVATSIYALAR VAZIRLIGI
BUXORO DAVLAT UNIVERSITETI

XUSENOV MURODJON ZOXIROVICH,
SALIMOV RO‘ZIBEK NASIM O‘G‘LI

BUXORO DAVLAT UNIVERSITETINING AXBOROT XAVFSIZLIGI SIYOSATI

Buxoro-2025

MUNDARIJA

1. Kirish

Buxoro davlat universiteti (keyingi o‘rinlarda – Universitet) O‘zbekiston Respublikasi Prezidentining 1992-yil 28-fevraldagi PF-356 sonli Farmoni hamda Vazirlar Mahkamasining 1992-yil 11-martdagi 125-sonli Qaroriga asosan Buxoro davlat pedagogika instituti negizida tashkil etilgan. O‘zbekiston Respublikasi Prezidentining 24.12.2021 sanasidagi PQ-60-son va PQ-61-sonli Qarorlari bilan akademik va tashkiliy-boshqaruv va moliyaviy mustaqillik berilgan.

- Universitet O‘zbekiston Respublikasi Prezidentining 2023-yil 3-iyuldagi “Ma’muriy islohotlar doirasida oliy ta’lim, fan va innovatsiyalar sohasida davlat boshqaruvini samarali tashkil qilish chora-tadbirlari to‘g‘risida” PQ-200-son qarori va boshqa me’yoriy-huquqiy hujjatlar asosida ish olib boradi.

- Universitet davlat oliy ta’lim muassasasi hisoblanib, oliy ta’limning asosiy va qo‘shma ta’lim dasturlarini bajarish bo‘yicha ta’lim faoliyatini bilan shug‘ullanadi. Shuningdek O‘zbekiston Respublikasi qonunchilik hujjatlariga muvofiq o‘quv, ilmiy-metodik va boshqa faoliyatlarni amalga oshiradi hamda ta’lim xizmatlarini ko‘rsatadi.

- Universitet o‘z faoliyatida O‘zbekiston Respublikasi Konstitutsiyasi, O‘zbekiston Respublikasi “Ta’lim tog‘risida”gi Qonuni, O‘zbekiston Respublikasi Oliy Majlis palatalarining qarorlari, O‘zbekiston Respublikasi Prezidentining farmon va qarorlari, Vazirlar Mahkamasining qarorlari, O‘zbekiston Respublikasi Oliy ta’lim, fan va innovatsiyalar vazirining buyruqlari hamda mazkur Universitet nizomiga amal qiladi.

Universitetning asosiy maqsadi quyidagilar hisoblanadi:

zamonaviy talablar, ilg‘or xalqaro tajriba va mehnat bozori ehtiyojlari asosiy yuqori malakali, ijodiy fikrlaydigan, halol kadrlarni tayyorlash;

iqtisodiyotning tegishli sohalari bo‘yicha talabalarning fundamental, bazaviy, shuningdek, amaliy kasbiy tayyorgarligini ta’minlaydigan o‘quv reja va dasturlar asosida bakalavrlar, magistrlar tayyorlash;

ish beruvchi ehtiyojidan kelib chiqib, talabalardan tahliliy fikrlash va kasbiy ko‘nikmalar rivojlantirish, yangi bilimlarni mustaqil ravishda egallash va ulardan foydalanish ko‘nikmasini shakllantirishni ta’minlaydigan o‘qitishning zamonaviy shakl va metodlari, pedagogik innovatsion, axborot-kommunikatsiya texnologiyalarini keng qo‘llash;

fanlarni tanlash imkoniyatini ta’minlagan holda Yevropa kredit tizimini (European Credit Transfer and Accumullation System) joriy etish, shu jumladan talabalar o‘quv yuklamasi hajmini aniqlashning xalqaro shartli birliklarini (kreditlar) o‘tkazish va jamlash tizimini qo‘llagan holda o‘quv jarayonini tashkil etish;

universitetning professor-o‘qituvchilari tarkibini yuqori darajada kasbiy pedagogik mahoratga, huquqiy va siyosiy madaniyatga ega mutaxassislar bilan mustahkamlash;

rivojlangan xorijiy davlatlarning yetakchi ta’lim va ilmiy muassasalari bilan hamkorlikni, qo‘shma huquqiy tadqiqotlarni, professor-o‘qituvchilar va talabalar o‘zaro almashinuvini takomillashtirish;

davlat va xo‘jalik boshqaruvi organlari, iqtisodiyotning tegishli sohalari hamda boshqa tashkilotlarda amaliy ish tajribasiga ega bo‘lgan mutaxassislarni ta’lim

jarayoniga keng jalb etish, ularning malakasini oshirishda samarali tizimni yaratish, xorijiy mamlakatlarning yetakchi ta’lim, tadqiqot muassasalarining yuqori malakali mutaxassislarini o‘quv, ilmiy-metodik ishlarni tashkil etish jarayonlariga jalb qilish;

tegishli ta’lim yo‘nalishlari bo‘yicha o‘quv majmualarini, qo‘llanmalarni yaratish va ularni o‘quv jarayonlariga tatbiq qilish;

xorijiy hamkorlar bilan birgalikda kadrlarni tayyorlash bo‘yicha qo‘shma ta’lim dasturlarini (double degree) amalga oshirish, o‘quv-ta’lim jarayoniga xorijiy olimlarni va mutaxassislarni jalb qilish;

milliy iqtisodiyotning tegishli tarmoqlari bo‘yicha ustuvorlikka ega bo‘lgan va ishlab chiqarish ehtiyojidan kelib chiqqan holda ilmiy-tadqiqot ishlarni olib borish va natijalarini amaliyotga tatbiq qilish;

ilmiy-tadqiqot va tajriba-konstruktorlik ishlarni amalga oshirish va bu ishlarga talabalarni jalb etish;

“HEMIS” platformasini yoki oliy ta’lim tizimini avtomatik boshqarishga qaratilgan boshqa tizimlarni joriy etgan holda ochiq, shaffof, subyektivlik va suiiste’molchilikdan xoli bo‘lgan ta’lim muhitini yaratish;

talabalarni ma’naviy-axloqiy tarbiyalash, huquqiy, siyosiy madaniyatini va huquqiy ongini oshirish bo‘yicha samarali tizimni yaratish ularda vatanparvarlik, yuksak ma’naviy-axloqiy fazilatlarni, korrupsiyaga murosasizlik tuyg‘usini shakllantirish hamda rivojlantirish.

Universitet o‘z vazifalarini amalga oshirish maqsadida quyidagi funksiyalarni amalga oshiradi:

davlat ta’lim standartlari asosida mamlakatda o‘tkazilayotgan demokratik va huquqiy islohotlar, fuqarolik jamiyatini shakllantirish va zamonaviy xalqaro standartlarning yuksak talablariga javob beradigan, iqtisodiyotning tegishli sohalari bo‘yicha yuqori malakali kadrlar tayyorlashni tashkil etadi;

huquqiy va siyosiy madaniyatga, amaliy ish tajribasiga kasbiy va pedagogik mahoratga ega yuqori malakali kadrlarni ta’lim jarayoniga keng jalb etish bo‘yicha choralarni ko‘radi, shuningdek, tegishli tashkilotlar bilan hamkorlikni amalga oshiradi;

o‘quv jarayonini ta’lim berishning kredit-modul tizimi va innovatsion o‘qitish usullarini qo‘llagan holda umume’tirof etilgan xalqaro ta’lim standartlari va talablariga muvofiq ishlab chiqilgan hamda talabalarda iqtisodiyotning tegishli sohalari bo‘yicha tizimli tahlil qilish qobiliyati va amaliy ko‘nikmalarni rivojlantirishga qaratilgan ta’lim dasturi asosida olib boradi;

talabalarning mustaqil tayyorgarligini chuqurlashtirishni hisobga olgan holda ish beruvchilar ehtiyojidan kelib chiqib, tahliliy fikrlash va kasbiy ko‘nikmalarni rivojlantirishga qaratilgan, o‘quv reja va dasturlar hamda o‘quv-metodik materiallarni o‘quv jarayonida qo‘llaydi;

o‘quv jarayonida axborot – kommunikatsiya texnologiyalarini keng qo‘llash, talabalar, o‘qituvchilar va yosh tadqiqotchilarni global axborot va ta’lim resurslaridan foydalanish imkoniyatlarini kengaytiradi;

professor o‘qituvchilar tarkibi mehnatni normallashtirishni faqat o‘quv tusdagi tadbirlarga asoslangan holda mustaqil amalga oshiradi hamda pedagogik xodimlar

tomonidan ilmiy-metodik, ilmiy tadqiqot, tashkiliy-metodik, ma’naviy-axloqiy va tarbiyaviy ishlarning bajarilishni rag‘batlantiradi;

universitet tomonidan o‘tkaziladigan tadqiqotlar natijalarini o‘quv rejalari va ta’lim dasturiga joriy etish uchun fanlarni o‘qitish sifati va darajasini oshirishga yo‘naltirilgan ilmiy va o‘quv–uslubiy materiallar ishlab chiqadi;

tizimli asosda pedagogik va ilmiy xodimlar malakasini oshirish va stajirovkadan o‘tkazish, ilmiy tadqiqotlar olib borish, ta’lim jarayoniga xorijiy mutaxassislarni jalb etish, shuningdek, talabalarning akademik almashinuvini ta’minlash bo‘yicha yetakchi xorijiy ilmiy ta’lim muassasalari, tahliliy, tadqiqot markazlari, xalqaro tashkilotlar bilan aloqani mustahkamlaydi;

ijobiy xalqaro tajribani kengroq qo‘llash, shu jumladan, talabalar o‘quv yuklamasi hajmini aniqlashning shartli birliklari (kreditlar) ni o‘tkazish va jamlash tizimini qo‘llaydi;

davlat va xo‘jalik boshqaruv organlari hamda boshqa tashkilotlar bilan birgalikda ilmiy-tadqiqot ishlarini tashkil etadi, ularning samaradorligini oshirish va tadqiqotlarning natijalarini amaliyotga keng joriy etish orqali fan-ta’lim-ishlab chiqarish integratsiyasini ta’minlaydi;

o‘qitishning kredit modul tizimini va talabalar bilimini baholash usullarini takomillashtirib, o‘quv jarayonida zamonaviy axborot kommunikatsiya texnologiyalarini keng qo‘llaydi hamda o‘quv bazasini takomillashtirib boradi;

rivojlangan xorijiy davlatlarning yetakchi ta’lim va ilmiy muassasalari bilan hamkorlikni, qo‘shma huquqiy tadqiqotlarni, professor-o‘qituvchilar va talabalar o‘zaro almashinuvini doimiy amalga oshirib boradi;

xorijiy hamkorlar bilan birgalikda kadrlarni tayyorlash bo‘yicha qo‘shma ta’lim dasturlarini (double degree) mustaqil amalga oshiradi, o‘quv-ta’lim jarayoniga xorijiy olimlar va mutaxassislarni faol jalb qiladi;

falsafa doktori (Doctor of Philosophy) va fan doktori (Doctor of Science) ilmiy darajalarini olish uchun dissertatsiya ishlarini zamonaviy talablar, iqtisodiyotning ustuvor yo‘nalishlariga muvofiqligini ta’minlash bo‘yicha tegishli chora-tadbirlar amalga oshiradi;

o‘z oldida turgan vazifalarini bajarish maqsadida zamonaviy o‘quv va moddiy texnik bazani yaratadi, o‘quv, ilmiy tadqiqot bo‘linmalari, kafedralarni o‘qitishning zamonaviy texnik vositalari, axborot kommunikatsiya tizimlari va dasturiy majmualar bilan ta’minlaydi;

O‘zbekiston Respublikasining ilmiy va ijodiy salohiyatini rivojlantirishga qodir mutaxassislarni tayyorlashda yuksak iste’dod sohiblariga bilimning tegishli sohalari va fanning aniq yo‘nalishlari bo‘yicha o‘z qobiliyatlarini namoyon etish hamda rivojlantirish, o‘zlaridagi noyob iste’dodni ro‘yobga chiqarish uchun imkoniyatlar yaratadi;

talabalarni jamiyatning to‘laqonli a’zosi, vatanparvar, vijdonan va halol mehnat qiluvchi, o‘z kasbining yetuk mutaxassisi bo‘lib yetishishi uchun kompleks chora-tadbirlarni amalga oshiradi;

talabalarning bo‘sh vaqtlarini mazmunli o‘tkazishlariga ko‘maklashish, ularda milliy g‘urur, vatanparvarlik va fidoyilik tuyg‘ularini shakllantirish choralarini ko‘radi;

ma’naviy, madaniy, milliy qadriyatlarni keng targ‘ib qilish, kitobxonlikni rivojlantirish, talabalarni milliy va jahon adabiyoti durdonalariga qiziqishini oshirish hamda dunyoqarashini shakllantirishga yo‘naltirilgan tadbirlarni amalga oshiradi;

universitet xalqaro reytingi va raqobatbardoshligini oshirish maqsadida chet el fuqarolari uchun ta’lim olish imkoniyatini kengaytiradi;

Axborot-resurs markazini huquqiy, ijtimoiy-siyosiy va iqtisodiy mazmundagi bosma va kitob mahsulotlari hamda o‘quv, ilmiy va boshqa adabiyotlar, jumladan, xorijiy adabiyotlar fondi, o‘qitishning texnik vositalari, shuningdek, global axborot-huquqiy va ta’lim resurslarini muntazam yangilab borishini ta’minlaydi.

Universitet o‘z vazifalari va funksiyalarini amalga oshirish uchun o‘z faoliyatida axborot-kommunikatsiya texnologiyalarini samarali joriy etadi va qo‘llaydi. Bunday sharoitda axborot xavfsizligini ta’minlash zarur vazifadir.

Axborot xavfsizligi axborotning konfidensialligi, yaxlitligi va foydalana olishligini saqlash, shuningdek, Universitet faoliyat yuritayotgan va joriy qilingan axborot resurslarining uzluksiz ishlashini ta’minlash nuqtai nazaridan ko‘rib chiqiladi. Axborot xavfsizligiga apparat, dasturiy ta’minot, amaliyot, jarayon va tashkiliy tuzilmalarni o‘z ichiga olgan bir qator chora-tadbirlarni joriy etish va amalga oshirish orqali erishiladi.

Axborot xavfsizligini ta’minlash bo‘yicha kompleks chora-tadbirlar Universitetning uzluksiz ishlashini, tahdidlarni amalga oshirish natijasida yetkaziladigan zararni minimallashtirishni, axborot-kommunikatsiya infratuzilmasini turli tahdidlardan himoya qilishni, ularning ta’sirini bashorat qilishni va oldini olishni, ishbilarmonlik obro‘sini va qonuniy talablarga muvofiqligini saqlashi lozim.

Universitetning axborot xavfsizligi siyosati uning axborot aktivlari va axborot-kommunikatsiya infratuzilmasini himoya qilishning asosiy tamoyillarini belgilaydi. U Universitet axborot xavfsizligini boshqarish tizimini boshqarish va qurish bo‘yicha tegishli hujjatlarni qabul qilish uchun asos bo‘lib xizmat qiladi. Ushbu Axborot xavfsizligi siyosati – Universitet o‘z faoliyatida rahbarlik qiladigan axborot xavfsizligi sohasidagi hujjatlashtirilgan yo‘riqnomalar, qoidalar, jarayonlar va vositalar to‘plamidir.

Mazkur Axborot xavfsizligi siyosati Oliy ta’lim, fan va innovatsiyalar vazirligi huzuridagi Raqamli ta’lim texnologiyalarini rivojlantirish markazi (2025-yil 01-iyundagi 05/101-son xat), O‘zbekiston Respublikasi Raqamli texnologiyalar vazirligi (2025-yil 21-avgustdagi 29-8/5931-son xat) hamda O‘zbekiston Respublikasi Davlat xavfsizlik xizmati bilan (2025-yil 23-sentabrdagi 5/1788-son xat) kelishilgan.

2. Me’yoriy hujjatlar

Axborot xavfsizligi siyosati quyidagi keltirilgan me’yoriy-huquqiy hujjatlarga asoslangan holda ishlab chiqilgan:

O‘zbekiston Respublikasining 2003-yil 11-dekabrdagi “Axborotlashtirish to‘g‘risida”gi O‘RQ-560-II-son Qonuni;

O‘zbekiston Respublikasining 2004-yil 29-apreldagi “Elektron hujjat aylanishi to‘g‘risida”gi O‘RQ-611-II-son Qonuni;

O‘zbekiston Respublikasining 2014-yil 11-sentabrdagi “Tijorat siri to‘g‘risida”gi O‘RQ-374-son Qonuni;

O‘zbekiston Respublikasining 2015-yil 9-dekabrdagi “Elektron hukumat to‘g‘risida”gi O‘RQ-395-son Qonuni;

O‘zbekiston Respublikasining 2019-yil 2-iyuldagi “Shaxsga doir ma’lumotlar to‘g‘risida”gi O‘RQ-547-son Qonuni;

O‘zbekiston Respublikasining 2022-yil 15-apreldagi “Kiberxavfsizlik to‘g‘risida”gi O‘RQ-764-son Qonuni;

O‘zbekiston Respublikasining 2022-yil 29-sentabrdagi “Elektron tijorat to‘g‘risida”gi O‘RQ-792-son Qonuni;

O‘zbekiston Respublikasining 2022-yil 12-oktabrdagi “Elektron raqamli imzo to‘g‘risida”gi O‘RQ-793-son Qonuni;

O‘zbekiston Respublikasi Prezidentining 2020-yil 15-iyundagi “O‘zbekiston Respublikasining axborot tizimlari va resurslarini himoya qilish davlat tizimini joriy etish chora-tadbirlari to‘g‘risida” PF-6007-son Farmoni;

O‘zbekiston Respublikasi Prezidentining 2020-yil 5-oktabrdagi “Raqamli O‘zbekiston – 2030” strategiyasini tasdiqlash va uni samarali amalga oshirish chora-tadbirlari to‘g‘risida” PF-6079-son Farmoni;

O‘zbekiston Respublikasi Prezidentining 2007-yil 3-apreldagi “O‘zbekiston Respublikasida axborotni kriptografik muhofaza qilishni tashkil etish chora-tadbirlari to‘g‘risida” PQ-614-son qarori;

O‘zbekiston Respublikasi Prezidentining 2011-yil 8-iyuldagi “Milliy axborot resurslarini muhofaza qilish bo‘yicha chora-tadbirlari to‘g‘risida” PQ-1572-son qarori;

O‘zbekiston Respublikasi Prezidentining 2018-yil 21-noyabrdagi “Axborot texnologiyalari va kommunikatsiyalarining joriy etilishini nazorat qilish, ularni himoya qilish tizimini takomillashtirish chora-tadbirlari to‘g‘risida” PQ-4024-son qarori;

O‘zbekiston Respublikasi Prezidentining 2019-yil 14-sentabrdagi “Axborot texnologiyalari va kommunikatsiyalarining joriy etilishini nazorat qilish, ularni himoya qilish tizimini takomillashtirishga oid qo‘shimcha chora-tadbirlar to‘g‘risida” PQ-4452-son qarori;

O‘zbekiston Respublikasi Prezidentining 2020-yil 15-iyundagi “O‘zbekiston Respublikasida kiberxavfsizlikni ta’minlash tizimini yanada takomillashtirish chora-tadbirlari to‘g‘risida” PQ-4751-son qarori;

O‘zbekiston Respublikasi Prezidentining 2023-yil 31-maydagi “O‘zbekiston Respublikasining muhim axborot infratuzilmasi obyektlari kiberxavfsizligini ta’minlash tizimini takomillashtirish bo‘yicha chora-tadbirlar to‘g‘risida” PQ-167-son qarori;

O‘zbekiston Respublikasi Prezidentining 2023-yil 3-iyuldagi “Ma’muriy islohotlar doirasida oliy ta’lim, fan va innovatsiyalar sohasida davlat boshqaruvini samarali tashkil qilish chora-tadbirlari to‘g‘risida” PQ-200-son qarori;

O‘zbekiston Respublikasi Vazirlar Mahkamasining 1999-yil 26-martdagi “O‘zbekiston Respublikasi axborot resurslarini tayyorlash va ularni ma’lumotlarni uzatish tarmoqlarida, shu jumladan, internetda tarqatish tartibi to‘g‘risidagi nizomni tasdiqlash to‘g‘risida” 137-son qarori;

O‘zbekiston Respublikasi Vazirlar Mahkamasining 2005-yil 22-noyabrdagi “Axborotlashtirish sohasida normativ-huquqiy bazani takomillashtirish to‘g‘risida” 256-son qarori;

O‘zbekiston Respublikasi Vazirlar Mahkamasining 2011-yil 4-maydagi “Vazirlar Mahkamasining ijro etuvchi apparatida, davlat va xo‘jalik boshqaruvi, mahalliy davlat hokimiyati organlarida yagona himoyalangan elektron pochtani va elektron hujjat aylanishi tizimini joriy etish hamda ulardan foydalanish chora-tadbirlari to‘g‘risida” 126-son qarori;

O‘zbekiston Respublikasi Vazirlar Mahkamasining 2011-yil 7-noyabrdagi “O‘zbekiston Respublikasi Prezidentining “Milliy axborot resurslarini muhofaza qilishga doir qo‘shimcha chora-tadbirlar to‘g‘risida” 2011-yil 8-iyuldagi PQ-1572-son qarorini amalga oshirish chora-tadbirlari haqida” 296-son qarori;

O‘zbekiston Respublikasi Vazirlar Mahkamasining 2013-yil 14-iyundagi “O‘zbekiston Respublikasi Prezidentining 2011-yil 8-iyuldagi “Milliy axborot resurslarini muhofaza qilish bo‘yicha chora-tadbirlari to‘g‘risida” PQ-1572-son qarorini amalga oshirish bo‘yicha qo‘shimcha chora-tadbirlari to‘g‘risida” 170-son qarori;

O‘zbekiston Respublikasi Vazirlar Mahkamasining 2015-yil 16-oktabrdagi “O‘zbekiston Respublikasi axborotlashtirish obyektlarida konfidensial axborot xavfsizligini tashkil etish va ta’minlash tartibi to‘g‘risidagi Nizomni tasdiqlash to‘g‘risida” 295-son qarori;

O‘zbekiston Respublikasi Vazirlar Mahkamasining 2021-yil 15-iyundagi “Raqamli iqtisodiyot va elektron hukumatning rivojlanish holatini reyting baholash tizimini yanada takomillashtirish chora-tadbirlari to‘g‘risida” 373-son qarori;

O‘zbekiston Respublikasi Bosh vazirining o‘rinbosari – Davlat sirlarini saqlash bo‘yicha idoralararo komissiya raisi tomonidan 2006-yil 5-dekabrda tasdiqlangan-tarqatilishi cheklangan ma’lumotlarga ega hujjatlar, fayllar va nashrlarni ro‘yxatga olish, ishlov berish va saqlash tartibi to‘g‘risidagi yo‘riqnoma;

O‘zbekiston Respublikasi Adliya vazirligida 2023 yil 22-sentabrda 3458-son bilan ro‘yxatga olingan O‘zbekiston Respublikasi davlat xavfsizlik xizmati raisining 2023 yil 4-sentabrdagi “O‘zbekiston Respublikasi kiberxavfsizlik va muhim axborot infratuzilmasi obyektlarining kiberxavfsizligini ta’minlash darajasini baholash tartibi to‘g‘risidagi nizomni tasdiqlash haqida” 91-son buyrug‘i;

O‘zbekiston Respublikasi Adliya vazirligida 2024 yil 14 noyabrda 3573-son bilan ro‘yxatga olingan O‘zbekiston Respublikasi Davlat xavfsizlik xizmati Raisining 2024 yil 15-oktabrdagi “Kiberxavfsizlik talablariga muvofiqlik yuzasidan ekspertizadan o‘tkazish tartibi to‘g‘risidagi nizomni tasdiqlash haqida”gi 113-son buyrug‘i;

O‘zbekiston Respublikasi Adliya vazirligida 2024 yil 14-noyabrda 3574-son bilan ro‘yxatga olingan O‘zbekiston Respublikasi Davlat xavfsizlik xizmati Raisining 2024 yil 15-oktabrdagi “Axborot tizimlari va resurslarining kiberxavfsizligini ta’minlash uchun qo‘llaniladigan apparat, apparat-dasturiy hamda dasturiy vositalarni sertifikatlashtirish tartibi to‘g‘risidagi nizomni tasdiqlash haqida”gi 114-son buyrug‘i;

O‘zbekiston Respublikasi Adliya vazirligida 2024 yil 14 noyabrda 3570-son bilan ro‘yxatga olingan O‘zbekiston Respublikasi Davlat xavfsizlik xizmati Raisining 2024 yil 24-oktabrdagi “O‘zbekiston Respublikasi muhim axborot infratuzilmasi obyektlarini toifalash va ularning yagona reestrini shakllantirish tartibi to‘g‘risidagi vaqtinchalik nizomni tasdiqlash haqida”gi 118-son buyrug‘i;

O‘z DSt ISO/IEC 13335-1:2009 “Axborot texnologiyalari. Xavfsizlikni ta’minlash usullari. Axborot va kommunikatsiya texnologiyalari xavfsizligini boshqarish. (1-qism). Axborot va kommunikatsiya texnologiyalari xavfsizligini boshqarish konsepsiyasi va modellari”;

O‘z DSt 2590:2012 “Axborot texnologiyasi. Milliy axborot tizimini shakllantirish doirasida davlat organlari tomonidan foydalaniladigan axborot tizimlari integratsiyasiga va o‘zaro faoliyatiga qo‘yiladigan talablar”;

O‘z DSt 1109:2013 “Axborot texnologiyasi. Axborotning kriptografik himoyasi. Atamalar va ta’riflar”;

O‘zMSt ISO/IEC 27005:2024 “Axborot texnologiyalari. Xavfsizlikni ta’minlash usullari. Axborot xavfsizligi risklarini boshqarish”;

O‘z DSt ISO/IEC 27011:2014 “Axborot texnologiyalari. Xavfsizlikni ta’minlash usullari. Telekommunikatsiya tashkilotlarida axborot xavfsizligini boshqarish bo‘yicha rahbariy ko‘rsatmalar”;

O‘z DSt 2814:2014 “Axborot texnologiyasi. Avtomatlashtirilgan tizimlar. Axborotdan ruxsatsiz foydalana olishdan muhofazalanganlik darajalari bo‘yicha tasniflash”;

O‘z DSt 2815:2014 “Axborot texnologiyasi. Tarmoqlararo ekranlar. Axborotdan ruxsatsiz foydalana olishdan muhofazalanganlik darajalari bo‘yicha tasniflash”;

O‘z DSt 2816:2014 “Axborot texnologiyasi. Axborotni muhofaza qilish vositalarining dasturiy ta’minotini deklaratsiya qilinmagan imkoniyatlar yo‘qligini nazorat qilish darajasi bo‘yicha tasniflash”;

O‘z DSt 2817:2014 “Axborot texnologiyasi. Hisoblash texnikasi vositalari. Axborotdan ruxsatsiz foydalana olishdan muhofazalanganlik darajalari bo‘yicha tasniflash”;

O‘z DSt 2875:2014 “Datamarkazlar uchun talablar”. “Infratuzilma va axborot xavfsizligini ta’minlash” standartidagi telekommunikatsiya obyektlari infratuzilmasining tayyorligi va xavfsizligini ta’minlash;

O‘z DSt ISO/IEC 27010:2015 “Axborot texnologiyalari. Xavfsizlikni ta’minlash usullari. Sohalararo va tashkilotlararo kommunikatsiyalarda axborot xavfsizligini boshqarish bo‘yicha qo‘llanma”;

O‘z DSt 2927:2015 “Axborot texnologiyalari. Axborot xavfsizligi. Atamalar va ta’riflar”;

O‘z DSt ISO/IEC 15408-1:2016 “Axborot texnologiyalari. Xavfsizlikni ta’minlash usullari. Axborot texnologiyalarining xavfsizligini baholash mezonlari. (1-qism). Kirish va umumiy model”;

O‘z DSt ISO/IEC 15408-2:2016 “Axborot texnologiyasi. Xavfsizlikni ta’minlash usullari. Axborot texnologiyalarining xavfsizligini baholash mezonlari. (2-qism). Xavfsizlikning funksional komponentlari”;

O‘z DSt ISO/IEC 15408-3:2016 “Axborot texnologiyasi. Xavfsizlikni ta’minlash usullari. Axborot texnologiyalarining xavfsizligini baholash mezonlari. (3-qism). Xavfsizlikka qo‘yiladigan ishonch komponentlari”;

O‘zMSt ISO/IEC 27002:2024 “Axborot texnologiyasi. Xavfsizlikni ta’minlash usullari. Axborot xavfsizligini boshqarishning amaliy qoidalari”;

O‘z DSt ISO/IEC 27031:2016 “Axborot texnologiyasi. Xavfsizlikni ta’minlash usullari. Biznes uzluksizligini ta’minlashga axborot texnologiyalarini tayyorligi bo‘yicha rahbariy ko‘rsatmalar”;

O‘z DSt ISO/IEC 27033-1:2016 “Axborot texnologiyasi. Xavfsizlikni ta’minlash usullari. Tarmoq xavfsizligi. 1-qism”;

O‘z DSt ISO/IEC 27033-1:2016 “Axborot texnologiyasi. Xavfsizlikni ta’minlash usullari. Tarmoq xavfsizligi. 4-qism. Xavfsizlik shlyuzlaridan foydalangan holda tarmoqlar o‘rtasida xavfsizlikni ta’minlash”;

O‘z DSt ISO/IEC 27033-2:2016 “Axborot texnologiyasi. Xavfsizlikni ta’minlash usullari. Tarmoq xavfsizligi. 2-qism. Tarmoq xavfsizligini loyihalashtirish va joriy etish bo‘yicha rahbariy ko‘rsatmalar”;

O‘z DSt ISO/IEC 27033-5:2016 “Axborot texnologiyasi. Xavfsizlikni ta’minlash usullari. Tarmoq xavfsizligi. 5-qism. “Virtual xususiy tarmoqlarni qo‘llagan holda tarmoqlararo xavfsizligini ta’minlash uchun kommunikatsiyalar”;

O‘z DSt 3078:2016 “Telekommunikatsiyalar tarmoqlari. Virtual xususiy tarmoqlar *(VPN)*. Umumiy talablar”;

O‘z DSt ISO/IEC 27032:2017 “Axborot texnologiyasi. Xavfsizlikni ta’minlash usullari. Kiberxavfsizlik bo‘yicha rahbariy ko‘rsatmalar”;

O‘z DSt 3243:2017 “Axborot texnologiyasi. Lokal va korporativ hisoblash tarmoqlari. Umumiy texnik talablar”;

O‘z DSt 1047:2018 “Axborot texnologiyasi. Atamalar va ta’riflar”;

O‘z DSt ISO/IEC 27014:2018 “Axborot texnologiyasi. Xavfsizlikni ta’minlash usullari. Axborot xavfsizligini korporativ boshqarish”;

O‘z DSt 3386:2019 (O‘z DSt ISO/IEC 27035-1:2016; MOD) “Axborot texnologiyasi. Xavfsizlikni ta’minlash usullari. Axborot xavfsizligi insidentlarini boshqarish. l-qism, Insidentlarni boshqarish prinsiplari”;

O‘z DSt 3387:2019 (O‘z DSt ISO/IEC 27035-2:2016; MOD) “Axborot texnologiyasi. Xavfsizlikni ta’minlash usullari. Axborot xavfsizligi insidentlarini boshqarish. 2-qism. Insidentlarga ta’sir etishni rejalashtirish va unga tayyorlanish bo‘yicha rahbariy ko‘rsatmalar”;

O‘z DSt ISO/IEC 27001:2020 “Axborot texnologiyasi. Xavfsizlikni ta’minlash usullari. Axborot xavfsizligini boshqarish tizimlari. Talablar”;

O‘z DSt ISO/IEC 27000:2022 “Axborot texnologiyasi. Xavfsizlikni ta’minlash usullari. Axborot xavfsizligini boshqarish tizimlari. Sharh va lug‘at”;

O‘z DSt ISO/IEC 27003:2022“Axborot texnologiyasi. Xavfsizlikni ta’minlash usullari. Axborot xavfsizligini boshqarish tizimini joriy etish bo‘yicha qo‘llanma”;

O‘z DSt ISO/IEC 27007:2022 “Axborot texnologiyalari. Xavfsizlikni ta’minlash usullari. Axborot xavfsizligini boshqarish tizimlarini audit o‘tkazish bo‘yicha rahbariy ko‘rsatmalar”;

O‘z DSt ISO/IEC 27008:2022 “Axborot texnologiyasi. Xavfsizlikni ta’minlash usullari. Axborot xavfsizligini boshqarish bo‘yicha auditorlar uchun qo‘llanma”;

O‘zMSt 285:2024 “Axborot texnologiyasi. Axborotni kriptografik muhofazasi. Xeshlash funksiyasi”;

O‘zMSt 286:2024 “Axborot texnologiyasi. Axborotning kriptografik muhofazasi. Elektron raqamli imzoni shakllantirish va tekshirish jarayonlari”;

RH 45-015:2016 “Tashkiliy-farmoyish hujjatlarini rasmiylashtirish tartibi”;

O‘zbekiston Respublikasi hududida axborot xavfsizligi siyosatini ishlab chiqish bo‘yicha uslubiy qo‘llanma (*2016-yil 23-fevraldagi 7-sonli 2013-2020-yillarda O‘zbekiston Respublikasi Milliy axborot-kommunikatsiya tizimini rivojlantirishni muvofiqlashtirish bo‘yicha Respublika Komissiyasi bayonnomasiga 10-ilova; keyingi – o‘rinlarda Uslubiy qo‘llanma*);

O‘zbekiston Respublikasi Raqamli texnologiyalar vazirligi hamda davlat va xo‘jalik boshqaruvi organlari o‘rtasida axborot xavfsizligi insidentlariga javob berish, o‘rganish va oldini olish bo‘yicha o‘zaro hamkorlik reglamenti *(O‘zbekiston Respublikasi Axborot va kommunikatsiya xavfsizligi texnik kengashining 2017-yil 17-noyabrdagi 7-son bayonnomasiga 1-ilova, keyingi o‘rinlarda – Hamkorlik reglamenti);*

Davlat va xo‘jalik boshqaruvi organlari, mahalliy davlat hokimiyati organlarida axborot xavfsizligini ta’minlashga qo‘yiladigan talablar” *(O‘zbekiston Respublikasi Axborot va kommunikatsiya xavfsizligi bo‘yicha texnik kengashning 2017-yil 17-noyabrdagi 7-sonli bayonnomasiga 2-ilova, keyingi o‘rinlarda – Talablar).*

Universitetning axborot xavfsizligi bo‘yicha ichki hujjatlari:

- Universitetning 2023-yil 18-apreldagi “Buxoro davlat universitetida axborot-kommunikatsiya texnologiyalarini keng joriy etish va raqamlashtirish jarayonlarini yanada jadallashtirish to‘g‘risida” 177-U-son buyrug‘i;

- Universitetning 2023-yil 6-maydagi “Buxoro davlat universitetida konfidensial ma’lumotlarga ega hujjatlarni muhofaza qilish, ular bilan ishlashni to‘g‘ri tashkil etish to‘g‘risida” 208-U-son buyrug‘i;

- Universitetning 2023-yil 23-avgustdagi “Ma’naviy-ma’rifiy, tarbiyaviy va sport sohasidagi ishlarni yanada takomillashtirish to‘g‘risida”gi 420 U son buyrug‘i asosida ishlab chiqilgan universitetning “Odob-axloq kodeksi”.

3. Atamalar va ta’riflar

3.1 Mazkur hujjatda O‘z DSt 2927:2015 “Axborot texnologiyalari. Axborot xavfsizligi. Atamalar va ta’riflar” va O‘z DSt 1047:2018 “Axborot texnologiyalari. Atamalar va ta’riflar” davlat standartiga muvofiq quyidagi atamalar va ta’riflardan

foydalanilgan:

3.1.1 **avtorizatsiya** – foydalanuvchining foydalana olish huquqlarini tekshirish va unga berilgan huquqlarga muvofiq resurslardan foydalana olishga ruxsat olish;

3.1.2 **Active Directory** – ruxsatlar va tarmoqqa kirishni boshqarish uchun Microsoft Windows Serverning katalog xizmati;

3.1.3 **anonimayzer** – veb-saytlarga, tarmoqlarga yoki internet xizmatlariga murojaat qilayotgan foydalanuvchilar uchun xavfsizlikni oshirish maqsadida ishlatiladi;

3.1.3 **autentifikatsiya** – foydalanuvchi (tarmoq abonenti, xabar jo‘natuvchi), dastur, qurilma yoki ma’lumotlarning (axborot, olinadigan xabar, kalit) haqiqiyligini belgilash jarayoni;

3.1.4 **axborot** – 1) manbalaridan va taqdim etish shaklidan qat’i nazar, shaxslar, predmetlar, faktlar, voqealar, hodisalar va jarayonlar to‘g‘risidagi ma’lumotlar; 2) qiziqish uyg‘otadigan va saqlanishi, qayta ishlanishi lozim bo‘lgan bilimlar, faktlar, ma’lumotlar jami;

3.1.5 **axborot xavfsizligi** – 1) axborotlarning axborot egasiga zarar yetkazuvchi tasodifiy yoki qasddan qilinadigan ta’sirlar (tahdidlar)ga qarshi tura olish integral xususiyati; 2) hisoblash texnikasi yoki avtomatlashtirilgan tizim vositalari tomonidan qayta ishlanadigan axborotning ichki va tashqi tahdidlardan muhofazalanganlik holati;

3.1.6 **axborot resurslari** – axborot tizimi tarkibidagi elektron shakldagi axborotlar, ma’lumotlar banklari, ma’lumotlar bazasi;

3.1.7 **axborotni muhofaza qilish** – axborot egasi manfaatlariga zarar keltirilishining oldini olish yoki qiyinlashtirishga qaratilgan huquqiy, tashkiliy va texnik (apparat-dasturiy) tadbirlar kompleksi;

3.1.8 **axborotni kriptografik muhofaza qilish vositasi** – axborot xavfsizligini ta’minlash uchun axborotning kriptografik almashtirilishini amalga oshiradigan apparat, dasturiy yoki apparat-dasturiy vositalar;

3.1.9 **axborot tizimi** – axborotlarni yig‘ish, saqlash, izlash, ishlash va ulardan foydalanish imkonini beruvchi axborot resurslari, axborot texnologiyalari va aloqa vositalarining tashkiliy tartibga solingan yig‘indisi;

3.1.10 **axborot tizimining xavfsizligi** – axborot tizimining, uning normal ishlash rejimiga ruxsat etilmagan aralashuvdan, shuningdek, tizim komponentlarini o‘g‘irlash, noqonuniy o‘zgartirish yoki buzishdan muhofaza qilinganligi;

3.1.11 **axborotlashtirish obyekti** – turli daraja va maqsadlardagi axborot tizimlari, telekommunikatsiya tarmoqlari, axborotni qayta ishlash texnik vositalari, bu vositalar o‘rnatilgan va ekspluatatsiya qilinadigan, shuningdek, muzokaralar, shu jumladan, konfidensial muzokaralar olib borish uchun mo‘ljallangan alohida xonalar;

3.1.12 **axborot xavfsizligi siyosati** – axborot xavfsizligini boshqarish tizimi, obyektlari va ishtirokchilarining faoliyat turlarini belgilaydigan va cheklaydigan qoidalar to‘plami;

3.1.13 **axborot xavfsizligini boshqarish tizimi** – axborot xavfsizligini ishlab chiqish, joriy qilish, uning ishlashi, monitoringi, tahlili, unga xizmat ko‘rsatish va uni takomillashtirish uchun mo‘ljallangan biznes risklarni baholash usullaridan foydalanishga asoslangan umumiy boshqarish tizimining qismi;

3.1.14 **axborot xavfsizligi buzg‘unchisi (buzg‘unchi)** – tizim resurslaridan ruxsat etilmagan tarzda foydalana olishga (bu resurs bilan ishlashda uning uchun taqiqlangan harakatlarni bajarishga urinish) xato, bilmaslik oqibatida yoki yovuz niyatda (o‘z manfaatlari yo‘lida) yoki shunchaki (o‘yin yoki o‘zini namoyon qilish maqsadida) uringan (urinib ko‘rgan) va buning uchun turli xil imkoniyatlar, metodlar va vositalardan foydalangan shaxs (subyekt);

3.1.15 **axborot xavfsizligi buzg‘unchisi modeli** – foydalana olishni chegaralash qoidalarini buzuvchining abstrakt tavsifi;

3.1.16 **axborot xavfsizligiga tahdidlar modeli** – axborot xavfsizligi mavjud tahdidlarining, ularning aktualligi, amalga oshirish imkoniyatlari va oqibatlarining tavsifi;

3.1.17 **axborot xavfsizligi riski (risk)** – muayyan xavfni amalga oshirishda, ma’lumotlarni qayta ishlash tizimining muayyan zaifligidan foydalanish imkoniyati;

3.1.18 **axborotning zaifligi** – axborotning konfidensialligi, yaxlitligi, undan erkin foydalanish mumkinligi buzilishiga va uni noqonuniy tarzda ko‘paytirilishiga olib kelishi mumkin bo‘lgan turli beqarorlashtiruvchi omillar ta’siriga moyilligi;

3.1.19 **buzg‘unchi** – axborot tizimi va uning resurslaridan ruxsat etilmagan tarzda foydalana olishdan manfaatdor bo‘lgan va ularni ruxsatsiz olish yoki o‘zgartirish uchun oldindan o‘ylab harakat qilgan shaxs yoki tashkilot;

3.1.20 **dasturiy ta’minot** – ma’lumotlarni qayta ishlash tizimi va dasturiy hujjatlarni ishlatish zarur bo‘lgan dasturlar to‘plami;

3.1.21 **elektron raqamli imzo** – elektron hujjatdagi mazkur elektron hujjat axborotini elektron raqamli imzoning yopiq kalitidan foydalangan holda maxsus o‘zgarishlar natijasida hosil qilingan hamda elektron raqamli imzoning ochiq kaliti yordamida elektron hujjatdagi axborotda xatolik mavjud emasligini aniqlash va elektron raqamli imzo kalitining egasini identifikatsiya qilish imkonini beradigan imzo;

3.1.22 **elektron pochta** – tarmoqlar orqali xabarlarning foydalanuvchidan foydalanuvchiga yuborilishini, shuningdek, bu xabarni o‘qish va saqlash imkonini beradigan servis dasturlar tizimi;

3.1.23 file-server – lokal tarmoqda ma’lumotlarni saqlash va ularga murojaat qilish imkoniyatini ta’minlaydigan server turi;

3.1.24 flesh-xotira – kompyuter uchun tashqi axborot va ma’lumotlarni tashuvchi qurilma turi;

3.1.25 **foydalana olishlik** – axborot va uning tashuvchisining holati, unda foydalanuvchilar tomonidan ular uchun mo‘ljallangan axborotning hech qanday qarshiliksiz va o‘z vaqtida olinishi ta’minlanadi;

3.1.26 **foydalana olinishi cheklangan axborot** – davlat sirlari va konfidensial axborotdan iborat ma’lumotlarga ega bo‘lgan hujjatlashtirilgan axborot, ulardan foydalana olish qonun hujjatlariga muvofiq chegaralanadi;

3.1.27 **hujum** – xavfsizlikni ta’minlash mexanizmlarini chetlab o‘tish maqsadida yoki ularning kamchiliklaridan foydalanish maqsadida qo‘llaniladigan harakatlar;

3.1.28 **internet tarmog‘i** – standart ochiq protokollar orqali axborot almashinish uchun o‘zaro birlashtirilgan mustaqil kompyuter tarmoqlarining global (Butunjahon) ko‘prigi;

3.1.29 **jismoniy tahdid** – amalga oshirish oqibatida butun tizimga fizik zarar bo‘lib hisoblangan tahdid;

3.1.30 **kalit** – shifrlash va deshifrlash amallarini boshqaruvchi simvollar ketma-ketligi;

3.1.31 **konfidensiallik** – axborot va uning tashuvchisining holati, bunda u bilan ruxsat etilmagan tarzda tanishishning yoki ruxsat etilmagan tarzda hujjatlashtirish (nusxa ko‘chirish)ning oldini olish ta’minlanadi;

3.1.32 **konfidensial axborot** – Davlat sirlaridan iborat ma’lumotlarga ega bo‘lmagan hujjatlashtirilgan axborot, undan foydalanish qonun hujjatlariga muvofiq chegaralanadi;

3.1.33 **konfidensiallik belgisi** – obyektda mavjud bo‘lgan axborotning konfidensialligini tavsiflovchi axborot elementi;

3.1.34 **log-fayl** – serverning ishlashi haqidagi tizim ma’lumotlari va foydalanuvchi harakatlari haqidagi ma’lumotlarni o‘z ichiga olgan fayl;

3.1.35 **lokal hisoblash tarmog‘i** – bitta bino yoki bitta korxona bilan cheklangan bitta lokal hududda qator hisoblash texnikasi qurilmalarini bog‘laydigan axborot-hisoblash tarmog‘i;

3.1.36 **ma’lumotlar bazasi** – obyektiv shaklda ifodalangan va bu ma’lumotlar elektron hisoblash mashinalari yordamida topiladigan va qayta ishlanadigan tarzda tizimlashtirilgan ma’lumotlar (moddalar, hisob-kitoblar) jami;

3.1.37 **nazorat qilinadigan hudud** – doimiy yoki bir martalik ruxsati bo‘lmagan begona shaxslar va transport vositalarining nazoratsiz bo‘lishi taqiqlangan joy *(hudud, bino, binoning bir qismi)*;

3.1.38 **Need-To-Know** – “Bilish kerak” tamoyili axborot xavfsizligi va foydalanishni boshqarishda asosiy tushuncha bo‘lib, foydalanuvchilarga faqat o‘zlarining muayyan ish vazifalarini yoki vazifalarini bajarishlari uchun zarur bo‘lgan ma’lumotlar yoki resurslardangina foydalanish imkoniyati berilishi;

3.1.39 **operatsion tizim** – kompyuter va boshqa avtomatlashtirilgan qurilmalarda, jumladan smartfonlarda, planshetlarda, noutbuklarda, serverlarda va boshqa qurilmalarda ishlovchi dasturlarning ishlashi uchun mo‘ljallangan dasturiy ta’minot (Windows, macOS, Linux, Android, iOS va boshqalar). Operatsion tizim qurilma va dasturlarning to‘g‘ri ishlashini boshqarib turadi hamda foydalanuvchi va qurilma o‘rtasidagi aloqani ta’minlaydi;

3.1.40 **parol** – shaxsning, o‘zini axborot kommunikatsiya tizimiga tanishtirish jarayonida qo‘llaniladigan belgilar ketma-ketligi bo‘lib, axborot kommunikatsiya tizimidan foydalanish huquqiga ega bo‘lish uchun foydalaniluvchining konfidensial bo‘lmagan qayd yozuvi hisoblanadi;

3.1.41 **parol bilan himoya qilish** – tizimga va uning resurslariga parollar orqali kirish jarayonini boshqarish;

3.1.42 **parol kompрometatsiyasi** – parolning sir saqlanmasligi, oshkor qilinishi;

3.1.43 **qayd yozuvi** – axborot tizimlari va manbalariga kirishda foydalaniladigan foydalanuvchi identifikatori;

3.1.44 **risk** – muayyan xavfni amalga oshirishda, ma’lumotlarni qayta ishlash tizimining muayyan zaifligidan foydalanish imkoniyati (ehtimoliy xavf);

3.1.45 **risklarni boshqarish** – riskka nisbatan va uni boshqarish bo‘yicha muvofiqlashtirilgan faoliyat;

3.1.46 **risklarni baholash** – risk mohiyatini aniqlash maqsadida bajariladigan, hisoblangan risk va risk mezonlarini taqqoslash jarayoni;

3.1.47 **server** – kompyuterga, boshqa bir kompyuterga xizmat ko‘rsatish imkonini beradigan apparat va dasturiy ta’minot yig‘indisi;

3.1.48 **spam-filtr** – elektron pochta xizmatlarida, foydalanuvchilarga elektron pochta orqali yuboriladigan xabarlar orasidan zararli xabarlarni aniqlash va ajratib olish uchun ishlatiladi;

3.1.49 **Spin-off** – bir kompaniyaning bir qismi (filiali yoki bo‘limi) sifatida ajralib chiqib yangi, mustaqil korxona tashkil etilishi;

3.1.50 **shaxsga doir ma’lumotlar** – muayyan jismoniy shaxsga taalluqli bo‘lgan yoki uni identifikatsiya qilish imkonini beradigan, elektron tarzda, qog‘ozda va (yoki) boshqa moddiy jismda qayd etilgan axborot;

3.1.51 **tahdidlar modeli** – axborot xavfsizligi tahdidlari xarakteristikalari yoki xususiyatlarining fizik, matematik, tavsifiy taqdim etilishi;

3.1.52 **uchinchi shaxs** – subyekt, mulkdor va (yoki) operator bo‘lmagan, ammo shaxsga doir ma’lumotlarga ishlov berish bo‘yicha holatlar yoki munosabatlar orqali ular bilan bog‘liq bo‘lgan har qanday shaxs;

3.1.53 **vakolat** – obyektni yoki obyektlar klassini identifikatsiya qilishni va ushbu obyektlardan foydalanishning barcha ruxsat etilgan turlarini taqdim etish;

3.1.54 **vakolatli organ** – O‘zbekiston Respublikasi Davlat xavfsizlik xizmati;

3.1.55 **virtual xususiy tarmoq** – tarmoq kanal ustidan shifrlash va tunnellash protokollaridan foydalanadigan muhofazalangan tarmoq bog‘lanish. Virtual xususiy tarmoqni (VPN), korporativ Wi-Fi tarmoqlardan farqli ravishda, foydalanuvchilarning tarmoqqa ulanishini maksimal osonlashtirish uchun shifrlashga ega bo‘lmagan muhofazalanmagan Wi-Fi bog‘lanish ustidan amalga oshirish mumkin;

3.1.56 **virusga qarshi dastur** – viruslarni aniqlash uchun mo‘ljallangan va ularni yo‘q qilish taklifini berishi mumkin bo‘lgan yoki yo‘q qiluvchi dastur;

3.1.57 **xavfsizlik** – obyektning tasodifiy va qasddan qilinadigan tahdidlar ta’siriga qarshi tura olish qobiliyati;

3.1.58 **yaxlitlik** – axborot va uning tashuvchisining holati bo‘lib, bunda umuman va uning alohida tarkibiy qismlarining bo‘linmasligi va ruxsat etilmagan tarzda yoki qasddan yo‘q qilinishi, buzilishi, chiqib ketishi, o‘g‘irlanishi, qalbakilashtirilishining oldini olish ta’minlanadi;

3.1.59 **zaiflik** – ma’lumotlarni qayta ishlash tizimidagi kamchilik, undan foydalanish uning yaxlitligini buzishi va noto‘g‘ri ishlashiga olib kelishi mumkin;

3.1.60 **zarar** – obro‘sizlantirish natijasida yuzaga kelgan zarar yoki ziyonning moddiy o‘lchami.

4. Belgilar va qisqartmalar

4.1 Ushbu Axborot xavfsizligi siyosatida (keyingi o‘rinlarda – Siyosat) quyidagi belgilar va qisqartmalardan foydalanilgan:

AKT – axborot-kommunikatsiya texnologiyalari;

AKHV – axborotlarni kriptografik himoyalash vositalaridan;

AXBT – axborot xavfsizligini boshqarish tizimi;

BD (Blu-ray Disk) – optik disk;

DDoS (Distributed Denial-of-Service) – xizmat ko‘rsatishni taqsimlangan rad etish;

DHCP (Dynamic Host Configuration Protocol) – tarmoq ichidagi IP-manzillarni tarqatish uchun tez va avtomatik markaziy boshqaruvni ta’minlash uchun foydalaniladigan protokol;

DLP (Data Loss Prevention) – ma’lumotlar sizib chiqishini oldini olish tizimi;

DoS (Denial-of-Service) – xizmat ko‘rsatishni rad etish;

DUK – davlat unitar korxonasi;

DVD (Digital Versatile Disc) – raqamli ko‘p qirrali disk;

ERI – elektron raqamli imzo;

HTTP (HyperText Transfer Protocol) – veb-saytlar orqali ma’lumot almashuvini boshqarish uchun ishlatiladigan protokol;

HTTPS (HyperText Transfer Protocol Secure) – veb-saytlar orasidagi ma’lumot almashuvi uchun ishlatiladigan xavfsizlikni ta’minlovchi protokol;

IDPS (Intrusion Detection & Prevention System) – hujumlarni aniqlash va bartaraf etish tizimi;

LDAP (Lightweight Directory Access Protocol) – iyerarxik katalog tuzilmasidan ma’lumotlarni saqlash va olish uchun ishlatiladigan ochiq protokol;

MB – ma’lumotlar bazasi;

MBBT– ma’lumotlar bazasini boshqarish tizimi;

MCHJ – mas’uliyati cheklangan jamiyat;

NAT (Network Address Translation) – tarmoq manzili tarjimoni;

SIEM (Security information and event management) – axborot xavfsizligi hodisalarini boshqarish tizimidan;

SSH (Secure Shell) – xavfsiz tarmoq orqali masofaviy qurilmalar yoki serverlarga kirish va boshqarishning xavfsiz usulini ta’minlovchi tarmoq protokoli;

SSL/TLS (Secure Sockets Layer/Transport Layer Security) – kriptografik protokollar bo‘lib, ular lokal va korporativ tarmoq, asosan internet orqali xavfsiz aloqani ta’minlaydi;

URL (Uniform Resource Locator) – internetdagi manbalarni, veb-saytlarni yoki boshqa onlayn resurslarni aniqlash uchun ishlatiladigan unikal manba (manzil) turi;

USB (Universal Serial Bus) – ish stansiyasini qo‘shimcha qurilmalar bilan bog‘lovchi tizim;

VPN (Virtual private network) – virtual xususiy tarmoq;

XDFU – xizmat doirasida foydalanish uchun;

CD (Compact disc) – kompakt disk;

Wi-Fi (Wireless Fidelity) – qurilmalarni lokal tarmoqqa ulash uchun ishlatiladigan simsiz aloqa standartlari to‘plami.

5. Foydalanish sohasi

5.1 Mazkur Siyosat Universitetda axborot xavfsizligini ta’minlash masalasida Universitetning harakatlarni rejalashtirish tizimini, axborot xavfsizligi sohasidagi maqsad va vazifalarni, qoidalarni, ko‘rsatmalarni, shuningdek, Universitet tomonidan o‘z faoliyatida qo‘llaniladigan boshqa asosiy tamoyillarni, axborot xavfsizligining tashkiliy, texnologik jihatlarini shakllantirishning asosiy tamoyillarini belgilaydi.

5.2 Siyosat Universitet axborot texnologiyalarini rivojlantirishning hozirgi holati va yaqin istiqbollari, maqsadlari, vazifalari va ularni ishlashining huquqiy asoslarini, ishlash rejimlarini hisobga oladi shuningdek, himoya obyektlari xavfsizligiga tahdidlar tahlilini o‘z ichiga oladi.

5.3 Siyosat Universitet tuzilmalarida integratsiyalashgan AXBT qurish uchun asos sifatida foydalanilishi lozim.

5.4 Universitet axborot xavfsizligi siyosatining talablari Universitet va uning barcha tarkibiy bo‘linmalari tomonidan bajarilishi shart, ularga quyidagilar kiradi:

1) Universitet bosh binosi (manzil: Buxoro viloyati, Buxoro shahri, M. Iqbol ko‘chasi, 11-uy) hududida joylashgan axborotlashtirish obyektlari:

- Fizika-matematika va axborot texnologiyalari fakulteti
- Jismoniy tarbiya va sport fakulteti
- Iqtisodiyot va turizm fakulteti
- San’atshunoslik va pedagogika fakulteti
- Tarix va yuridik fakulteti
- Kompyuter markazi
- Ilmiy amaliy muzey
- Axborot resurs markazi

2) Filologiya fakulteti (manzil: Buxoro viloyati, Buxoro shahri, Alpomish ko‘chasi, 1-uy)

3) Xorijiy tillar fakulteti (manzil: Buxoro viloyati, Buxoro shahri, Hamza ko‘chasi, 16-uy)

4) Tabiiy fanlar va agrobiotexnologiya fakulteti (manzil: Buxoro viloyati, Buxoro tumani, Rabotiqalmoq MFY)

5) Sirtqi (maxsus sirtqi) va masofaviy ta’lim bo‘limi binosidagi (manzil: Buxoro viloyati, G‘ijduvon tumani, Soktare MFY)

6) Maktabgacha ta’lim innovatsion klasteri (manzil: Buxoro viloyati, Buxoro tumani, Gala Osiyo shaharchasi, Do‘stlik MFY);

7) 7-sonli talabalar turar joyi binosidagi (manzil: Buxoro viloyati, Buxoro shahri, B. Naqshband ko‘chasi, 158-uy).

5.5 Universitet tashkiliy tuzilmasidagi quyidagi tashkilotlar o‘z axborot infratuzilmalaridan kelib chiqqan holda o‘zlarining axborot xavfsizligi siyosatini Universitetning ushbu Siyosatiga asoslangan holda ishlab chiqadilar va Universitet Raqamli ta’lim texnologiyalari departamenti bilan kelishadilar:

- Pedagog kadrlarni qayta tayyorlash va ularning malakasini oshirish mintaqaviy markazi;

- Buxoro davlat universiteti Qorako‘l akademik litseyi.

5.6 Raqamli ta’lim texnologiyalari departamenti (keyingi o‘rinlarda – Departament) Universitetning barcha axborot tizimlariga xizmat ko‘rsatadi, rivojlantiradi hamda axborot va kiberxavfsizligini ta’minlaydi. Shuningdek, Siyosatning 5.5-bandida keltirilgan Universitetning tashkiliy tuzilmasiga kiruvchi davlat muassasalari hamda tashkilotlarning Siyosatini ishlab chiqishda O‘zbekiston Respublikasi qonunchiligiga asosan autsorsing xizmatini ko‘rsatishi mumkin.

5.9 Universitetning O‘quv ishlar bo‘yicha prorektori axborot-kommunikatsiya texnologiyalarini joriy etish va raqamlashtirish (Chief Digital Officer) hamda Universitetda axborot xavfsizligini ta’minlash masalalari bo‘yicha mas’ul rahbar (keyingi o‘rinlarda – Mas’ul rahbar) hisoblanadi. Mas’ul rahbarga ushbu vazifalar Universitet rektori buyrug‘i bilan yuklanadi. Mas’ul rahbar Universitetda axborot xavfsizligini ta’minlash bo‘yicha ishlarni muvofiqlashtiradi.

5.10 Universitetda axborot xavfsizligini ta’minlash masalalari bo‘yicha mas’ul etib Departamentning Raqamli ta’lim texnologiyalarini joriy etish va axborot xavfsizligini ta’minlash sektori muhandis-dasturchisi (keyingi o‘rinlarda – Axborot xavfsizligi administratori) Rektor buyrug‘i bilan belgilanadi va axborot xavfsizligini ta’minlash bo‘yicha vazifalar yuklatiladi, shuningdek, mazkur Axborot xavfsizligi administratori qayta belgilanishi yoki yuklatilgan vazifalarni bajarishdan ozod etilishi mumkin.

Universitetda Departamentning Tarmoqlarni boshqarish va texnik qo‘llab-quvvatlash sektori bosh mutaxassisi Lokal tarmoq administratori hisoblanadi.

5.11 Axborot xavfsizligi administratori Departamentning tegishli mas’ul xodimlari bilan birgalikda Universitetda ushbu Siyosat qoidalariga rioya qilinishi ustidan doimiy monitoring olib borilishini ta’minlaydi. Bundan tashqari, ushbu Siyosatga muvofiq axborot xavfsizligi talablariga rioya etilishini davriy ravishda ichki audit tekshiruvini o‘tkazadi va keyinchalik audit natijalari to‘g‘risidagi hisobotni Departament boshlig‘iga kiritadi.

5.12 Departament boshlig‘i Universitetda axborot xavfsizligini ta’minlash bo‘yicha ishlarni muvofiqlashtiradi va bajarilgan ishlar to‘g‘risida Axborot xavfsizligi administratori bilan birgalikda Mas’ul rahbarga ma’lumot kiritib borilishini ta’minlaydi.

6. Maqsad va vazifalar

6.1 Siyosatning asosiy maqsadlari quyidagilardan iborat:

- axborot munosabatlari subyektlarini moddiy, jismoniy, ma’naviy yoki boshqa zarar yetkazilishidan, axborotlashtirish obyektlarining faoliyatiga tasodifiy yoki ataylab ruxsatsiz aralashish yoki ulardagi ma’lumotlarga ruxsatsiz kirish va undan noqonuniy foydalanishdan himoya qilish;

- axborot xavfsizligi bilan bog‘liq hodisalarning yuzaga kelishi mumkin bo‘lgan oqibatlarini bartaraf etish va minimallashtirish, tahdidlarni prognozlash, oldini olish, axborot tizimlaridagi zaifliklarni aniqlash va yo‘q qilish;

- keng qamrovli tahdidlarni hisobga olgan holda, axborot xavfsizligini, Universitet axborot resurslari va ma’lumotlar bazalarining uzluksiz, barqaror ishlashini ta’minlash bo‘yicha tashkiliy-texnik tadbirlar kompleksini shakllantirish;

- axborot xavfsizligi sohasidagi qonun hujjatlari, yo‘riqnomalar va nizomlarga va umumiy siyosatga rioya qilinishini ta’minlash;

- Universitet faoliyatiga oid axborotlar shuningdek, muhim axborot resurslarining konfidensialligi, yaxlitligi va foydalana olishligini ta’minlash;

- Universitet axborot tizimlari va resurslarini zaxiralash va qayta tiklash holatida bo‘lishini ta’minlash;

- zaxiralash tizimlarining doimiy aktualligini ta’minlash.

6.2 Siyosatning asosiy vazifalari quyidagilardan iborat:

- axborot xavfsizligiga ichki va tashqi tahdidlarni, axborot munosabatlarining manfaatdor tomonlariga zarar yetkazadigan sabablar va sharoitlarni o‘z vaqtida aniqlash va prognoz qilish;

- Universitetning axborotlashtirish obyektlariga ruxsatsiz kirishning oldini olish va urinishlarni aniqlash;

- konfidensial axborotlar va himoya obyektlarining konfidensialligi, yaxlitligi va foydalana olishligi ustidan nazoratni ta’minlash;

- mavjud axborot tizimlari va resurslar, AXBTlaridagi zaifliklarni aniqlash va bartaraf etish;

- axborot xavfsizligi nuqtai nazaridan Universitetning axborot-kommunikatsiya infratuzilmalarida foydalaniladigan axborot texnologiyalariga yagona talablarni ishlab chiqish;

- axborot xavfsizligiga tahdidlarni himoya qilish va ularga qarshi kurashishning tashkiliy-texnik usullari va zamonaviy texnik, shuningdek, dasturiy vositalaridan foydalangan holda axborot xavfsizligini ta’minlashga kompleks yondashuvni ta’minlaydigan AXBTni yaratish va rivojlantirish;

- axborotlashtirish obyektlarida axborot xavfsizligiga tahdidlarni amalga oshirish natijasida yetkazilgan zararni maksimal darajada kamaytirish uchun sharoit yaratish;

- hayot ta’minot tizimlarining zaxiralanishini ta’minlash;

- Universitetda axborot xavfsizligini ta’minlash bo‘yicha kadrlarni bilim va ko‘nikmalarini shakllantirish, axborot xavfsizligi tahdidlari yo‘nalishida xodimlarning xabardorligini oshirish.

7. Asosiy qoidalar

7.1 Siyosat quyidagi asosiy tamoyillarga asoslanadi:

- qonuniylik – O‘zbekiston Respublikasi Konstitutsiyasi va qonunchiligiga, foydalanuvchilarning qonuniy huquqlariga, amaldagi qonunlar va normativ hujjatlar talablariga qat’iy muvofiq ravishda axborot xavfsizligi choralarini amalga oshirish;

- jalb qilish va shaxsiy javobgarlik – Universitet rahbariyati va barcha xodimlari, professor-o‘qituvchilari hamda talabalari axborot xavfsizligini ta’minlash jarayonida ishtirok etadilar;

- vazifalarni taqsimlash – axborot xavfsizligini ta’minlash masalalaridagi rol va javobgarliklarni Universitet xodimlari o‘rtasida aniq taqsimlash;

- shaxsiy javobgarlik – xodimlarning mehnat shartnomalari va lavozim yo‘riqnomalarida, shuningdek, xodimlar bilan tuzilgan boshqa turdagi shartnomalarda (bitimlarda, kelishuvlarda) kiritilgan axborot xavfsizligi talablariga rioya etilishi uchun shaxsan javobgardirlar;

- professionallik – axborot xavfsizligini ta’minlash uchun mas’ul bo‘lgan xodimlarning bilim darajasi kasbiy darajasi doimiy ravishda takomillashtirilish va axborot xavfsizligini boshqarish jarayonlarida qo‘llash;

- o‘zaro hamkorlik va harakatlarning muvofiqligi – axborot xavfsizligini ta’minlash bo‘yicha harakatlar manfaatdor idoralar bilan kelishilgan holda amalga oshirish, shuningdek, maqsadlar, vazifalar, prinsiplar va vositalar bo‘yicha o‘zaro hamkorlikda ish olib borish;

- kuchaytirilgan xavfsizlik – axborot xavfsizligini ta’minlash bo‘yicha chora-tadbirlarni tahdidlarning barcha turlaridan samarali himoya qilishni tashkil etish zarurligini hisobga olgan holda tanlash;

- tizimli yondashuv – AXBTni qurishda, axborot xavfsizligini ta’minlash masalasini tushunish va hal qilish uchun muhim bo‘lgan barcha ta’sir qiluvchi va vaqtni o‘zgartiruvchi elementlar, shartlar va omillarni hisobga olinishi;

- to‘liqlilik – himoyaning bir xil bo‘lmagan usullari va vositalaridan foydalanish (ular birgalikda zaif nuqtalarni o‘z ichiga oladi va barcha muhofaza qilinadigan obyektlarning jamlangan himoyasini ta’minlaydi);

- himoyaning uzluksizligi – axborot xavfsizligini ta’minlash jarayoni o‘z vaqtida doimiy amalga oshiriladi;

- harakatlarning nazorati va hisobga olinishi – qabul qilingan axborot xavfsizligi talablarining xodimlar tomonidan bajarilishi nazorat qilinadi va ularning Universitet axborot tizimlari va resurslaridagi barcha harakatlari hisobga olinadi.

7.2 Universitetda axborot xavfsizligini ta’minlash bo‘yicha ko‘rilgan usul va choralar quyidagilarga yo‘naltirilgan bo‘lishi lozim:

- axborot va kiberxavfsizlik tahdidlarni aniqlash, oldini olish;

- himoya qilish tizimidagi zaifliklar va kamchiliklarni aniqlash va bartaraf etish;

- vujudga kelgan hodisalarga tezkor choralar ko‘rish;

- tahdidlar amalga oshirilgan taqdirda axborot resurslarining hayotiyligini ta’minlash;

- tahdidlarni lokalizatsiya qilish va axborot tizimlari va resurslarining normal ishlashini tiklash bilan ularni amalga oshirish oqibatlarini bartaraf etish.

7.3 Universitetda axborot xavfsizligi axborotni himoya qilishning huquqiy, tashkiliy, texnik va boshqa usullari hamda choralaridan foydalangan holda, shuningdek, amalga oshirilayotgan axborot xavfsizligi choralari samaradorligini har tomonlama uzluksiz monitoring qilish orqali ta’minlanishi kerak.

Universitetda qo‘llaniladigan axborot xavfsizligi choralari ushbu Siyosatning 11-bandida keltirilgan.

8. Himoya obyektlari

8.1 Universitetda axborot xavfsizligiga tahdidlardan himoya qilish obyektlari quyidagilar:

8.1.1 Qog‘oz va elektron shakldagi ma’lumotlar, shu jumladan konfidensial axborotlar:

- rasmiy (ish faoliyatga oid) ma’lumotlar;
- uchinchi tomon tashkilotlarining konfidensial ma’lumotlari (yetkazib beruvchilar, mijozlar, sheriklar, bo‘ysunuvchi tashkilotlar va boshqalar);
- yuqori turuvchi tashkilotlar bilan almashilgan konfidensial ma’lumotlar;
- tijorat sirini tashkil etuvchi ma’lumotlar;
- xodimlar, professor-o‘qituvchilar va talabalarning shaxsga doir ma’lumotlari;
- hay’at, kengash va boshqa yig‘ilishlarda muhokama qilingan konfidensial xarakterdagi ma’lumotlar;
- buxgalteriya hisobi registrlari;
- Axborot tashuvchilari (CD/DVD/BD, tashqi qattiq disklar, mobil qurilmalar sifatida USB flesh-xotiralar, qattiq disklar va noutbuklar va h.k.).
- kuzatuv kameralari, qo‘riqlash signalizatsiyasi hamda yong‘indan darak beruvchi signalizatsiya tizimlari joylashgan xonalar;
- muhandislik infratuzilmasi: xonalar, hisoblash qurilmalari, telekommunikatsiyalar xizmatlari, kommunal tarmoqlar (isitish, havoni tozalash va sovitish);
- zaxira elektr manbalari bilan ta’minlovchi qurilmalar, shu jumladan elektr toki ishlab chiqaruvchi quyosh panellari va generatorlar.
- Universitetning ma’lumot uzatish lokal hamda korporativ tarmoq obyektlari, serverlar, ma’lumotlarni uzatish kanallari, tarmoq kabellari, tarmoq qurilmalari (marshrutizatorlar, marshrut jadvallari, boshqariladigan va boshqarilmaydigan kommutatorlar).

8.1.2 Axborot tizimlari va resurslari:

- Universitetning rasmiy veb-sayti (buxdu.uz);
- Onlayn o‘qitish tizimi (moodle.buxdu.uz)
- Oliy ta’lim jarayonlarini boshqarish axborot tizimi (hemis.buxdu.uz)
- Masofaviy o‘qitish tizimi (masofaviy.buxdu.uz)
- Oliy ta’lim jarayonlarini boshqarish axborot tizimi talabalar uchun (student.buxdu.uz)
- Raqamli universitet tizimi (uniwork.buxdu.uz)
- Universitetning “Comparative linguistics, translation and literary studies” jurnali sayti (citrus.buxdu.uz)
- Professor-o‘qituvchilar tomonidan ilmiy jurnallarda chop etilgan maqolalarni kiritish tizimi (journal.buxdu.uz)
- “Buxoro davlat universiteti ilmiy axboroti” ilmiy jurnali sayti (srep.buxdu.uz)
- Universitetning “Pedagogik mahorat” ilmiy-nazariy va metodik jurnal sayti (pedskills.buxdu.uz)
- Fayl serverlar
- Ishchi stansiyalar;
- Server uskunalari;
- Kirish chiqishni nazorat qilish tizimi;
- Videokuzatuv tizimi.

8.2 Universitet axborot tizimlari va resurslari xavfsizligi darajasiga ko‘ra tasnif ushbu Siyosatning 14-ilovasiga muvofiq Universitet axborot resurslari Reestriga keltirilgan.

8.3 Universitetda mavjud axborot tizimlari va resurslarini axborot xavfsizligi darajasi bo‘yicha tasniflash davlat va xo‘jalik boshqaruvi organlari, mahalliy davlat hokimiyati organlarida axborot xavfsizligini ta’minlashga qo‘yiladigan talablarga asosan shakllantirilgan va 1-jadvalda keltirilgan.

1-jadval. Universitetda mavjud axborot tizimlari va resurslarini axborot xavfsizligi darajasi bo‘yicha tasniflash

T/r	Axborot tizimi va resurs nomi	Masshtabi	Axborot toifasi	Ahamiyat-lilik darajasi	Himoya-langanlik sinfi*
1.	buxdu.uz	Sohaga tegishli global miqyosida	Ochiq axborot	O‘rta	IS3
2.	moodle.buxdu.uz	Sohaga tegishli global miqyosida	Ochiq axborot	O‘rta	IS3
3.	hemis.buxdu.uz	Sohaga tegishli global miqyosida	Ochiq axborot	O‘rta	IS3
4.	masofaviy.buxdu.uz	Sohaga tegishli global miqyosida	Ochiq axborot	O‘rta	IS3
5.	student.buxdu.uz	Sohaga tegishli global miqyosida	Ochiq axborot	O‘rta	IS3
6.	uniwork.buxdu.uz	Sohaga tegishli global miqyosida	Ochiq axborot	O‘rta	IS3
7.	citrus.buxdu.uz	Sohaga tegishli global miqyosida	Ochiq axborot	Yuqori	IS4
8.	journal.buxdu.uz	Sohaga tegishli global miqyosida	Ochiq axborot	Yuqori	IS4
9.	srep.buxdu.uz	Sohaga tegishli global miqyosida	Ochiq axborot	Yuqori	IS4
10.	pedskills.buxdu.uz	Sohaga tegishli global miqyosida	Ochiq axborot	Yuqori	IS4
11.	Korporativ elektron pochta	Sohaga tegishli lokal miqyosida	Ochiq axborot	Yuqori	IS4
12.	Fayl serverlar	Sohaga tegishli global miqyosida	Ochiq va konfidensial axborot	Yuqori	IS4
13.	Ishchi stansiyalar	Sohaga tegishli lokal miqyosida	Ochiq va konfidensial axborot	Yuqori	IS4
14.	Server uskunalari	Sohaga tegishli lokal miqyosida	Ochiq axborot	Yuqori	IS4
15.	Ichki telefon tarmog‘i	Sohaga tegishli lokal miqyosida	Ochiq axborot	Yuqori	IS4
16.	Kirish chiqishni nazorat qilish tizimi	Sohaga tegishli lokal miqyosida	Konfidensial axborot	Yuqori	IS4
17.	Videokuzatuv tizimi	Sohaga tegishli lokal miqyosida	Konfidensial axborot	Yuqori	IS4

T/r	Axborot tizimi va resurs nomi	Masshtabi	Axborot toifasi	Ahamiyat-lilik darajasi	Himoya-langanlik sinfi*
18.					
19.					

** Izoh: Eng past xavfsizlik klassi birinchi sinf (IS1), eng yuqori darajasi — to‘rtinchi sinf (IS4)*

8.4. Quyida 2-jadvalda ko‘rsatilgan Universitetning axborot tizimlari va ma’lumotlar bazasida Universitet xodimlari va talabalarning shaxsga doir ma’lumotlari mavjud. O‘zbekiston Respublikasi Vazirlar Mahkamasining 2022-yil 5-oktabrdagi 570-son “Shaxsga doir ma’lumotlarni qayta ishlash sohasidagi ayrim normativ-huquqiy hujjatlarni tasdiqlash to‘g‘risida”gi qaroriga muvofiq shaxsga doir ma’lumotlarni qayta ishlash bo‘yicha ushbu ma’lumotlar bazalariga tegishli himoya darajasi beriladi.

Universitet axborot tizimlarida qayta ishlanadigan shaxsga doir ma’lumotlarni himoya qilish bo‘yicha tegishli talablar ushbu siyosatning 17-ilovasiga muvofiq “Himoyalangan ma’lumotlarga ishlov berish tartibi”da belgilangan.

2-Jadval. Belgilangan himoya darajasiga ega shaxsga doir ma’lumotlarni qayta ishlash bo‘yicha ma’lumotlar bazalari ro‘yxati

Resurs nomi	Shaxsga doir ma’lumotlar turi	Himoya darajasi
moodle.buxdu.uz	xodimlar va talabalarining shaxsga doir ma’lumotlari	2
hemis.buxdu.uz	xodimlar va talabalarining shaxsga doir ma’lumotlari	2
student.buxdu.uz	xodimlar va talabalarining shaxsga doir ma’lumotlari	2
Kirish chiqishni nazorat qilish tizimi	xodimlar va talabalarining shaxsga doir ma’lumotlari	1

8.5 Universitet axborot resurslarini himoya qilish darajasi bo‘yicha tasniflash ushbu siyosatning 14-ilovasi “Universitet axborot resurslari reestri”da keltirilgan.

9. Risk va axborot xavfsizligiga tahdidlar modeli

9.1 Universitetning axborot xavfsizligiga tahdidlar modeli har bir muhim himoya obyekti uchun belgilanadi va quyidagilarni o‘z ichiga oladi:

- himoya obyektining tavsifi;
- himoya obyektiga bo‘lishi mumkin bo‘lgan xavfsizlik tahdidlarining ro‘yxati va tavsifi;
- huquqbuzar modeli;
- tahdidlarni amalga oshirishning oqibatlari.

9.2 Universitetning axborot xavfsizligiga tahdidlar ularning paydo bo‘lishi tabiati bo‘yicha tabiiy (obyektiv) va sun’iy (subyektiv) bo‘lishi mumkin.

9.3 Axborot xavfsizligiga tahdidlar manbalari ichki va tashqi bo‘lishi mumkin.

9.4 Axborot xavfsizligiga tahdidlar tufayli ular qasddan va tasodifiy bo‘lishi mumkin.

9.5 Risklarni aniqlash O‘zMSt ISO/IEC 27005:2024 “Axborot texnologiyasi.

Xavfsizlikni ta’minlash usullari. Axborot xavfsizligi risklarini boshqarish” davlat standarti talablariga muvofiq amalga oshiriladi.

9.6 Risklarni identifikatsiyalash natijalari xavf darajalarini va ushbu xavflardan himoya qilish uchun tanlangan chora-tadbirlar, usullar va vositalarni amalga oshirishga asos bo‘lib xizmat qiladi.

9.7 Risklarni identifikatsiya qilish risklarni baholashga (xavfni tahlil qilish) tizimli yondashuvni va xavflarning ahamiyatini aniqlash uchun baholangan xavflarni risk mezonlari bilan taqqoslashni o‘z ichiga oladi.

Risklarni aniqlash bilan bir qatorda risklarni boshqarish jarayonlari quyidagilarni o‘z ichiga olishi kerak: xavfni qayta ishlash, xavfni qabul qilish, risk bilan bog‘lanish va maslahatlar, xavflarni monitoring qilish va ko‘rib chiqish.

9.8 Axborot xavfsizligiga tahdidlarning dolzarbligini aniqlash uchun ikkita mezondan foydalaniladi:

- tahdidlarning xavfliligi;
- tahdidning paydo bo‘lishi va amalga oshirilishi ehtimoli.

Tahdidni amalga oshirish natijasida yuzaga keladigan oqibatlarga qarab baholanishi 3-jadvalga asosan, xavfni qabul qilish mezoni 4-jadvalga asosan tavsiflangan.

3-jadval. Axborot xavfsizligi tahdidning baholanishi

Tahdidning ehtimolligi	**Tahdid sharhi**	**Tahdidning baholanishi**
Juda past	Tahdid deyarli umuman sodir bo‘lmaydi	0-0,2
Past	Ushbu tahdidning sodir bo‘lish ehtimolligi kam, tahdid sodir bo‘lishini ko‘rsatuvchi belgilar mavjud emas	0,2-0,4
O‘rta	Tahdidning sodir bo‘lishi teng ehtimolli	0,4-0,6
Yuqori	Ushbu tahdid sodir bo‘lishi mumkin (oldin tahdidlar bo‘lgan) yoki oldinlari ushbu tahdid bo‘lganligini ko‘rsatuvchi statistika va boshqa ma’lumotlar mavjud yoki buzg‘unchida ushbu tahdidni amalga oshirish uchun ma’lum bir sabablar mavjud	0,6-0,8
Juda yuqori	Tahdid sodir bo‘lish ehtimoli ko‘proq. Oldinlari ushbu tahdid bo‘lganligini ko‘rsatuvchi statistika va boshqa ma’lumotlar mavjud yoki buzg‘unchida ushbu tahdidni amalga oshirish uchun jiddiy sabablar mavjud	0,8-1

4-jadval. Xavfni qabul qilish mezoni

Xavf darajasi	**Xavfni baholash**	**Miqdorni aniqlash**	**Tavsifi**
Past (yashil)	Qanday bo‘lsa shundayligicha qabul qilinadi	0-1	Xavf boshqa harakatlarsiz qabul qilinishi mumkin
O‘rta (sariq)	Boshqaruv vositalari mavjud bo‘lgan hollarda qabul qilinadi	1-2	O‘rta va uzoq muddatli istiqbolda doimiy takomillashtirish doirasida risklarni boshqarish faoliyati va ichidagi harakatlarni belgilash chora-tadbirlarini o‘tkazish lozim

Yuqori (qizil)	Qabul qilib bo‘lmaydigan	2 dan yuqori	Qisqa muddatda xavfni kamaytirish choralarini ko‘rish kerak.

9.9 “Yuqori”, ya’ni qiymati xavfni qabul qilish mezonidan yuqori bo‘lgan axborot xavfsizligi risklari uchun ushbu risklarni kamaytirish choralarini ko‘rish kerak. Ushbu chora-tadbirlar tahdidning paydo bo‘lishini kamaytirish yoki yo‘q qilishga, zaiflik darajasini yo‘q qilishga yoki kamaytirishga qaratilgan bo‘lishi mumkin.

Agar choralar ko‘rilsa, xavflar riskning paydo bo‘lishi va zaiflikning mavjudligi parametrlarining yangi qiymatlarini hisobga olgan holda qayta hisoblab chiqiladi. Natijada yangi xavf qiymati qoldiq risk hisoblanadi.

9.10 “Yuqori” darajaga ega bo‘lgan xavflarga nisbatan xavflarni kamaytirish choralarini ko‘rish kerak. Ko‘rsatilgan qarshi choralar, shuningdek, chora-tadbirlar ko‘rilganidan keyin axborot xavfsizligining qoldiq risk hisoblanadi.

9.11 Axborot xavfsizligining “yuqori” darajadagi risklarini kamaytirishga, shuningdek zarur axborot xavfsizligi vositalarini tanlashga qaratilgan chora-tadbirlar ushbu Siyosatning 11-bo‘limida keltirilgan.

9.13 Universitetning axborot aktivlariga nisbatan “Axborot xavfsizligi risklarini baholash” natijalari ushbu siyosatning 23-ilovasida batafsil keltirilgan.

10. Axborot xavfsizligi buzg‘unchisi modeli

10.1 Axborot xavfsizligi buzg‘unchisi modeli subyektlarning imkoniyatlari va turlari, ruxsatsiz ta’sirlarning maqsadi to‘g‘risidagi ma’lumotlarni tizimlashtirish va ularga qarshi turishning yetarli darajada tegishli usullarini ishlab chiqish uchun shakllantiriladi.

Buzg‘unchi modelini ishlab chiqishda quyidagilar e’tiborga olinishi kerak:

- buzg‘unchilarning toifalari;
- buzg‘unchilarning xavflilik darajasi va ahamiyatini baholash va uning texnik imkoniyatlarini tahlil qilish xususiyatlari;
- cheklov choralari va qarshi kurashish choralari.

10.2 Axborot xavfsizligini buzg‘unchilari – atayin g‘arazli niyat bilan (g‘arazli manfaatlar asosida) yoki ularsiz (o‘yin yoki o‘zini ko‘rsatish hamda boshqa maqsadlarda), shuningdek g‘arazli maqsadda bo‘lgan tajribali foydalanuvchilar buzishga qaratilgan ta’qiqlangan harakatlarni (operatsiyalarni) bajarishga uringan, shuningdek buning uchun turli xil imkoniyatlar, usul va vositalardan foydalangan shaxslardir.

10.3 Himoya obyektlariga nisbatan huquqbuzarliklarni xavfsizlik obyektlariga to‘g‘ridan-to‘g‘ri kirish huquqiga ega bo‘lgan Universitet xodimlari, himoya qilish obyektlaridan foydalanish huquqiga ega bo‘lmagan xodimlar va Universitetning xodimlari bo‘lmagan shaxslar bo‘lishi mumkin.

10.4 Buzg‘unchilarning asosiy guruhlari va toifalari:

Buzg‘unchilarni ko‘rib chiqishda himoya qilish obyektlariga va shunga mos ravishda uning tarkibiy qismlariga ta’sir qilish imkoniyatlariga qarab guruhlarga bo‘lish kerak. Buzg‘unchilarning ikki guruhi mavjud:

1) tashqi buzg‘unchilar — nazorat qilinadigan hududning ichki qismiga kirish

huquqiga ega bo‘lmagan va tegishli ravishda muhofaza qilinadigan obyekt va uning tarkibiy qismlariga bevosita ta’sir qilish imkoniga ega bo‘lmagan shaxslar;

2) ichki buzg‘unchilar — nazorat qilinadigan hududning ichki qismiga kirish huquqiga ega bo‘lgan shaxslar va shunga mos ravishda himoya qilish obyektiga va uning qismlariga kirish huquqiga ega bo‘lgan shaxslar.

10.5 Yuqoridagi guruhlardan qat’iy nazar, buzg‘unchilarni mumkin bo‘lgan harakatlar orqali to‘rtta sinfga ajratish mumkin:

- birinchi (1-sinf) ma’lumotlarni qayta ishlash uchun oldindan belgilangan funksiyalar orqali vazifalarni boshlash bilan tavsiflanadi;

- ikkinchi (2-sinf), birinchi darajali foydalanuvchilarning imkoniyatlarini o‘z ichiga oladi va qo‘shimcha ravishda yangi ma’lumotlarni qayta ishlash funksiyalari bilan o‘z dasturlarini yaratish va ishlatish qobiliyatiga ega;

- uchinchi (3-sinf) himoyalangan obyektning ishlashini boshqarish, ya’ni asosiy dasturiy ta’minotga, uning tarkibi va konfiguratsiyasiga ta’sir qilish qobiliyatiga ega;

- to‘rtinchi (4-sinf) himoya obyektlarining texnik jihozlarini loyihalashtirish, amalga oshirish va ta’mirlash bilan shug‘ullanuvchi shaxslarning, shu jumladan himoya obyekti tarkibida ma’lumotlarni qayta ishlashning yangi funksiyalari bilan jihozlangan va dasturiy ta’minotni qamrab oluvchi imkoniyatlari bilan ajralib turadi.

10.6 Buzg‘unchilarni axborot texnologiyalari sohasi mutaxassisi sifatiga ko‘ra ajratish:

- tajribasiz foydalanuvchi (A sinfi): ushbu sinfga tajovuzkor kamdan-kam uchraydigan, ammo tizimning ishlamay qolishiga olib kelishi mumkin bo‘lgan himoya obyektida beparvolik yoki noto‘g‘ri harakatlar manbai sifatida xavf tug‘diradi;

- ishonchli foydalanuvchi (B sinfi): buzg‘unchilarning ushbu himoya obyekti buzilishining manbai bo‘lishi mumkin, ammo dasturlarni o‘rnatishga, tashqi manbalardan, shu jumladan Internetdan foydalanishga urinish erkin foydalanishni boshqarish tizimi va axborotni himoya qilish vositalari tomonidan to‘xtatiladi;

- yuqori malakali foydalanuvchi (D sinfi): ushbu sinf buzg‘unchilarining kirishni boshqarish va axborotni muhofaza qilishning belgilangan qoidalarini buzishga bo‘lgan barcha urinishlari xavfsizlik tizimi tomonidan bloklangan xavfsizlik auditi tizimida qayd etilishi kerak.

10.7 Mumkin bo‘lgan harakatlarga asoslanib, potensial qoidabuzar to‘rt darajadan biriga tegishli bo‘lishi mumkin:

1) buzg‘unchining imkoniyatlarining birinchi (past) darajasi oldindan ta’minlangan ma’lumotlarni qayta ishlash funksiyalari bilan belgilangan to‘plamdan vazifalarni ishga tushirish bilan tavsiflanadi;

2) ikkinchi (o‘rta) daraja birinchi darajali foydalanuvchilarning imkoniyatlarini, shuningdek qo‘shimcha ravishda axborotni qayta ishlashning yangi funksiyalari bilan o‘z dasturlarini yaratish va ishga tushirish qobiliyatini o‘z ichiga oladi;

3) uchinchi (yuqori) daraja, himoyalangan obyektning ishlashini nazorat qilish, ya’ni asosiy dasturiy ta’minot, uning tarkibi, konfiguratsiyasi va ishlashiga ta’sir qilish qobiliyatiga ega;

4) to‘rtinchi (juda yuqori) daraja, himoya qilish obyektlarining texnik vositalarini loyihalash, joriy etish va ta’mirlashni amalga oshiruvchi shaxslarning ma’lumotlarni

qayta ishlashning yangi funksiyalariga ega bo‘lgan apparat va dasturiy ta’minotni obyekt himoya qilish tizimiga kiritishgacha bo‘lgan barcha imkoniyatlari bilan tavsiflangan.

10.8. Har bir potensial qoidabuzarlik uchun Universitet axborot xavfsizligini buzg‘unchi modeliga uning toifasi bilan bir qatorda quyidagilar kiradi:

1) buzg‘unchining xususiyatlari — uning imkoniyatlari va harakatlari, u axborot xavfsizligini buzish uchun foydalanishi mumkin bo‘lgan ta‘sir qilish usullari va vositalari, buzilish sabablari (xato, mas’uliyatsizlik, va b);

2) u ta’sir qilishi mumkin bo‘lgan himoya obyektlari;

3) buzg‘unchilarga qarshi asosiy cheklovchi choralar (qarshi choralar).

10.9. Buzg‘unchi quyidagi usul va vositalardan foydalanishi mumkin:

1) axborot va ma’lumotlarni yig‘ish;

2) passiv tutib olish vositalari;

3) axborot tizimiga yoki uni himoya qilish tizimiga kiritilgan standart vositalardan foydalanish va ularning kamchiliklari;

4) faol ta’sir vositalaridan foydalanish (qo‘shimcha vositalarni o‘zgartirish va ulash, ma’lumotlarni uzatish kanallariga ulanish, dasturiy xatcho‘plarni amalga oshirish, maxsus instrumental texnologik dasturlardan foydalanish).

Universitet potensial buzg‘unchilarining modeli 5-jadvalda keltirilgan.

5-jadval. Axborot xavfsizligini buzg‘unchilarning modellari

Model ko‘rsatkichlari	Tavsif
Ichki buzg‘unchilar	
1. Axborot tizimlari va tarmoqlarining ro‘yxatdan o‘tgan (vakolatli) foydalanuvchilari (to‘g‘ridan-to‘g‘ri foydalanuvchilar) bo‘lgan xodimlar	
Tajriba	ishonchli foydalanuvchi (B sinfi)
Imkoniyatlar	birinchi (past) daraja
Xarakteri	Tahdidlarni amalga oshirish imkoniyati mavjudligi, asosan, o‘z vakolatlarini kengaytirishga va himoya obyekti bilan o‘zaro munosabatlarning faqat standart dasturiy va texnik vositalaridan foydalangan holda axborotni himoya qilish vositalarini yengib o‘tishga urinishlar, himoya obyektiga beparvo yoki noto‘g‘ri harakatlar manbai bo‘lib xizmat qilishi mumkin, shuningdek ular ma’lumotlarning mavjudligi va himoyalangan ma’lumotlarning tarqalishi bilan tavsiflanadi. Motivlar har xil bo‘lishi mumkin, asosan xato, mas’uliyatsizlik yoki shaxsiy manfaat
Ta’sirga duchor bo‘lgan himoya obyektlari	axborot tizimlari, tarmoq, oxirgi qurilmalar, dasturiy ta’minot va ma’lumotlar (ma’lumotlar) raqamli shaklda
Cheklovchi choralar va qarshi kurash usullari	huquqlarni farqlash va himoya obyektlariga kirishni boshqarish; axborot tizimlarida xodimlarning harakatlarini hisobga olish; ma’lumotlarning tarqalishi kanallarini kamaytirish yoki nazorat qilish; konfidensial ma’lumotlarni oshkor qilmaslik bo‘yicha xodimlarning talablariga muvofiqligi
2. Axborot tizimlaridan foydalanmaydigan xodimlar (qo‘riqlash xodimlari, xona va binolarga xizmat ko‘rsatadigan texnik xodimlar)	
Tajriba	**A toifasi (tajribasiz foydalanuvchi)**
Imkoniyatlar	birinchi (past) daraja
Xarakteri	Ushbu turdagi huquqbuzarning tahdidlarini amalga oshirish imkoniyatlari himoya obyektiga ruxsatsiz jismoniy kirishni olish bilan cheklanadi yoki ular asosan himoya obyektiga beparvo yoki noto‘g‘ri harakatlar manbai bo‘lib xizmat qiladi, bu tizimning ishdan chiqishiga yoki hatto ishlamay qolishiga olib kelishi mumkin. Ular ma’lumot to‘plashlari yoki passiv ushlash vositalaridan foydalanishlari mumkin. Motivlar har xil bo‘lishi mumkin, asosan xatolar yoki mas’uliyatsizlik
Ta’sirga duchor bo‘lgan himoya obyektlari	Universitetning har qanday axborot aktivlari, shuningdek moddiy yoki nomoddiy shaklidagi ma’lumotlar
Cheklovchi choralar va qarshi kurash usullari	himoya obyektlarini joylashtirish bo‘yicha talablarni bajarish; himoya obyektiga nisbatan ruxsatsiz jismoniy kirish va harakatlarning oldini olish va oldini olishga qaratilgan rejim va tashkiliy-texnik chora-tadbirlardan foydalanish; kadrlarni tanlash va joylashtirish; himoya obyektlari joylashgan binolarga kirishlarni boshqarish
3. Universitetning texnik vositalariga xizmat ko‘rsatuvchi xodimlar	

Model ko‘rsatkichlari	Tavsif
Tajriba	C toifasi (malakali foydalanuvchi) yoki yuqori malakali foydalanuvchi (D sinfi)
Imkoniyatlar	ikkinchi (o‘rta) daraja yoki uchinchi (yuqori) daraja
Xarakteri	Himoya obyektining texnik va dasturiy vositalariga ruxsatsiz jismoniy kirishning mavjudligi, ammo ularning ro‘yxatdan o‘tgan foydalanuvchisi emas. Amaldagi usullar va vositalar: ma’lumotlarni yig‘ish, passiv ushlash vositalari, doimiy vositalardan foydalanish yoki faol ta’sir qilish vositalaridan foydalanish. Motivlar har xil bo‘lishi mumkin, asosan xatolar yoki o‘z-o‘zini tasdiqlash
Ta’sirga duchor bo‘lgan himoya obyektlari	ular xizmat ko‘rsatadigan texnik vositalar (axborotni qayta ishlash va saqlash vositalari, tarmoq uskunalari va axborotni himoya qilish vositalari), shu jumladan ularga o‘rnatilgan dasturiy ta’minot va ularda saqlanadigan ma’lumotlar
Cheklovchi choralar va qarshi kurash usullari	himoya obyekti joylashgan xonalarga jismoniy shaxslarni qabul qilish uchun cheklovchi omillardan foydalanish; ish tartibini nazorat qilish, ishni nazorat qilish
4. Universitet tarmoqlari, axborot tizimlari va axborotni himoya qilish vositalariga xizmat ko‘rsatuvchi administratorlar	
Tajriba	C toifasi (malakali foydalanuvchi)
Imkoniyatlar	uchinchi (yuqori) yoki to‘rtinchi (juda yuqori) daraja
Xarakteri	Himoya obyektiga ruxsat berilgan jismoniy va mantiqiy kirishning mavjudligi va imtiyozli foydalanuvchilar guruhining a’zolari. Ushbu turni buzuvchining o‘ziga xos xususiyati shundaki, ular himoya obyektining ishonchli xodimlari qatoriga kiradi va ularga himoya obyekti tarkibiy qismlarining ichki holatiga ta’sir qilish tahdidini amalga oshirish uchun keng imkoniyatlar beriladi. Tahdidni amalga oshirish uchun standart vositalardan yoki faol ta’sir vositalaridan foydalanish mumkin. Motivlar har xil bo‘lishi mumkin, asosan xatolar yoki o‘z-o‘zini tasdiqlash.
Ta’sirga duchor bo‘lgan himoya obyektlari	Universitetning axborot tizimlari, ularning tarkibiga texnik vositalar, dasturiy ta’minot va axborot tizimi tomonidan saqlanadigan va qayta ishlanadigan ma’lumotlar kiradi
Cheklovchi choralar va qarshi kurash usullari	himoya obyektiga kirishda ushbu xodimlarning harakatlarini hisobga olish va nazorat qilish; imtiyozli foydalanuvchilarni boshqarish tizimini qo‘llash; xavfsizlik nazorati tizimi tomonidan ushbu sinf buzuvchisining kirishni chegaralash qoidalari va axborotni himoya qilish vositalarini chetlab o‘tishga qaratilgan barcha urinishlari, xavfsizlik tizimi tomonidan ushbu urinishlarni blokirovka qilish; ushbu toifadagi xodimlarga nisbatan javobgarlik choralarini kuchaytirish
5. Axborot tizimlarini ishlab chiquvchi Universitet xodimlari (dasturlarni ishlab chiquvchilar)	
Tajriba	C toifasi (malakali foydalanuvchi)
Imkoniyatlar	uchinchi (yuqori) yoki to‘rtinchi (juda yuqori) daraja
Xarakteri	Axborot tizimining amaliy dasturini ishlab chiqishda yoki dastur dasturining normal ishlashini buzish yoki ma’lumotlarning tarqalishi bilan bog‘liq noqonuniy xatti-harakatlarni amalga oshirish uchun e’lon qilinmagan funktsional imkoniyatlarni (xatcho‘plarni) o‘rnatishda ishlab chiquvchilarning xatolariga olib keladigan tahdidlarni amalga oshirish imkoniyati mavjudligi.

Model ko‘rsatkichlari	Tavsif
	Tahdidni amalga oshirish uchun standart vositalardan yoki faol ta’sir vositalaridan foydalanish mumkin. Motivlar har xil bo‘lishi mumkin, asosan xatolar yoki o‘z-o‘zini tasdiqlash
Ta’sirga duchor bo‘lgan himoya obyektlari	axborot tizimlarining dasturiy ta’minoti va axborot tizimlarining o‘zi
Cheklovchi choralar va qarshi kurash usullari	ishlab chiqishda ushbu xodimlarning harakatlarini hisobga olish va nazorat qilish; manba kodi analizatorlaridan foydalangan holda Universitetning alohida xodimlari tomonidan ishlab chiqilgan dasturlarni tahlil qilish; Universitetning uchinchi tomon xodimlari tomonidan dasturning funksional imkoniyatlari, kirish va chiqish ma’lumotlarini sinovdan o‘tkazish; axborot xavfsizligi talablariga muvofiq dasturiy mahsulotlarni sertifikatlash
6. Xavfsizlik xizmati xodimlari (qo‘riqlash)	
Tajriba	A toifasi (tajribasiz foydalanuvchi)
Imkoniyatlar	to‘rtinchi (juda yuqori) daraja
Xarakteri	Ruxsat etilgan jismoniy mavjudligi xonalarga va boshqa himoya obyektlariga jismoniy kirish. Ular passiv ushlab turish vositalaridan yoki standart vositalardan foydalanishlari mumkin. Motivlar har xil bo‘lishi mumkin, asosan mas’uliyatsizlik yoki shaxsiy manfaat
Ta’sirga duchor bo‘lgan himoya obyektlari	jismoniy himoyalangan xonalar Universitetning moddiy aktivlari
Cheklovchi choralar va qarshi kurash usullari	xonalarga kirishni hisobga olish (videokuzatuv, kirish va chiqish jurnalini yuritish); ushbu toifadagi xodimlarga nisbatan javobgarlik choralarini kuchaytirish; tegishli kadrlar tanlovi.
Tashqi buzg‘unchilar	
1. Ishdan bo‘shatilgan xodimlar	
Tajriba	ilgari egallab turgan lavozimiga qarab toifasi
Imkoniyatlar	ilgari egallagan lavozimiga qarab darajasi
Xarakteri	Ushbu turdagi tashqi huquqbuzarning tahdidlarini amalga oshirish imkoniyatlari shaxsiy foyda olish yoki zarar yetkazish, noqonuniy xatti-harakatlar qilish uchun Universitetning himoyalangan ma’lumotlarini, shu jumladan ruxsatsiz kirish yoki axborotni himoya qilish vositalarini chetlab o‘tish bilan bog‘liq texnologik va texnik ma’lumotlarni oshkor qilish yoki ulardan foydalanish bilan cheklanadi. Asosiy sabab-xudbin qiziqish
Ta’sirga duchor bo‘lgan himoya obyektlari	Universitetdagi mehnat faoliyati davomida olgan bilimlari va konfidensial ma’lumotlari
Cheklovchi choralar va qarshi kurash usullari	xodim ishdan bo‘shatilgandan keyin konfidensial ma’lumotlarni oshkor qilmaslik majburiyatlarini bajarish; ishdan bo‘shatilgandan keyin ularning kirish tafsilotlaridan foydalanish imkoniyatini istisno qilish;

Model ko‘rsatkichlari	Tavsif
	ular tomonidan konfidensial ma’lumotlar, kirish tafsilotlari va identifikatorlari, himoya vositalari va boshqalarni etkazib berish. ishdan bo‘shatilganda
2. Mijozlar yoki uchinchi tomon vakillari bo‘lgan mehmonlar	
Tajriba	A toifasi (tajribasiz foydalanuvchi) yoki yuqori malakali foydalanuvchi (D sinfi)
Imkoniyatlar	birinchi (past) daraja yoki to‘rtinchi (juda yuqori) daraja
Xarakteri	Ushbu turdagi tashqi buzg‘unchilarning tahdidlarini amalga oshirish qobiliyati himoyalangan obyektga ruxsatsiz jismoniy kirishni qo‘lga kiritish bilan bog‘liq. Amaldagi usullar va vositalar passiv ushlash vositalari yoki bo‘lishi mumkin standart vositalar. Asosiy sabab — xudbin qiziqish
Ta’sirga duchor bo‘lgan himoya obyektlari	jismoniy himoyalanmagan moddiy boyliklar va axborotni qayta ishlash vositalari
Cheklovchi choralar va qarshi kurash usullari	himoyalanadigan obyektlarni joylashtirish talablarini bajarish; xonalarni xavfsizlik zonalariga bo‘lish; xavfsizlik va tashkiliy-texnik chora-tadbirlar majmuidan foydalangan holda ruxsat etilmagan xonalarga (hududlarga) tashrif buyuruvchilarning kirishini cheklash; tashrif buyuruvchilarni nazorat qilish va ro‘yxatga olish; tashrif buyuruvchilarga hamrohlik qilish; past xavfsizlik zonalarida tashrif buyuruvchilarni qabul qilish
3. Shartnoma asosida ishlarni bajaruvchi (pudratchilar, yetkazib beruvchilar, ishlab chiquvchilar va boshqalar), shuningdek autsorsing xizmatlarini ko‘rsatadigan uchinchi tomon tashkilotlarining vakillari	
Tajriba	yuqori malakali foydalanuvchi (D sinfi)
Imkoniyatlar	ikkinchi (o‘rta) daraja yoki uchinchi (yuqori) daraja
Xarakteri	Himoya qilinadigan obyektga mantiqiy va jismoniy kirish huquqiga ega bo‘lgan, lekin ularning ro‘yxatdan o‘tgan foydalanuvchisi bo‘lmagan — himoyalangan obyektning texnik va dasturiy ta’minotini ishlab chiquvchilar, ularni o‘rnatish, ishga tushirish, foydalanish vaqtida texnik xizmat ko‘rsatish va boshqalar. Ushbu turdagi qoidabuzarlarning o‘ziga xos xususiyati shundaki, maxsus buzg‘unchi vositalarga o‘rnatilgan ishlash algoritmiga qarab turli harakatlarni amalga oshirishi mumkinligi. Maxsus buzg‘unchi vositalarni ishga tushirish himoyalangan obyektning butun hayoti davomida ishlashi paytida istalgan vaqtda sodir bo‘lishi mumkin. Tahdidlarni amalga oshirish uchun faol ta’sir qilish vositalari qo‘llaniladi. Asosiy sabab — xudbin qiziqish.
Ta’sirga duchor bo‘lgan himoya obyektlari	ular tomonidan foydalaniladigan va xizmat ko‘rsatadigan apparat va dasturiy ta’minot
Cheklovchi choralar va qarshi kurash usullari	ish tartibini nazorat qilish; ushbu ishlarda Universitet vakilining mavjudligi;

Model ko‘rsatkichlari	Tavsif
	faqat himoyalangan obyektning zarur vositalariga kirishni ta’minlash va ushbu kirishni nazorat qilish; mahsulotni loyihalashda texnik talablarga rioya qilish; “oq shapka” tamoyilidan foydalangan holda zaiflik testi.
4. Tashqi foydalanuvchilar Universitet axborot tizimlariga tashqi tarmoq orqali kirish imkoniyati mavjud foydalanuvchilar	
Tajriba	A toifasi (tajribasiz foydalanuvchi) yoki yuqori malakali foydalanuvchi (D sinfi)
Imkoniyatlar	birinchi (past) daraja yoki uchinchi (yuqori) daraja
Xarakteri	Universitetning axborot tizimlariga mantiqiy kirish huquqiga ega bo‘lish, ularning ro‘yxatdan o‘tgan foydalanuvchisi bo‘lish. Mumkin bo‘lgan tahdidlar, asosan, faqat standart dasturiy ta’minot va apparat vositalaridan foydalangan holda o‘z vakolatlarini kengaytirish va axborot xavfsizligi choralarini yengib o‘tishga urinishlar bilan bog‘liq. Asosiy sabab — xudbin qiziqish.
Ta’sirga duchor bo‘lgan himoya obyektlari	kirish huquqi berilgan axborot tizimlari
Cheklovchi choralar va qarshi kurash usullari	huquqlarni farqlash va himoya qilinadigan obyektlarga kirishni nazorat qilish; axborot tizimlarida foydalanuvchi harakatlarini hisobga olish
5. Himoya tizimini chetlab o‘tib, tashqi tarmoq orqali himoyalangan obyektga ruxsatsiz mantiqiy kirish huquqiga ega bo‘lgan buzg‘unchilar	
Tajriba	C toifasi (tasniflangan foydalanuvchi)
Imkoniyatlar	ikkinchi (o‘rta), uchinchi (yuqori) yoki to‘rtinchi (juda yuqori) daraja
Xarakteri	Maxsus dasturiy ta’minot va apparat vositalari yoki tizimdagi zaifliklarni qo‘llash orqali maqsadli harakatlarni amalga oshirish. Tahdidlarni amalga oshirish uchun faol ta’sir qilish vositalari qo‘llaniladi. Asosiy sabab — xudbin qiziqish yoki o‘zini o‘zi tasdiqlash.
Ta’sirga duchor bo‘lgan himoya obyektlari	Universitetning lokal tarmog‘i hamda ularga ulangan axborot resurslari va axborot tizimlari, shuningdek axborotni qayta ishlash, saqlash va uzatish vositalari.
Cheklovchi choralar va qarshi kurash usullari	ushbu buzg‘unchilarning ruxsat etilmagan harakatlarining oldini olish va bostirishga qaratilgan apparat va dasturiy ta’minotni himoya qilish vositalari majmuasidan foydalanish; tarmoqlar va dasturiy ta’minotdagi zaifliklarni aniqlash va oldini olish.

11. Axborot xavfsizligi choralari

11.1 Universitetda MBBTni qurish uchun axborot xavfsizligining barcha choralari ko‘riladi va ular quyidagilardan iborat:

- huquqiy choralar;
- xulqiy va axloqiy (psixologik) choralar;
- tashkiliy choralar;
- texnologik choralar;
- muhandislik-texnik choralar;
- dasturiy va texnik choralar;
- tashqi foydalanuvchilar bilan munosabatlarda xavfsizlik choralari.

11.2 Huquqiy choralar

11.2.1 Universitetda hamda ularning alohida himoya obyektlarida axborot xavfsizligini ta’minlashning huquqiy choralari, me’yoriy-huquqiy va tashkiliy-ma’muriy hujjatlar to‘plamini (qoidalar, tartiblar, nizomlar, talablar, yo‘riqnomalar, qo‘llanmalar) shakllantirish bilan bog‘liq tegishli ishlarni bajarish orqali amalga oshiriladi.

11.2.2 Axborot xavfsizligi sohasida Universitetning me’yoriy-huquqiy bazasi Axborot xavfsizligi administratori tomonidan shakllantirilishi va saqlanishi kerak.

11.2.3 Universitetning axborot xavfsizligi sohasidagi me’yoriy-huquqiy bazasi – normativ-huquqiy hujjatlarni, shu jumladan, O‘zbekiston Respublikasining xalqaro va davlat standartlarini, Vazirlikning tegishli hujjatlarini, shuningdek, Universitetning ichki hujjatlarini o‘z ichiga olishi kerak.

11.2.4 Universitetning axborot xavfsizligi bo‘yicha ichki hujjatlar quyidagilar:

a) Universitetning 2023-yil 18-apreldagi “Buxoro davlat universitetida axborot-kommunikatsiya texnologiyalarini keng joriy etish va raqamlashtirish jarayonlarini yanada jadallashtirish to‘g‘risida” 177-U-son buyrug‘i;

b) Universitetning 2023-yil 6-maydagi “Buxoro davlat universitetida konfidensial ma’lumotlarga ega hujjatlarni muhofaza qilish, ular bilan ishlashni to‘g‘ri tashkil etish to‘g‘risida” 208-U-son buyrug‘i;

d) Universitetning 2023-yil 23-avgustdagi “Ma’naviy-ma’rifiy, tarbiyaviy va sport sohasidagi ishlarni yanada takomillashtirish to‘g‘risida”gi 420-U-son buyrug‘i asosida ishlab chiqilgan universitetning “Odob-axloq kodeksi”.

11.2.5 Universitetda axborot xavfsizligini ta’minlash uchun ichki me’yoriy hujjatlarni ishlab chiqish Departament boshlig‘i va Axborot xavfsizligi administratori tomonidan amalga oshiriladi.

11.2.6 Axborot xavfsizligi bo‘yicha ichki me’yoriy-hujjatlar va ularda belgilangan talablar Departament boshlig‘i va Axborot xavfsizligi administratori tomonidan Universitet boshqaruv apparati, departament, markaz, bo‘lim xodimlariga, fakultet dekanlari va o‘rinbosarlariga, kafedra mudirlari va professor-o‘qituvchilarga hamda talabalariga yetkazilishi, barcha rahbar va xodimlar belgilangan talablarga qat’iy rioya qilishlari shart.

11.3 Xulqiy va axloqiy (psixologik) choralar

11.3.1 Xulqiy va axloqiy (psixologik) choralar O‘zbekiston Respublikasi Vazirlar Mahkamasining 2022-yil 14-oktabrdagi “Davlat fuqarolik xizmatchilari tomonidan

odob-axloq qoidalariga rioya etilishini ta’minlash bo‘yicha qo‘shimcha chora-tadbirlar to‘g‘risida” 595-son qarori talablari asosida Universitetning 2023 yil 23 avgustdagi “Ma’naviy-ma’rifiy, tarbiyaviy va sport sohasidagi ishlarni yanada takomillashtirish to‘g‘risida”gi 420-U-son buyrug‘i bilan “Odob-axloq kodeksi” va ichki mehnat qoidalari tasdiqlangan. Xodimlarning xatti-harakatlari yuqoridagi hujjatlar bilan tartibga solinadi.

11.3.2 Axborotni himoya qilishning xulqiy va axloqiy (psixologik) jihatdan Universitet rahbariyati va xodimlari, professor-o‘qituvchilari hamda talabalari o‘z kasbiy va ta’lim olish faoliyatini quyidagi prinsiplar asosida amalga oshirishlari kerak:

- qonuniylik;
- fuqarolar huquqlari, erkinliklari va qonuniy manfaatlarining ustuvorligi;
- vatanparvarlik va xizmat burchiga fidoiylik;
- davlat va jamiyat manfaatlariga sodiqlik;
- adolatlilik, halollik va xolislik;
- manfaatlar to‘qnashuviga yo‘l qo‘ymaslik.

11.3.3 Universitet rahbariyati va xodimlari, professor-o‘qituvchilari hamda talabalari quyidagilarga majbur:

- xizmat vazifalarini bajarishda davlat prinsiplari va talablariga qat’iy rioya etish;
- o‘z xizmat vazifalarini vijdonan, yuksak kasbiy darajada bajarish;
- rahbariyat tomonidan berilgan topshiriqlarini o‘z vaqtida va sifatli bajarish;
- o‘z faoliyatini qonun hujjatlarida va ichki hujjatlarida belgilangan lavozim vakolatlari doirasida amalga oshirish;
- o‘z xizmat vazifalarini bajarishda biror-bir shaxslar yoki tashkilotlarga yon bosmaslik va ustunlik bermaslik, ularning ta’siridan mustaqil bo‘lish, fuqarolarning huquqlari, majburiyatlari va qonuniy manfaatlarini hisobga olish, kamsitish holatlariga yo‘l qo‘ymaslik;
- o‘z xizmat vazifalarini bajarishiga to‘sqinlik qiluvchi biror-bir shaxsiy, mulkiy va boshqa manfaatlarning ta’siri bilan bog‘liq bo‘lgan xatti-harakatlarga barham berish;
- normativ-huquqiy hujjat va idoraviy hujjatlarda belgilangan cheklashlar va taqiqlarga rioya qilish, o‘z xizmat vazifalarini og‘ishmay bajarish;
- o‘z xizmat faoliyatiga biror-bir ta’sir ko‘rsatish imkoniyatiga barham berish;
- o‘zlarining xizmat vazifalarini vijdonan bajarishda shubha paydo qilishi mumkin bo‘lgan xulq-atvordan o‘zini tiyish, shuningdek, o‘z obro‘siga yoki Universitet nufuziga zarar yetkazishga qodir bo‘lgan vaziyatlarga yo‘l qo‘ymaslik;
- xizmat mavqeyidan davlat organlari, boshqa tashkilotlar, ularning mansabdor shaxslari, shuningdek, fuqarolar faoliyatiga noqonuniy ta’sir ko‘rsatish uchun foydalanmaslik;
- davlat organida xabarlarni va xizmat axborotlarini taqdim qilishning belgilangan qoidalariga rioya etish;
- korrupsiya holatlariga qarshi kurashishi va ularning profilaktikasiga faol ko‘maklashishi shart;
- kasbiy faoliyati davomida o‘zlariga ma’lum bo‘lgan axborotning saqlanishini va konfidensialligini ta’minlash yuzasidan barcha choralarni ko‘rishlari shart, ularning

oshkor etilganligi uchun ular qonun hujjatlarida belgilangan tartibda javob beradilar.

11.3.4 Xulqiy va axloqiy himoya choralari profilaktik bo‘lib, quyidagilarni o‘z ichiga oladi:

- xodimlar o‘rtasida tushuntirish ishlarini olib borish;
- psixologik monitoring;
- buzg‘unchilarga nisbatan intizomiy choralarni qo‘llash;
- xodimlarni rag‘batlantirish.

11.3.5 Tushuntirish ishlari Axborot xavfsizligi administratori tomonidan bo‘lim boshlig‘i bilan birgalikda Universitet xodimlari o‘rtasida maxsus darslar, o‘quv-seminarlar yoki individual suhbatlar shaklida olib boriladi. Zarurat tug‘ilganda autsorsing xizmatidan foydalanishi yoki sohada yuqori malakaga ega bo‘lgan mutaxassis jalb qilishlari mumkin.

11.3.6 Tushuntirish ishlari quyidagilarga qaratiladi:

- xodimlar Universitet faoliyatiga tahdidlarning ta’siri va yuzaga kelishi mumkin bo‘lgan oqibatlar, shuningdek, buzg‘unchilarga nisbatan qo‘llanilishi mumkin bo‘lgan javobgarlik choralari to‘g‘risidagi tushuntirish ishlarini olib borish;
- xodimlar o‘rtasida Siyosatning elementlari va talablarini bajarish zarurati to‘g‘risida xabardorlikni oshirish;
- xodimlarning axborot xavfsizligini ta’minlash masalalarida bilish darajasi va javobgarlik hissini oshirish;
- axborot xavfsizligini ta’minlash qoidalari va talablariga rioya qilinishini ta’minlaydigan xatti-harakatlar va axloqiy me’yorlarni ishlab chiqish;
- axborot xavfsizligini ta’minlash muammolarini hal qilishda xodimlarning hamjihatligini oshirish.

11.3.7 Tushuntirish ishlari yiliga kamida bir marta Universitetning barcha xodimlari uchun amalga oshiriladi.

11.3.8 Universitetning kadrlar masalasi bo‘yicha mas’ul bo‘linmalari yangi ishga qabul qilinadigan barcha xodimlar bilan konfidensial ma’lumotni oshkor etmaslik haqida kelishuv imzolanishini amalga oshiradi.

11.3.9 Psixologik monitoring ham shaxsga, ham umuman tashkilotga nisbatan qo‘llaniladi. Bu o‘z o‘rnida xodimlar orasidagi har qanday tartibsizliklarni tezda aniqlash, qoidalar va nizomlarga rioya qilish bilan bog‘liq ravishda mas’uliyatli va vijdonli xodimlarni shu bilan birga, mas’uliyatsiz va beparvo xodimlarni aniqlashga imkon beradi.

11.3.10 Xodimlar axborot xavfsizligini ta’minlash bo‘yicha qoidalar va talablarni bajarishga majbur bo‘ladigan sharoitlarni yaratishga, ya’ni ular buzilgan taqdirda o‘rnatilgan ichki tartib asosida jazo choralari qo‘llaniladi.

11.3.11 Universitet rahbariyati tomonidan mehnat shartnomalari doirasida mehnat qonunchiligiga muvofiq buzg‘unchilarga nisbatan tanbeh yoki jarima shaklidagi intizomiy choralar qo‘llanilishi mumkin. Universitet rahbariyatining xodimlar o‘rtasida xulq-atvorini tartibga solish yuzasidan huquq va majburiyatlari O‘zbekiston Respublikasi Vazirlar Mahkamasining 2022-yil 14-oktabrdagi “Davlat fuqarolik xizmatchilari tomonidan odob-axloq qoidalariga rioya etilishini ta’minlash bo‘yicha qo‘shimcha chora-tadbirlar to‘g‘risida” 595-son qarorida batafsil keltirilgan.

11.4 Tashkiliy choralar

11.4.1 Universitetda tashkiliy tadbirlar quyidagilarga qaratiladi:

- bo‘linmalar va xodimlar o‘rtasida vazifalar va majburiyatlarni taqsimlash;
- muhofaza qilish obyektlarini aniqlash va tasniflash, axborot xavfsizligi xatarlarini tahlil qilish va baholash;
- konfidensial ma’lumotlarni himoya qilish va oshkor qilmaslik;
- axborotni himoya qilish tizimi va vositalarini yaratish va rivojlantirish;
- axborot xavfsizligi bilan bog‘liq hodisalarga javob berish;
- xodimlarning axborot xavfsizligi sohasidagi malakasi va xabardorligini oshirish;
- xavfsizlik darajasini baholash;
- jismoniy himoyani ta’minlash.

11.4.2 Universitet xodimlari o‘rtasida vazifalar va majburiyatlarni taqsimlash bo‘yicha quyidagi tashkiliy choralar ko‘riladi:

a) Lokal tarmoq, Axborot tizimi va Axborot xavfsizligi administratorlarini (keyingi o‘rinlarda)belgilash;

b) konfidensial ma’lumotlar, lokal tarmoq, tarmoq qurilmalari, axborot tizimlari va resurslari, axborot xavfsizligi vositalarini o‘z ichiga olgan axborotlashtirish obyektlariga jismoniy va mantiqiy kirish huquqini olgan shaxslar ro‘yxatini shakllantirish;

d) ma’lumotlarni qayta ishlash, saqlash, uzatish va himoya qilishning aniq vositalarining ishlashi uchun javobgar shaxslarni belgilash;

e) tegishli tashkiliy va ma’muriy hujjatlar bilan xodimlar uchun ma’lumotlarni saqlovchi va tashuvchi vositalarini biriktirish;

f) Axborot xavfsizligi administratori hamda Bo‘lim boshlig‘i tomonidan lokal tarmoq va tizim administratorlariga yuklatilgan vazifalarni bajarilishini nazorat qilish.

Axborot xavfsizligini ta’minlash uchun mas’ul rahbar va xodimlar o‘rtasida vazifalar hamda javobgarlikni taqsimlash Siyosatning 14-bo‘limiga muvofiq amalga oshirilishi kerak.

Lokal tarmoq administratori yo‘riqnomasi ushbu siyosatning 3-ilovasiga muvofiq, Axborot tizimi administratori yo‘riqnomasi 4-ilovaga muvofiq, Axborot va kiberxavfsizlikni ta’minlash bo‘yicha mas’ul xodimning yo‘riqnomasi ushbu Siyosatning 5-ilovada keltirilgan.

Shu bilan birga Universitet raqamli infratuzilmasini rivojlantirish, uning uzluksiz ishlashini nazorat qilish shu bilan birga, ushbu axborot va kiberxavfsizligini ta’minlash ushbu siyosatning 6-ilovasi “Axborot xavfsizligini ta’minlash sektori va Raqamli ta’lim texnologiyalari departamentining Universitet infratuzilmasida axborot va kiberxavfsizlikni ta’minlash sohasidagi vazifalarini amalga oshirish to‘g‘risidagi nizom”da belgilangan.

11.4.3 Himoya obyektlarini aniqlash va tasniflash, axborot xavfsizligi riskini tahlil qilish va baholash bo‘yicha quyidagi tashkiliy choralar ko‘riladi:

a) muhofaza qilish obyektlari va axborot aktivlarini aniqlash uchun inventarizatsiya o‘tkazish;

b) muhofaza qilish obyektlari ro‘yxatini va axborot aktivlari (resurslari) Reestrini shakllantirish, har bir obyekt yoki resurs uchun himoya sinfini aniqlash;

d) ushbu Siyosatning 9-bo‘limiga muvofiq har bir himoya obyekti uchun tahdid modelini aniqlash va axborot xavfsizligi riskini baholash.

Axborot aktivlarini (resurslarini) inventarizatsiya qilish, tasniflash va Reestrini shakllantirish ushbu Siyosatning 14-ilovasida keltirilgan axborot aktivlarini boshqarish tartibiga muvofiq amalga oshiriladi.

Inventarizatsiya Universitetda Axborot xavfsizligi administratori, Universitet tuzilmalarida tashkilot rahbari tomonidan mas’ul bo‘linmalari bilan birgalikda yiliga kamida bir marta tashkil etiladigan va amalga oshiriladigan ichki audit doirasida amalga oshiriladi. Inventarizatsiya natijalariga ko‘ra, agar kerak bo‘lsa, muhofaza qilish obyektlari ro‘yxatiga va Universitet axborot aktivlari Reestriga o‘zgartirish va qo‘shimchalar kiritiladi.

11.4.4 Konfidensial ma’lumotlarni himoya qilish va oshkor qilmaslik bo‘yicha quyidagi tashkiliy choralar ko‘riladi:

a) konfidensial ma’lumotlar ro‘yxatini tuzish va tasdiqlash;

b) konfidensial ma’lumotlar ro‘yxatiga kiritilgan har bir toifadagi ma’lumotlar bilan tanishishga ruxsat berilgan shaxslar ro‘yxatini aniqlash va tasdiqlash;

d) mehnat shartnomalarida konfidensial ma’lumotlarni oshkor qilish va yo‘qotish uchun javobgarlik talablarini belgilash hamda har bir xodim bilan konfidensial ma’lumotni oshkor etmaslik haqida kelishuv imzolash;

e) xodimlarni ishga olishda konfidensial ma’lumotlar ro‘yxati bilan tanishtirish va uni oshkor qilish va yo‘qotish uchun javobgarlik choralari mavjudligini imzo qo‘yish yo‘li bilan tanishtirish.

Konfidensial ma’lumotlarni oshkor qilmaslik bo‘yicha xodimlarning javobgarligi bo‘yicha majburiyatlari “Konfidensial ma’lumotlarini oshkor qilmaslik to‘g‘risidagi Nizomda” belgilanadi.

11.4.5 Axborotni muhofaza qilish tizimi va vositalarini joriy etilishi, ishlashi va rivojlanishi bilan bog‘liq quyidagi tashkiliy choralar ko‘riladi:

a) axborot xavfsizligini ta’minlash bo‘yicha chora-tadbirlarni amalga oshirish doirasida axborot xavfsizligi vositalarini joriy etish;

b) joriy qilingan axborot xavfsizligi vositalariga texnik talablarni ishlab chiqish;

d) tizimni va axborotni muhofaza qilish vositalarini joriy etish va saqlashga tayyorgarlik ko‘rish bo‘yicha binolarni ajratish, foydalanish bo‘yicha ko‘rsatmalarni ishlab chiqish, mas’ul javobgar xodimni tayinlash va xodimning malaka oshirishini o‘z ichiga olgan tashkiliy tadbirlarni amalga oshirish;

e) axborot xavfsizligi vositalarini joriy qilishda eksperimental, ekspluatatsion va qabul sinovlarini o‘tkazish;

f) himoya qilish tizimini boshqarish, shu jumladan sozlamalarni boshqarish, ish qobiliyatini tiklash, dasturiy ta’minot yangilanishlarini o‘rnatishni boshqarish, operatsion hujjatlarni tuzatish, xavfsizlik hodisalarini nazorat qilish, jarayonlar va nazorat natijalarini hujjatlashtirish;

g) ekspluatatsiya va xavfsizlikni ta’minlashda kamchiliklar mavjud bo‘lganda axborot xavfsizligi tizimini takomillashtirish bo‘yicha takliflarni tayyorlash va taqdim etish.

11.4.6 Axborot xavfsizligi bilan bog‘liq hodisalarni aniqlash, oqibatlarini bartaraf

etish va tekshiruvlarni o‘tkazish nuqtai nazaridan tashkiliy choralar ko‘riladi, ular 12-bo‘limda, shuningdek, ushbu Siyosatning 19-ilovasida “Hodisalar va favqulodda vaziyatlarni boshqarish, shuningdek, uchinchi tomon tashkilotlari bilan o‘zaro aloqalar bo‘yicha reglament”da keltirilgan.

11.4.7 Axborot va kiberxavfsizlikni ta’minlash sohasida xodimlarning malakasini va xabardorligini oshirish nuqtai nazaridan quyidagi tashkiliy choralar ko‘riladi:

a) axborot xavfsizligini ta’minlash uchun mas’ul bo‘lgan xodimlarni kamida bir yilda bir marta malakasini oshirish;

b) Universitet xodimlarini xabardorligini oshirish va ushbu Siyosat talablari va qoidalarini bajarish maqsadida trening yoki o‘quv-seminarlarni tashkil etish va o‘tkazish;

d) Universitet xodimlarini ularning xabardorlik darajasini tekshirish bo‘yicha mashg‘ulotlar natijalari bo‘yicha sertifikatlash;

e) Universitetning har bir xodimini ushbu Siyosatning kerakli bo‘limlari bilan mazkur Siyosatning 21-ilovasida keltirilgan jurnalga imzo qo‘yish yo‘li bilan tanishtirish.

f) Axborot xavfsizligini ta’minlash uchun mas’ul xodimlarning malakasini doimiy oshirib borish.

Universitet xodimlarini axborot xavfsizligi masalalari bo‘yicha bilim va ko‘nikmalarini oshirish maqsadida, Axborot xavfsizligi administratori mas’ul bo‘linmalar bilan birgalikda har yili tashkil etiladigan o‘quv-seminarlar jadvalini tuzadi va tasdiqlash uchun Mas’ul rahbarga kiritadi.

11.4.8 Xavfsizlik darajasini baholash bo‘yicha quyidagi tashkiliy choralar ko‘riladi:

a) muhofaza qilinadigan obyektlarni muhofaza qilish darajasini baholash uchun ichki va tashqi auditlarni o‘tkazish;

b) O‘zbekiston Respublikasi Prezidentining 2011-yil 8-iyuldagi “Milliy axborot resurslarini muhofaza qilish bo‘yicha chora-tadbirlari to‘g‘risida”gi PQ-1572-son qaroriga muvofiq akkreditatsiyadan o‘tgan tashkilotlar tomonidan Universitetning axborotlashtirish obyektlarini attestatsiyadan o‘tkazish;

d) Universitet rasmiy veb-saytlari hamda axborot tizimlarini axborot xavfsizligi talablariga muvofiqligini ekspertizadan o‘tkazish;

e) tashkiliy, texnik va boshqa himoya choralarining samaradorligini baholash, shuningdek, ekspertiza va attestatsiyalar natijalariga ko‘ra aniqlangan kamchiliklarni bartaraf etish.

Ichki auditning muntazamligi yiliga kamida bir marta, tashqi audit esa kamida uch yilda bir marta o‘tkazilishi lozim.

Ichki audit Universitetning mas’ul bo‘linmalari, Universitet tuzilmalari mas’ul xodimlari bilan birgalikda Axborot xavfsizligi administratori hamda Bo‘lim boshlig‘i tomonidan amalga oshiradi. Axborot xavfsizligining tashqi auditini o‘tkazish uchun bunday auditni o‘tkazishga vakolatli uchinchi tomon tashkilotlari jalb qilinadi.

11.4.9 Jismoniy himoyani ta’minlash bo‘yicha quyidagi tashkiliy choralar ko‘riladi:

a) Universitet joylashgan binolar hududiga kirish joyida biometrik

autentifikatsiyaga asoslangan kirishni nazorat qilish tizimlarini tashkil etish;

b) axborotlashtirish obyektlarini nazorat qilinadigan hudud chegarasiga nisbatan mumkin bo‘lgan maksimal masofada joylashtirish;

d) axborotni qayta ishlash, saqlash, uzatish va himoya qilish uchun asosiy texnik vositalarni (axborot resurslari serverlari, tarmoq qurilmalari, axborot xavfsizligi vositalarini) himoyalangan server xonalarida joylashtirish;

e) kommutatsiya jihozlarini qulflanadigan shkaflarda, shuningdek, server xonalarida joylashtirish;

f) hujjatlashtirilgan konfidensial ma’lumotlarni va axborot tashuvchi va saqlovchi vositalarni seyflarda, shkaflarda yoki boshqa muhofaza qilinadigan omborlarda saqlash hamda ushbu vositalarini hisobini yuritish.

11.5 Texnologik (texnik) choralar

11.5.1 Universitetda axborot xavfsizligini ta’minlash bo‘yicha texnologik (texnik) tadbirlar quyidagilarga qaratiladi:

- axborotni qayta ishlash va saqlash vositalarining normal ishlashi uchun yong‘in xavfsizligi va iqlim sharoitlarini ta’minlash;
- axborotni qayta ishlash, saqlash, uzatish va himoya qilishning texnik vositalarini zaxiralash;
- aloqa kanallarini zaxiralash;
- axborot tizimlari va resurslarini zaxiralash;
- kafolatlangan elektr ta’minoti bilan ta’minlash;
- himoya qilinadigan obyektlarni axborot xavfsizligini ta’minlash.

11.5.2 Universitet serverlarida joylashgan axborot tizimlari va resurslari Universitetning server xonasida joylashgan alohida ma’lumotlarni saqlash tizimi (NAS)ga avtomat tarzda belgilangan muddatlarda Universitetning Raqamli ta’lim texnologiyalari departamenti xodimlari tomonidan zaxiraga olinadi va saqlanadi.

11.5.3 Axborotni qayta ishlash, saqlash, uzatish va muhofaza qilish vositalarini, shuningdek, aloqa kanallari ishdan chiqqanda tezkor qayta tiklashni ta’minlashga qo‘yiladigan talablar ushbu Siyosatning 18-ilovasi “Favqulodda vaziyatlarda ish faoliyatini tiklashni va uzluksiz ishlashni ta’minlash rejasi”da belgilangan.

11.5.4 Universitetda mavjud axborot tizimlari va resurslari, shuningdek, tarmoq qurilmalari va axborot xavfsizligi obyektlarining sozlamalari zaxiraga olinadi. Ma’lumotlarni uzatish tarmog‘ining quvvati har kuni ish vaqtidan tashqari (soat 18:00 dan ertasi soat 09:00 gacha) tegishli server xonalarida ma’lumotlarni zaxiralash jarayonini muvaffaqiyatli yakunlashi kerak. Ma’lumotlarning zaxira nusxasini yaratish va tiklash ushbu Siyosatning 7-ilovasida keltirilgan “Tizim va amaliy dasturlarni yangilash, shuningdek, ma’lumotlarning zaxira nusxalarini shakllantirish va tiklash bo‘yicha nizom”ga muvofiq amalga oshiriladi.

11.5.5 Himoyalangan obyektlarni ishlatish vaqtida axborot xavfsizligini ta’minlash yoki axborotni qayta ishlashni tugatish to‘g‘risida Universitet rahbariyati bilan kelishilgan holda qaror qabul qilingandan so‘ng, axborot tashuvchilaridan ma’lumotlarni va barcha qoldiq ma’lumotlarni yo‘q qilish va/yoki jismoniy tashuvchilarni xavfsiz yo‘q qilish bo‘yicha zarur choralar ko‘riladi.

11.5.6 Ma’lumotlarni saqlovchi va tashuvchi tashqi qurilmalarni xavfsiz yo‘q

qilish Siyosatning 10-ilovasida keltirilgan “Mobil, ma’lumot saqlovchi va tashuvchi qurilmalar bilan ishlashda axborot xavfsizligini ta’minlash bo‘yicha yo‘riqnoma”ga muvofiq amalga oshiriladi.

11.5.7 Konfidensial ma’lumotlar bo‘lgan qog‘oz ko‘rinishidagi hujjatlar maxsus maydalagich (shreder) yordamida yo‘q qilinishi mumkin.

11.6 Muhandis-texnik choralar

11.6.1 Muhandis-texnik tadbirlar himoya qilinadigan obyektlarga ruxsatsiz shaxslarning kirishi uchun jismoniy kirishni oldini olish yoki to‘siqlar yaratishga qaratilgan va quyidagi tadbirlarni o‘z ichiga oladi:

1) Universitet joylashgan binolarga xodimlarning kirishini boshqarish tizimidan (keyingi o‘rinlarda – Face ID) foydalanish.

- hozirgi vaqtda Face ID tizimi Universitet (Buxoro viloyati, Buxoro shahri, M.Iqbol ko‘chasi, 11-uy) joylashgan binoda mavjud;

2) Universitet joylashgan binoda 770 ta videokuzatuv kameralari mavjud bo‘lib, arxiv 15-20 kun saqlanadi. Nazorati Universitetning Departament xodimlari tomonidan amalga oshiriladi.

3) konfidensial ma’lumotlar qayta ishlanadigan xonalarga (muzokaralar xonasi va boshqalar) qo‘riqlash signalizatsiya tizimini o‘rnatish;

4) hujjatlashtirilgan konfidensial ma’lumotlar va konfidensial ma’lumotlarni saqlovchi va tashuvchi vositalarni saqlash uchun qulflanadigan yong‘inga chidamli shkaflar yoki seyflardan foydalanish;

5) ish stansiyalari va tarmoq qurilmalariga jismoniy kirishni cheklash (blokirovka) uchun muhrlardan foydalanish;

6) tarmoq qurilmalarini va axborotni muhofaza qilish vositalarini mexanik qulf bilan qulflangan maxsus javonlarga o‘rnatish;

7) tarmoq kabellarini ushbu Siyosatning 13-bo‘limi talablariga asosan binolar ichkarisida va tashqarisida muhofaza qilinadigan joylarda yotqizish.

11.7 Dasturiy-apparat choralari

11.7.1 Universitetning axborot xavfsizligini ta’minlash bo‘yicha apparat-dasturiy choralar quyidagilarga qaratilgan:

- axborotni texnik muhofaza qilishni tashkil etish;
- axborotning kriptografik himoyasini tashkil etish.

11.7.2 Axborotni texnik muhofaza qilishni ta’minlash uchun axborotni quyidagi texnik muhofaza qilish vositalari qo‘llaniladi:

- tarmoqlararo ekranlar;
- IDPS vositalari;
- virusga qarshi himoya vositalari;
- kirishni boshqarish vositalari va boshqalar.

11.7.3 Universitet O‘z DSt ISO/IEC 27039:2017 “Axborot texnologiyasi. Xavfsizlikni ta’minlash usullari. Bostirib kirishni aniqlash tizimlarini tanlash, qo‘llash va tizim operatsiyalari” davlat standartiga muvofiq bostirib kirishdan himoya qilish choralarini ta’minlashi kerak, ularga quyidagilar kiradi:

- Universitetning lokal tarmog‘ini tashqi tarmoqlarga ulashda IDPS tarmoq vositalaridan foydalanish;

- Internet tarmog‘iga kirish ta’minlangan ish stansiyalarida xost IDPS (HIPS) dan foydalanish;

- talablarni aniqlash va IDPS vositalarini tanlash;

- ularga tezkor javob berish uchun IDPS vositalari tomonidan aniqlangan bostirib kirishlarni monitoring qilish vositalarini joriy etish.

11.7.4 Axborot xavfsizligi risklaridan kelib chiqqan holda, Universitet IDPS apparat va dasturiy ta’minot tarmog‘i vositasidan quyidagi talab va funksiyalarga ega bo‘lishi kerak:

- barcha protokollar bo‘yicha tarmoq trafik paketlarini chuqur tahlil qilish;

- Universitetning barcha tashqi tarmoq trafigini qayta ishlash (paketlarni chuqur tahlil qilish) va uzatishni ta’minlovchi ko‘rsatkichlarga ega bo‘lishi;

- tarmoq trafigida tarmoq tajovuzlarini aniqlash uchun signatur usulni qo‘llab-quvvatlash;

- ishlab chiqaruvchidan signatur ma’lumotlar bazasini yangilash imkoniyatiga ega bo‘lish:

- trafikdagi anomaliyalar va tarmoq protokollaridagi anomaliyalar asosida tarmoq trafigiga tarmoq tajovuzlarini aniqlashning xatti-harakatlar usulini qo‘llab-quvvatlash;

- shubhali trafikni bloklash va filtrlash;

- DoS va DDoS hujumlaridan himoya qilish funksiyasiga ega bo‘lishi;

- zararli koddan tarmoq trafigini aniqlash va filtrlash funksiyasiga ega;

- IDPS obyektining yaxlitligini nazorat qilish uchun boshqaruv funksiyasiga ega bo‘lishi;

- oddiy tarmoq boshqaruvi (administrator) protokoliga ega bo‘lish;

- aniqlangan va oldi olingan bosqinlar haqida xabar berish.

IDPS vositasi butun ichki lokal tarmoqni hamda Universitet serverlari va ularga ulangan ishchi stansiyalarini Universitet ulangan tashqi tarmoqdan kelib chiqadigan tashqi tarmoq tahdidlaridan himoya qilishi kerak.

Tarmoqlararo ekran tashqi tarmoq va lokal tarmoq ulanishi chegarasida marshrutizatordan kelayotgan kiruvchi tarmoq trafigini boshqarishni ta’minlaydi.

11.7.5 Universitetning lokal tarmoqqa ulangan ishchi stansiyalari va muhim serverlarida quyidagi talab va funksiyalarga ega HIPSni o‘rnatishi kerak:

- jarayonlarni, dasturlarni, fayllarni va operatsion tizimda ishlayotgan registrni monitoring qilishda kiruvchi faollikni aniqlash orqali tarmoqqa tajovuzlarni aniqlashning xatti-harakatlar usuliga ega bo‘lish;

- kiruvchi faoliyatni aniqlash uchun tarmoqni filtrlash imkoniyatiga ega bo‘lish;

- o‘zingizni zararli kod hujumlaridan himoya qila olishi;

- ilovalarni himoya qilish uchun ekspluatatsiyani blokirovka qilish funksiyasiga ega bo‘lishi;

- foydalanuvchiga kiruvchi faoliyat aniqlanganda fayllar, ilovalar va reestr bilan amallarni tanlash imkoniyatini taqdim etish.

HIPS sifatida Universitetda qo‘shimcha HIPS funksiyasiga ega bo‘lgan virusga qarshi himoya tizimidan foydalanadi.

HIPS ishlashi uchun antivirus ish stansiyalari va serverlarda mos ravishda sozlash.

11.7.6 Universitetda qo‘llaniladigan axborotni texnik muhofaza qilish usullari va vositalari, axborot xavfsiziligi siyosatining 13-ilovasidagi Axborotni texnik muhofaza qilishni tashkil etish bo‘yicha yo‘riqnomada keltirilgan.

11.7.7 Tarmoq infratuzilmasi xavfsizligini ta’minlash va tarmoqlararo ekranlardan foydalanish, axborot xavfsiziligi siyosatining 2-ilovasida keltirilgan Tarmoq infratuzilmasi va tarmoqlararo ekran darajasida axborot xavfsizligini ta’minlash to‘g‘risida nizomga muvofiq amalga oshiriladi.

11.7.8 Zararli dasturlardan himoya qilish, axborot xavfsiziligi siyosatining 7-ilovasida keltirilgan Antivirus himoyasi bo‘yicha yo‘riqnoma muvofiq texnik choralar ko‘riladi.

11.7.9 Universitetning axborot resurslariga kirishni tartibga solish axborot xavfsiziligi siyosatining 9-ilovasida keltirilgan Axborot manbalariga kirish matritsasini ishlab chiqish qoidalariga muvofiq amalga oshiriladi.

Universitet barcha AKT xizmatlaridan foydalanishni ta’minlash va javobgarlik doirasini belgilash maqsadida Universitetning har bir xodimiga taqdim etiladigan korporativ domenning foydalanuvchi qayd yozuvlari yordamida kirishni boshqarish vositalaridan foydalanadi.

11.7.10 Himoyalangan obyektlarga kirishda foydalanuvchilarning autentifikatsiyasi parollar va boshqa identifikatorlar, axborot xavfsiziligi siyosatining 6-ilovasida keltirilgan Parolli himoya bo‘yicha yo‘riqnoma muvofiq ishlab chiqariladi va foydalaniladi.

11.7.11 Universitetda axborotni kriptografik muhofaza qilish kriptografik ma’lumotlarni himoya qilish vositalari yordamida tashkil etilgan. Ma’lumotlarni uzatishda himoyalangan E-xat va E-ijro tizimlaridan foydalaniladi.

11.7.12 Universitet O‘zbekiston Respublikasi Prezidentining 2007 yil 3 apreldagi PQ-614-sonli farmoniga binoan kriptografik ma’lumotlarni himoya qilish vositalari uchun sertifikatlash organi tomonidan sertifikatlangan AKHVdan foydalanishi shart.

11.7.13 Universitetda axborotni kriptografik himoya qilish usullari va vositalari, axborot xavfsiziligi siyosatining 14-ilovasida keltirilgan “Axborotni kriptografik himoya qilishni tashkil etish bo‘yicha yo‘riqnoma”ga muvofiq amalga oshirilishi kerak.

11.8 Tashqi foydalanuvchilar bilan ishlashda xavfsizlik choralari

11.8.1 Tashqi foydalanuvchilar bilan ishlashda xavfsizlik choralari quyidagilarga qaratiladi:

- himoya qilish obyektlariga tashqi foydalanuvchilarning ruxsatsiz jismoniy kirishini istisno qilish;
- axborot tizimlari va resurslariga kirishda tashqi tashkilotlarning foydalanuvchilari tomonidan ruxsatsiz tarmoqqa kirishni istisno qilish.

11.8.2 Tashqi foydalanuvchilar bilan ishlashda xavfsizlik choralariga quyidagilar kiradi:

- tashrif buyuruvchilarning kelishi va ketishi jurnalini yuritish;
- xodimlar tomonidan bino ichida mehmonlarni kuzatib borish;
- tashrif buyuruvchilarni va uchinchi tomon tashkilotlarini alohida qabul

xonalarida qabul qilish;

- Universitet uchun dasturiy ta’minot va qurilmalarni ishlab chiqish, texnik xizmat ko‘rsatish yoki yetkazib berish bilan shug‘ullanuvchi uchinchi tomon tashkilotlari bilan tuzilgan shartnomalarda konfidensial ma’lumotlarni uchinchi shaxslarga tarqatmaslik talablarini belgilash.

11.8.3 Ishlab chiquvchilar, qurilmalarni yetkazib beruvchilar va shu kabi uchinchi tomon tashkilotlari xodimlari Universitetning himoya qilinadigan obyektlariga kirishni ta’minlashda ular bilan tuzilgan shartnomalarda “Konfidensial ma’lumotlarni oshkor etmaslik” shartlari va talablarini qat’iy belgilash. Shuningdek, uchinchi tomon tashkiloti tomonidan himoya obyektlariga kirish huquqini beradigan aniq shaxslar ro‘yxati aniqlanishi lozim va bunday ruxsat faqat shu shaxslarga berilishi shart.

11.8.4 Muhofaza qilish obyektlariga qabul qilingan uchinchi tomon tashkilotlari vakillari mas’ul xodim huzurida va nazoratida bo‘lishi hamda o‘ziga tegishli vazifani bajarishi shart.

11.8.5 Axborot tizimlari va resurslarga kirishda tashqi foydalanuvchilarning tarmoqdan ruxsatsiz kirishini istisno qilish maqsadida, ushbu Siyosatning 2-ilovasida keltirilgan “Tarmoq infratuzilmasi va tarmoqlararo ekran darajasida axborot xavfsizligini ta’minlash to‘g‘risida nizom”ga muvofiq, shuningdek, axborot tizimlari va resurslarga kirishda foydalanuvchining autentifikatsiyasi ushbu Siyosatning 8-ilovasida keltirilgan “Parolli himoya bo‘yicha yo‘riqnoma”ga muvofiq amalga oshiriladi.

12. Axborot xavfsizligi hodisalariga munosabat

12.1 AXBTni qurishdagi muhim jarayonlardan biri axborot xavfsizligi hodisalarini boshqarish jarayonidir.

Universitetda axborot xavfsizligi hodisalarini boshqarish “O‘zbekiston Respublikasi Raqamli texnologiyalar vazirligi bilan axborot xavfsizligi insidentlariga ta’sir etish, tekshirish va oldini olish bo‘yicha davlat va xo‘jalik boshqaruvi organlari o‘rtasidagi o‘zaro hamkorlik reglamenti”ga (keyingi o‘rinlarda – Hamkorlik reglamenti) muvofiq amalga oshiriladi.

12.2 Axborot xavfsizligi hodisalarini boshqarish jarayonining asosiy vazifalari yo‘qotishlarni minimallashtirish, shu jumladan, hodisalarini tezkorlik bilan aniqlash va takrorlanuvchi hodisalar riskini kamaytirishdir.

12.3 Axborot xavfsizligi hodisalarini boshqarish jarayonining asosiy vazifalari quyidagilardan iborat:

- axborot xavfsizligi hodisalarini tezkor aniqlash;
- axborot xavfsizligi hodisalarini tahlil qilish;
- axborot xavfsizligi hodisalarini ro‘yxatga olish;
- axborot xavfsizligi hodisalariga munosabatni muvofiqlashtirish va rahbariyatni va zarur bo‘lganda Hamkorlik reglamentiga muvofiq manfaatdor tashqi (masalan “Kiberxavfsizlik markazi” DUK) tashkilotni xabardor qilish;
- hodisalarning manbalari va sabablarini aniqlash, shuningdek, ularning oqibatlarini baholash;
- Universitetda hodisa aniqlangandan so‘ng, axborot xavfsizligi buzilishi

to‘g‘risida ishonchli va to‘liq ma’lumot olish hamda uning oqibatlarini baholash;

- ish tartibini buzish, axborot tizimlari va resurslariga yetkazilgan zararni minimallashtirish, axborot xavfsizligi hodisasi natijasida axborot tizimlari va resurslari, lokal tarmoq va axborot tizimlari va resurslari ishlamay qolgan taqdirda ularning faoliyatini qisqa vaqt ichida qayta tiklash;

- axborot xavfsizligi hodisasining oqibatlarini bartaraf etish natijalarini tahlil qilish;

- axborot xavfsizligi bilan bog‘liq hodisalar bo‘yicha tekshiruvlar o‘tkazish, axborot xavfsizligi hodisalari dalillarining xavfsizligi va yaxlitligini ta’minlash, sodir bo‘lgan axborot xavfsizligi hodisalari to‘g‘risida aniq ma’lumotlarni to‘plash va saqlash uchun sharoit yaratish;

- axborot xavfsizligi bilan bog‘liq hodisalarning takrorlanishini oldini olish bo‘yicha tavsiyalar va choralarni ishlab chiqish;

- Universitet xodimlarini axborot xavfsizligi hodisalarini aniqlash, oqibatlarini bartaraf etish va oldini olish bo‘yicha harakatlarga o‘rgatish va favqulodda vaziyatlarda tiklash rejalarini ishlab chiqish.

Universitetda Axborot xavfsizligi hodisalarini qayd etish jurnali shakli Siyosatning 20-ilovasida keltirilgan.

12.4 Universitetda axborot xavfsizligi hodisalarini aniqlash, oqibatlarini bartaraf etish va tekshiruvlar o‘tkazish uchun quyidagi tashkiliy-texnik tadbirlarni amalga oshirish kerak:

- hodisalarni aniqlash va ularga javob berish uchun mas’ullarni aniqlash;

- axborot xavfsizligi hodisalarini aniqlash va boshqarish uchun axborot xavfsizligi hodisalarini boshqarish tizimidan (SIEM) foydalanish;

- muhim muhofaza qilish obyektlarining Axborot xavfsizligi hodisalarini qayd etish jurnalini yuritish;

- har bir muhim himoya obyekti bo‘yicha Bo‘lim va boshqa manfaatdor bo‘linmalar mutaxassislaridan axborot xavfsizligi hodisalariga javob berish va tekshiruvlar o‘tkazish uchun javob guruhini tashkil etish;

- hodisalarni tahlil qilish, shu jumladan hodisalarning manbalari va sabablarini aniqlash, shuningdek, ularning oqibatlarini baholash;

- zarur hollarda huquqni muhofaza qiluvchi organlarni jalb qilgan holda sodir bo‘lgan hodisalar yuzasidan tekshiruvlar o‘tkazish;

- hodisalarni va ularning oqibatlarini bartaraf etish bo‘yicha chora-tadbirlarni amalga oshirish va hodisalarning takrorlanishini oldini olish uchun choralar ko‘rish.

Shuningdek, axborot xavfsizligi bilan bog‘liq hodisalarni ro‘yxatga olish jurnallari barcha obyektlarda tashkil etilishi va doimiy yuritilishi shart.

12.5 Axborot xavfsizligi to‘g‘risidagi hodisalar jurnaliga yuzaga kelgan barcha axborot xavfsizligi hodisalari qayd etiladi.

Axborot xavfsizligi hodisalarini qayd etish va Favqulodda (avariyaviy) vaziyatlarni hisobga olish jurnallarida hodisalar sodir bo‘lgan sana va vaqt, hodisalar turi, hodisaga bog‘liq bo‘lgan himoya obyektlari va oqibatlarning mohiyati ko‘rsatilishi kerak.

Kutilayotgan va haqiqiy axborot xavfsizligi hodisalarini to‘liq tahlil qilish uchun

jurnalda favqulodda vaziyatlar va dolzarb axborot xavfsizligi hodisalari to‘g‘risida yetarli miqdorda ma’lumot yozilishi zarur.

12.6 Universitetda Axborot xavfsizligi hodisalarini qayd etish jurnali Axborot xavfsizligi administratorlari tomonidan yuritiladi.

12.7 Universitetda axborot xavfsizligining quyidagi hodisalari qayd etiladi va hisobga olinadi:

- axborot tizimlari va resurslari faoliyatiga ruxsatsiz aralashuv natijasida tizimning ishlamay qolishi;
- rasmiy veb-saytlarning asosiy sahifasini ruxsatsiz o‘zgartirish (deface);
- keyinchalik zararli kontentni joylashtirish bilan axborot resursi fayl tizimiga ruxsatsiz kirish;
- axborot tizimiga bo‘lgan DoS va DDoS hujumlari;
- axborot tizimining ishlash qoidalarini buzish;
- axborot tizimiga ruxsatsiz kirish;
- axborot tizimi va resurslari himoyasini buzish;
- axborot tizimi va resurslarida saqlanayotgan ma’lumotlarni o‘zgartirish, shikastlash, yo‘q qilish, shuningdek, ushbu ma’lumotlar egasining yoki qonuniy egasining ruxsatisiz unga ataylab yolg‘on ma’lumotlarni kiritish;
- axborot tizimi va resurslari joylashgan server qurilmalari ishiga ruxsatsiz aralashuv;
- mavjud dasturlarga o‘zgartirishlar kiritish orqali axborot tizimi va resurslarida saqlanadigan yoki uzatiladigan ma’lumotlarni ruxsatsiz yo‘q qilish, blokirovka qilish, o‘zgartirish, nusxalash yoki ushlab turish;
- maxsus virusli dasturlarni ishlab chiqish, foydalanish va tarqatish;
- ma’lumotlarning konfidensialligi, yaxlitligi va mavjudligini buzilishi;
- texnologik jarayonning buzilishi;
- favqulodda vaziyatlar (yong‘inlar, toshqinlar va boshqa tabiiy ofatlar yoki ishlab chiqarishdagi baxtsiz hodisalar);
- tashqi tarmoqlar bilan aloqaning yo‘qolishi;
- har qanday sababga ko‘ra asosiy tarmoq, server qurilmalari, axborotni himoya qilish vositalari, ham texnik, ham dasturiy ta’minotning ishlamay qolishi;
- axborot tizimlari va resurslari dasturiy ta’minotining noto‘g‘ri ishlashi;
- uchinchi shaxslarning axborot tizimlari va resurslariga ruxsatsiz kirishi;
- ma’lumotlarni qayta ishlash, saqlash, uzatish bo‘yicha har qanday qoidalarning buzilishi;
- himoya vositalari yordamida aniqlangan tarmoq hujumlari;
- g‘ayritabiiy tarmoq faoliyati va g‘ayritabiiy dastur harakati;
- yangi tarmoq tugunlarini ulash va yangi xizmatlarning paydo bo‘lishi;
- ma’lumot tashuvchilar va ma’lumotlarning yo‘qolishi va o‘g‘irlanishi;
- zaifliklarning paydo bo‘lishi;
- ushbu Siyosatda belgilangan qoidalarning buzilishi.

12.8 Axborot xavfsizligini ta’minlash uchun doimiy monitoring olib borilishi va ular quyidagilarni o‘z ichiga olishi kerak:

- tarmoqlararo ekran, marshrutizatorlar, serverlar, ish stansiyalar, operatsion

tizimlar, MBBT va boshqalar (log-fayllar);

- vositalarning holatini vizual nazorat qilish;
- zararli dasturlarga qarshi vositalar, tarmoqlararo ekran va shu kabilarni o‘z ichiga olgan ma’lumotlarni himoya qilish vositalari haqida ma’lumotlar;
- axborot xavfsizligining ichki yoki tashqi auditi natijalari;
- xodimlar va yordamchi xodimlar tomonidan bildirilgan hodisalar to‘g‘risidagi ma’lumotlar.

12.9 Universitetda axborot va kiberxavfsizlik bilan bog‘liq hodisalarni aniqlashga javobgar shaxslar:

- Tarmoqlarni boshqarish va texnik qo‘llab-quvvatlash sektori xodimlari – Universitetning lokal tarmog‘i va tarmoq qurilmalari, ishchi stansiyalariga;
- Raqamli ta’lim texnologiyalarini joriy etish va axborot xavfsizligini taminlash sektori xodimlari – Universitetning ishchi stansiyalariga o‘rnatilgan axborot tizimlari va resurslariga, antiviruslarga, rasmiy veb-saytlarga, tarmoqlararo ekranga.

12.10 Xodimlar axborot xavfsizligi bilan bog‘liq hodisa yuz bergan taqdirda, yo‘nalishi bo‘yicha sektor bosh mutaxassislariga, o‘z navbatda sektor bosh mutaxassislari Departament boshlig‘i hamda Axborot xavfsizligi administratoriga xabar berishlari shart. Ushbu xodimlar hodisalarning oqibatlarini bartaraf etish uchun, ularning oqibatlarini ko‘paytirmaslik uchun ko‘rsatilgan mutaxassislar bilan kelishilmagan harakatlarni qilmasliklari kerak.

12.11 Sektorlar bosh mutaxassislari aniqlangan hodisalar to‘g‘risida Axborot xavfsizligi administratorini to‘liq va aniq ma’lumotlar (vujudga kelish vaqti, tahdidning xususiyati, tahdid sabablari va manbalari, ochiq muhofaza obyektlari, o‘lchovi, oqibatlari, qabul qilingan ustuvor choralar) bilan ta’minlashga majburdir.

12.12 O‘z navbatida, Axborot xavfsizligi administratori va Departament boshlig‘i hodisalar to‘g‘risida ma’lumotni tegishliligi bo‘yicha Axborot xavfsizligi hodisalarini qayd etish jurnaliga yozib qo‘yadi.

12.13 Axborot xavfsizligining muhim nomaqbul va salbiy oqibatlariga olib keladigan axborot xavfsizligi hodisalari yuz berganda, ular haqida Mas’ul rahbarga xabar berish shart.

12.14 Har bir axborot xavfsizligi hodisasi uchun hodisa ro‘y berishining sabablari, tahdid manbai aniqlanadi, oqibatlar ko‘lami baholanadi, tahdidni yo‘q qilish, hodisa oqibatlarini bartaraf etish choralari ko‘riladi, shuningdek, agar lozim topilsa, bunday hodisalarning takrorlanishiga yo‘l qo‘ymaslik uchun xavfsizlikni kuchaytirish bo‘yicha qo‘shimcha choralar ko‘rilishi lozim. Universitet rahbariyati qarori bilan oqibatlarni bartaraf etishga qo‘shimcha mutaxassislar va resurslar jalb qilinadi.

Hodisa oqibatlarini bartaraf etish uchun uchinchi tomon mutaxassislari yoki xizmat ko‘rsatuvchi tashkilot mutaxassislari jalb qilinishi mumkin. Hodisalar oqibatlarini bartaraf etishda tashqi ekspertlar yoki xizmat ko‘rsatuvchi tashkilot mutaxassislari jalb qilingan taqdirda, ular bilan konfidensial axborotlarni oshkor qilmaslik to‘g‘risida kelishuv imzolanishi kerak.

12.15 Aniqlangan axborot xavfsizligi hodisalariga javob berishda “Kiberxavfsizlik markazi” DUK bilan o‘zaro aloqada bo‘lishlari kerak.

12.16 Tekshiruv davomida hodisaning asl sabablari, buzg‘unchilar aniqlanadi va ushbu hodisa takrorlanmasligi uchun tavsiyalar ishlab chiqiladi. Ushbu tavsiyalar asosida Axborot xavfsizligi administratori va Departament boshlig‘i hodisa takrorlanishining oldini olish bo‘yicha choralar ko‘radi va zarur tadbirlarni amalga oshiradi.

12.17 Jiddiy oqibatlarga olib keladigan hodisalarni tekshirishda buzg‘unchilarni javobgarlikka tortish uchun huquqni muhofaza qilish organlari ishtirok etishi kerak.

12.18 Hodisa yuzasidan maxsus tekshiruv o‘tkazish, tashqi manfaatdor tomonlarga xabar berish va huquqni muhofaza qilish idoralarining ishtiroki to‘g‘risida qaror Universitet rahbariyati tomonidan voqeaning oqibatlaridan kelib chiqqan holda qabul qilinadi.

12.19 Axborot xavfsizligi bilan bog‘liq hodisalarga javob berishda mas’ul xodimlar ushbu Siyosatning 19-ilovasida keltirilgan “Hodisalar va favqulodda vaziyatlarni boshqarish, shuningdek, uchinchi tomon tashkilotlari bilan o‘zaro aloqalar bo‘yicha reglament”ga shuningdek, uchinchi tomon tashkilotlari bilan o‘zaro munosabatlarni boshqarish qoidalari asosida ish ko‘riladi.

13. Aloqa kanallarining xavfsizligini ta’minlash

13.1 Ma’lumot uzatish uchun ishlatiladigan elektr va tarmoq kabellari ma’lumotni o‘g‘irlash va buzilishining oldini olish uchun buzilishdan himoyalangan bo‘lishi kerak. Ushbu riskni kamaytirish uchun quyidagi himoya choralari qo‘llaniladi:

- elektr va aloqa kabellari (imkon qadar) yer ostida, kanalizatsiya va kollektorlarda, binolar ichida bo‘lishi kerak yoki ruxsatsiz jismoniy kirishdan himoyalangan bo‘lishi kerak;
- tarmoq simlarini ruxsatsiz ochilish va ma’lumotlarni to‘sib qo‘yish, shuningdek, shikastlanishdan himoya qilish uchun, jamoat joylaridan o‘tmaslik uchun yotqizilgan ekranlangan kabellar ishlatiladi. Jamoat joylarini aylanib o‘tib, kabel yotqizish uchun texnik imkoniyatlar bo‘lmagan taqdirda, bunday kabellar metalldan yasalgan qutilarga yotqizilishi kerak, ular ruxsatsiz ochish imkoniyatini istisno qiladi;
- ish stansiyalarini ulash uchun mo‘ljallangan foydalanilmagan tarmoq kabeli ulagichlari axborotni qayta ishlash qurilmalarini ruxsatsiz ulanish imkoniyatini istisno qilish uchun maxsus marka bilan muhrlangan bo‘lishi kerak.

13.2 Tarmoq simlari imkon qadar bir-biriga salbiy ta’sirlarining (magnit shovqin) oldini olish uchun iloji boricha elektr simlaridan alohida yotqizilishi kerak, shuningdek, ruxsatsiz ulanishlar yoki shikastlanishlardan himoyalangan bo‘lishi kerak masalan, kabel yo‘nalishi ommaviy joylarni chetlab o‘tkazilgan bo‘lishi kerak.

13.3 Universitetning telekommunikatsiya tarmoqlari orqali uzatishda axborotning konfidensialligini ta’minlash uchun quyidagi himoya choralari amalga oshiriladi:

- korporativ tarmoq orqali bog‘lashda muhofaza qilinadigan obyektlarda har 90 kunda shifrlash sertifikatlarini o‘zgartirgan holda himoyalangan VPN-kanallardan foydalanish;
- xodimlar va foydalanuvchilarning axborot tizimlariga ulanishini ta’minlash vaqtida VPN-kanallar, IPSec kabi xavfsizlik usullaridan hamda HTTPS, SSL/TLS,

SSH protokollaridan foydalangan holda xavfsiz ulanishlarni tashkil etish;

- Universitet, shuningdek, uchinchi tomon tashkilotlar o‘rtasida xabarlar (yozishmalar) almashish uchun Edo.ijro.uz – Ijro intizomi idoralararo hujjat aylanish tizimi tizimi va E-xat – Himoyalangan elektron pochta tizimi kabi himoyalangan axborot uzatish tizimlaridan foydalanish.

13.4 Universitet joylashgan binolarda ichki foydalanish uchun simsiz Wi-Fi tarmog‘ini tashkil qilishda quyidagi talablarga javob berish kerak:

- Wi-Fi signali tarqatiladigan hudud chegarasini aniqlash;
- qurilmalarni MAC manzili bo‘yicha Wi-Fi tarmog‘iga kirishda autentifikatsiya.
- Wi-Fi signali nazorat qilinadigan hududdan tashqariga chiqmasligi choralarini ko‘rish;
- Wi-Fi tarmog‘i Universitetning lokal tarmog‘iga ulanmagan holda, jismoniy jihatdan alohida tashkil etilishi kerak;
- Wi-Fi tarmog‘i uchun korporativ tarmoqning internetga ulanishidan farqli o‘laroq, internetga alohida ulanish tashkil qilinishi kerak;
- xodimlarning shaxsiy Wi-Fi qurilmalarini (ish stansiyalari, noutbuklar, planshetlar va uyali telefonlar) ichki tarmoq resurslariga, xususan lokal tarmoq, korporativ tarmoq va axborot tizimlariga ulashni taqiqlash;
- xavfsizlikni ta’minlash maqsadida lokal tarmoqqa oldin ulangan terminallarni (ish stansiyalari va noutbuklarni) ichki Wi-Fi tarmog‘iga ikkinchi kirish huquqi bilan ta’minlash taqiqlanadi (qat’iy belgilangan individual terminal qurilmalari Wi-Fi tarmoqlariga ulanishi kerak).

13.5 Foydalanish cheklangan axborotlarni hududdan tashqariga uzatish nazorat qilinadigan aloqa kanallari orqali, O‘zbekiston Respublikasida sertifikatlangan axborotni kriptografik himoya qilish vositalari bilan shifrlashni ta’minlash shart.

14. Javobgarlik taqsimoti

14.1 Axborot xavfsizligi rejimini yaratish va qo‘llab-quvvatlash uchun, alohida manbalarning axborot xavfsizligi uchun javobgarlikni aniq va hujjatlashtirilgan tarzda birlashtirish va axborotni muhofaza qilishning ba’zi jarayonlarini bajarish zarur.

14.2 Resurslarni taqsimlash va axborot xavfsizligini ta’minlash tartib-taomillarini amalga oshirish uchun javobgarlik Mas’ul rahbar zimmasiga yuklanadi.

14.3 Axborot xavfsizligini ta’minlashda Mas’ul rahbarning asosiy vazifalari:

- axborot xavfsizligi maqsadlarini aniqlash;
- Siyosatni shakllantirish, qayta ko‘rib chiqishni tashkillashtirish va tasdiqlash uchun Rektorga kiritish;
- Siyosatni amalga oshirish samaradorligini monitoring qilish;
- xavfsizlikni yaxshilash bo‘yicha tashabbuslarni doimiy, aniq va moddiy-ma’muriy qo‘llab-quvvatlash;
- zarur axborot xavfsizligi vositalarini ajratish bilan bog‘liq ishlarni tashkillashtirish;
- Universitetda axborot xavfsizligi uchun javobgarlarni ko‘rib chiqish va ularning vazifalarini belgilash, shuningdek, javobgarlarni belgilash uchun Rektorga takliflar kiritish;

- Axborot xavfsizligi administratorining axborot xavfsizligini ta’minlash bo‘yicha rejalari va dasturlarini tasdiqlash.

Universitetning AXBTni bevosita tashkil etish va nazoratni amalga oshirish Axborot xavfsizligi administratori zimmasiga, axborot tizimlarining xavfsizligini ta’minlash Raqamli ta’lim texnologiyalarini joriy etish va axborot xavfsizligini ta’minlash sektori zimmasiga yuklatilgan.

14.4 Lokal tarmoq administratori yo‘riqnomasi ushbu siyosatning 3-ilovasiga muvofiq, Axborot tizimi administratori yo‘riqnomasi 4-ilovaga muvofiq, Axborot va kiberxavfsizlikni ta’minlash bo‘yicha mas’ul xodimning yo‘riqnomasi ushbu Siyosatning 5-ilovada keltirilgan.

14.5 Universitet raqamli infratuzilmasini rivojlantirish, uning uzluksiz ishlashini nazorat qilish shu bilan birga, ushbu axborot va kiberxavfsizligini ta’minlash ushbu siyosatning 6-ilovasi “Axborot xavfsizligini ta’minlash sektori va Raqamli ta’lim texnologiyalari departamentining Universitet infratuzilmasida axborot va kiberxavfsizlikni ta’minlash sohasidagi vazifalarini amalga oshirish to‘g‘risidagi nizom”da belgilangan.

14.6 Ushbu Siyosat Universitetda axborot xavfsizligini ta’minlash uchun quyidagi javobgarlikni taqsimlaydi:

- Universitetda axborot xavfsizligini ta’minlash bo‘yicha barcha tadbirlar uchun Axborot xavfsizligi administratori, Departament boshlig‘i hamda xodimlari javobgardir;

- xodimga ishonib topshirilgan har qanday shakldagi ma’lumotni saqlash va uni himoya qilishning tegishli darajasini ta’minlash uchun ushbu xodim shaxsan javobgarlikni o‘z zimmasiga oladi;

- Universitet axborot tizimlari va resurslarida amalga oshirilgan harakatlar uchun Universitet xodimlari o‘zlariga yuklatilgan vazifalar doirasida javobgardirlar;

- xodimga xizmat vazifalarini bajarish uchun taqdim etilgan ish stansiyasining axborot xavfsizligi (shu jumladan jismoniy xavfsizligi) uchun xodimning shaxsan o‘zi javobgardir;

- Universitet joylashgan binolarga jismoniy joylashtirilgan lokal tarmoqning axborot xavfsizligi uchun Lokal tarmoq administratori javobgardir;

- soliq va bank muassasalari tomonidan taqdim etilgan ERIlardan foydalanish (qabul qilish, yangilash, xavfsiz saqlash, bekor qilish va boshqa harakatlar) Universitetda Buxgalteriya bosh buxgalteri javobgardir;

- Edo.ijro.uz va E-xat tizimlari uchun foydalaniladigan ERI kalitlaridan foydalanish (qabul qilish, yangilash, xavfsiz saqlash, bekor qilish va boshqa harakatlar) uchun Universitetda Rektor ijro apparati, Buxgalteriya bosh buxgalteri, Devonxona bosh mutaxassisi, Fakultet dekanlari, Kafedra mudirlari, shuningdek, barcha departament, markaz va bo‘limlar boshliqlari javobgardir;

- Universitetning Fuqaro va mehnat muhofazasi sektori xodimlari Universitetda yong‘in va texnik xavfsizlik, har bir xona ichidagi jihozlarning xavfsizligi uchun javobgardir.

14.7 Mas’ul rahbar va xodimlar uchun 14.5-bandda ko‘rsatilgan javobgarlik ushbu rahbar va xodimlarning lavozim yo‘riqnomalarida, shuningdek, Universitetning

tegishli boshqa ichki me’yoriy hujjatlarida belgilanadi.

14.8 Mas’ul rahbar yoki xodim ishda bo‘lmaganida (ta’til, kasallik, mehnat safari va boshqalar) uning vazifalarini belgilangan tartibda tayinlangan shaxs bajaradi. Ushbu shaxs tegishli huquqlarga ega bo‘ladi va o‘ziga yuklatilgan vazifalarning to‘g‘ri bajarilishi uchun javobgardir.

15. Siyosatni qayta ko‘rib chiqish va yangilash tartibi

15.1 Siyosatni qayta ko‘rib chiqish yilda bir marta yoki quyidagi holatlarda amalga oshiriladi:

- Siyosatni ayrim bandlari axborot xavfsizligiga tegishli yangi me’yoriy-huquqiy va me’yoriy texnik hujjatlarga zid bo‘lsa yoki amaldagi qonuniy hujjatlarga o‘zgartirish kiritilsa;
- Siyosat talablarini qayta ko‘rib chiqish zaruriyati paydo bo‘lsa;
- Universitet infratuzilmasiga dasturiy va texnik ta’minoti vositalarini yangi qo‘shilganda yoki o‘chirilganda, tizim konfiguratsiyasi o‘zgarganda, yangi himoya obyektlari qo‘shilganda;
- axborotni himoya qilish vositalari tarkibi o‘zgarganda;
- Universitet tarkibiy tuzilmasi o‘zgarganda (qayta tashkil etilganda).

15.2 Agar Siyosatning ayrim bandlari va boshqa me’yoriy hujjatlari O‘zbekiston Respublikasini axborot xavfsizligi sohasiga doir yangi qonuniy hujjatlariga zid bo‘lsa, bu holda Siyosatga o‘zgartirish kiritilguniga qadar ushbu bandlar o‘z yuridik kuchini yo‘qotadi.

15.3 Siyosatga o‘zgartirish va qo‘shimchalar, Mas’ul rahbar, Departament boshlig‘i va Axborot xavfsizligi administratori tashabbusi bilan kiritiladi va Rektor tomonidan tasdiqlanadi.

15.4 Siyosatni o‘zgartirish va qo‘shimchalar kiritish yoki dolzarbligi va samaradorligini baholash quyidagi hollarda amalga oshiriladi:

- tasdiqlangan Siyosat talablari va qoidalariga muvofiqligini baholash;
- Universitetning axborot tizimlari, infratuzilmasi axborot xavfsizligiga qo‘yilgan talablarga muvofiqligi;
- ko‘rilayotgan chora-tadbirlar, axborotni himoya qilish usullari va vositalarini samaradorligini baholash;
- Siyosatga o‘zgartirish, qo‘shimchalar kiritish yoki qayta ko‘rib chiqish zaruriyati tug‘ilganda.

15.5 Agar Universitetning axborot infratuzilmasi va shu bilan bog‘liq axborot texnologik jarayonlariga qo‘shimcha o‘zgartirishlar kiritilsa, uning AXBT tizimi o‘zgarsa, Siyosat to‘liq qayta ko‘rib chiqiladi.

15.6 Siyosatning yangi tahriri O‘zbekiston Respublikasi Oliy ta’lim, fan va innovatsiyalar vazirligining Raqamli ta’lim texnologiyalarini rivojlantirish markazi, O‘zbekiston Respublikasi Raqamli texnologiyalar vazirligi va O‘zbekiston Respublikasi Davlat xavfsizlik xizmati bilan qayta kelishilishi shart.

15.7 Universitet xodimlari Siyosat qayta ko‘rib chiqilgan va tasdiqlanganidan so‘ng Siyosat bilan imzo qo‘yish orqali tanishishlari lozim. Siyosat bilan tanishish jurnali shakli ushbu Siyosatning 21-ilovasida keltirilgan.

Universitet axborot xavfsizligi
siyosatga 1-ilova

Lokal tarmoq va himoyalangan tarmoq ulanishlarini tashkil etish to‘g‘risidagi NIZOM

1. Umumiy qoidalar

1.1 Ushbu Nizom Universitetda lokal tarmoq va xavfsiz tarmoq ulanishlarini tashkil etish qoidalari va tartibini belgilaydi.

1.2 Universitet doimiy ravishda o‘zining lokal tarmog‘i xavfsizligini to‘liq nazorat qiladi.

2. Lokal tarmoq maqsadi

2.1 Universitet lokal tarmog‘i quyidagilarni ta’minlaydi:
- xodimlar o‘rtasida axborot aylanishini ta’minlash;
- xodimlarining ish stansiyalarini tashqi internetga ulash;
- tashqi ma’lumotlarni uzatish kanallari ulanish.

3. Lokal tarmoq tarkibi

3.1 Universitet lokal tarmog‘i tarkibiga quyidagilar kiradi:
- Universitet lokal tarmog‘ini internet tarmog‘iga ulash kanallari;
- tarmoqni kommutatsiya qilish qurilmalari;
- tarmoqlararo ekran (FortiGate 100F) apparat vositasi, internet tarmog‘iga binolarning lokal tarmog‘iga ulanishining nuqtasida o‘rnatilgan Proksi-server;
- fayl server;
- axborot tizimlari va resurslari joylashgan server;
- kommutatsiya panellari va tarmoq kabellari.

4. Lokal tarmoqni tashkiliy boshqarish va rivojlantirish bo‘yicha ishlarni tashkil etish

4.1 Universitet lokal tarmog‘ini tashkiliy boshqarish, uning rivojlanish yo‘nalishlari va bosqichlarini belgilash, shuningdek, uni rivojlantirish bo‘yicha chora-tadbirlarni amalga oshirish Universitetda Raqamli ta’lim texnologiyalari departamenti Tarmoqlarni boshqarish va texnik qo‘llab-quvvatlash sektori bosh mutaxassisi (keyingi o‘rinlarda – Lokal tarmoq administratori) tomonidan amalga oshiriladi.

4.2 Lokal tarmoqlarni boshqarish Universitetda Lokal tarmoq administratori tomonidan amalga oshiriladi.

4.3 Lokal tarmoqlarni boshqarish quyidagilarni o‘z ichiga oladi:
- lokal tarmoqning axborot xavfsizligini ta’minlash;
- xavfsiz ulanishlarini tashkil qilish;

- tashqi telekommunikatsiya tarmoqlari bilan lokal tarmoqning ma’lumot almashinuvini boshqarish;

- lokal tarmoq ichidagi axborot oqimlarini boshqarish;

- foydalanuvchilarning lokal tarmoq orqali axborot tizimlari va resurslariga kirishini boshqarish, ularning vakolatlari va foydalanish huquqlarini aniqlash;

- foydalanuvchilarni, shuningdek, axborot tizimlari va resurslarini lokal tarmoqqa ulash va ajratish;

- lokal tarmoqni tashkil etadigan tarmoq qurilmalari, tarmoq manbalariga texnik xizmat ko‘rsatish;

- tarmoqda ishlatiladigan dasturiy va texnik vositalarni tanlash.

4.4 Lokal tarmoq administratori tarmoq qurilmalariga (kommutator va routerlar) texnik xizmat ko‘rsatilishini va ishlashini ta’minlaydi.

4.5 Universitetda Lokal tarmoq administratori axborot xavfsizligini ta’minlash masalalari bo‘yicha mas’ul xodim (keyingi o‘rinlarda – Axborot xavfsizligi administratori)ni va Departament boshlig‘ini ushbu Nizom qoidalari buzilishining barcha holatlari to‘g‘risida xabardor qilishi shart.

5. Lokal tarmoqni rivojlantirish

5.1 Lokal tarmoqni yanada rivojlantirishning asosiy yo‘nalishlari:

- markaziy kommutatorlarni – lokal tarmoq kommutator yadrosini modernizatsiya qilish;

- lokal tarmoq va internetning tashqi kanallariga ulanish uchun, ular o‘rtasida himoyalangan VPN-ulanishlarni tashkil etish funksiyasiga ega bo‘lgan apparat va dasturiy ta’minot sotib olish va ulardan foydalanish;

- tashqi tarmoqqa himoyalangan VPN-ulanishlarni, VPN-mijoz va proksi-server funksiyalari mavjud bo‘lgan tarmoqlararo ekran va DLP vositalarini sotib olish va foydalanish;

- zaxira nusxasini ta’minlash uchun ma’lumotlarni saqlash tizimlarini, shuningdek, lokal tarmoqni tashkil etuvchi muhim tugunlarning ishlashini nazorat qilish va zaxiralashni ta’minlash uchun yordamchi server tizimlarini olish va joylashtirish.

6. Lokal tarmoqda xavfsiz bog‘lanishlar sinflanishi

6.1 Universitetdagi lokal tarmoqlarda himoyalangan ulanishlar, uzatilayotgan ma’lumotlarning konfidensialligi va yaxlitligini ta’minlash uchun ishlatiladi.

6.2 Lokal tarmoqdagi xavfsiz ulanishlar ikkita mezon bo‘yicha tasniflanadi:

- ularni tashkil etish darajasi;

- himoya qilishning amaliy texnologiyalari.

6.3 Tashkilot darajasida Universitet lokal tarmoqlaridagi xavfsiz ulanishlar quyidagicha tasniflanadi:

- aloqa va axborot almashinuvini tashkil qilish uchun himoyalangan aloqalar;

- tashqi foydalanuvchilar va boshqa tashkilotlarning foydalanuvchilarini tashqi

tarmoq orqali axborot tizimlari va resurslariga (fuqarolarning murojaatlari, talabalar turar joylari uchun ariza berish kabi vazifalarni bajarishga mo‘ljallangan axborot tizimlari) ulashda himoyalangan ulanish.

7. Lokal tarmoqda himoyalangan ulanishlardan foydalanish tamoyillari

7.1 Universitet lokal tarmoqlarida quyidagi himoyalangan ulanishlar tashkil etiladi:

- internet orqali Universitet (https://buxdu.uz/) rasmiy veb-saytiga, shuningdek, Universitetning boshqa ochiq axborot resurslariga kirish huquqini taqdim etishda HTTPS va SSL/TLS protokollaridan foydalangan holda himoyalangan ulanishlardan foydalanish. (Tashqi foydalanuvchilar hamda internet foydalanuvchilari tomonidan foydalaniladi);
- fuqarolarning murojaatlari, talabalar turar joylari uchun ariza berishi kabi vazifalarni bajarishga mo‘ljallangan axborot tizimlariga ulanganda VPN-kanallar, IPSec kabi xavfsizlik usullaridan hamda HTTPS, SSL/TLS protokollaridan foydalangan holda xavfsiz ulanishlarni tashkil etish.

7.2 Universitet lokal tarmog‘ida 7.1-bandda ko‘rsatilgan himoyalangan ulanishlarni tashkil etish va buning ustidan nazorat Axborot xavfsizligi administratori hamda Departament boshlig‘iga yuklatilgan.

8. Javobgarlik

8.1 Lokal tarmoq foydalanuvchilari, Lokal tarmoq administratori hamda departament xodimlari quyidagilarga javobgardir:

- ushbu yo‘riqnomada nazarda tutilgan talablarni bajarishga;
- o‘ziga biriktirilgan ish stansiya va lokal tarmoqdagi ma’lumotlar xavfsizligini ta’minlashga;
- faqat avtorizatsiyaga ega bo‘lgan lokal tarmoqdagi resurslar va ma’lumotlarga kirishlari hamda kirishlarni boshqarish maqsadida joriy etilgan siyosatlarni yoki ruxsatlarni tushunishga va ularga qat’iy rioya qilishga;
- lokal tarmoq qurilmalaridagi o‘z faoliyatiga tegishli muhim ma’lumotlarning muntazam zaxira nusxasini yaratish va saqlab borishga;
- lokal tarmoqqa ulangan boshqa xodimlarga o‘zaro hurmat bilan munosabatda bo‘lishga.

8.2 Ushbu Nizomda belgilangan talablarning buzilishi Universitetning ichki mehnat qoidalari va O‘zbekiston Respublikasining mehnat qonunchiligiga muvofiq intizomiy javobgarlikka tortilishga olib keladi.

Universitet axborot xavfsizligi
siyosatga 2-ilova

Tarmoq infratuzilmasi va tarmoqlararo ekran darajasida axborot xavfsizligini ta’minlash to‘g‘risida NIZOM

1. Umumiy qoidalar

1.1 Ushbu Nizom tarmoqlararo ekrandan foydalangan holda Universitetda joylashgan axborot tizimlari va resurslarga kirishni boshqarish orqali axborot xavfsizligini ta’minlash mexanizmi va qoidalarini tartibga solish maqsadida ishlab chiqilgan.

1.2 Nizom Universitetning lokal tarmoqlarini, axborot tizimlari va resurslarini tarmoq darajasida ruxsatsiz kirishdan himoya qilishni tashkil etishning asosiy tamoyillarini belgilaydi.

2. Atamalar va ta’riflar

2.1 Ushbu Nizomda O‘zDSt 2927:2015 “Axborot texnologiyalari. Axborot xavfsizligi. Atamalar va ta’riflar” va O‘zDSt 1047:2018 “Axborot texnologiyasi. Atamalar va ta’riflar” davlat standartlaridagi atamalar va ularning ta’riflari qo‘llaniladi:

2.1.1 **tarmoq infratuzilmasi** – aloqa tarmoqlari, shuningdek, ish stansiyalari va serverlar o‘rtasida mantiqiy aloqani ta’minlovchi kommutatsion qurilmalarni o‘z ichiga olgan;

2.1.2 **OSI modeli** – 7 darajadan iborat ochiq axborot tizimlarining tarmoqlararo ta’sirining bazaviy etalon modeli, ularning uchtasi tarmoq infratuzilmasiga tegishli;

2.1.3 **OSI modelining fizik (birinchi) darajasi** – ma’lumotlarni uzatish vositasi, signallar va ikkilik ma’lumotlar bilan ishlash;

2.1.4 **OSI modelining kanal (ikkinchi) darajasi** – kommutatsiya darajasida fizik manzilga murojaat qilish;

2.1.5 **OSI modelining tarmoq (uchinchi) darajasi** – marshrutni va mantiqiy adresni IP protokoli darajasida aniqlash;

2.1.6 **tarmoqlararo ekran** – tizimga kiradigan va/yoki tizimdan chiqadigan ma’lumot ustidan nazoratni amalga oshiradigan tarmoq (bitta komponentli) yoki funksional-taqsimlangan dasturiy ta’minot (apparat-dasturiy ta’minot) vositasi (kompleks);

2.1.7 **tashqi tarmoq** – Universitet tomonidan boshqarilmaydigan tarmoqlar, shu jumladan internet va boshqalar;

2.1.8 **hujumlarni aniqlash va bartaraf etish tizimi (Intrusion Detection & Prevention System IDPS)** – bu kirishni yoki xavfsizlik buzilishlarini aniqlaydigan va avtomatik ravishda ulardan himoya qiladigan dasturiy yoki apparat asosidagi tarmoq va kompyuter xavfsizligi vositasi.

3. Umumiy talablar va tarmoq infratuzilmasi darajasidagi talablar

3.1 Tarmoq infratuzilmasini muhofaza qilish OSI modelining har bir sathini-jismoniy, kanal, tarmoq, transport va boshqalarni himoya qilishga asoslangan.

3.2 Jismoniy himoya qilish ma’lumotlarni uzatishda foydalaniladigan oddiy juftlik va optik kabellarining xavfsizligini ta’minlashdan iborat.

3.3 Kanal sathidagi himoya tegishli axborot xavfsizligi funksiyalariga ega kommutatorlarga asoslangan holda qurilgan.

Universitetda joylashgan tarmoq kommutatorlari va marshrutizatorlari hamda tarmoqlararo ekran (Kerio Control 9.3.5 build 4367 yoki FortiGate 100F) orqali:

- DHCP snooping – bu DHCP hujumlaridan himoya qilish uchun mo‘ljallangan almashtirish funksiyasi.
- IP Source Guard – IP-spoofingga qarshi kurashish uchun mo‘ljallangan, IP-paketdagi yuboruvchining IP-manzilini tekshiradi.
- IP Source Guard (Dynamic IP Lockdown) – bu DHCP snooping majburiy jadvali va statik o‘yinlar asosida trafikni filtrlash orqali bog‘lanish qatlami interfeyslarida IP-trafikni cheklaydigan o‘chirish funksiyasi. Funksiya IP-firibgarlikka qarshi kurashish uchun ishlatiladi.

3.4 Tarmoq darajasida himoya qilish obyekt va subyekt o‘rtasidagi aloqani o‘rnatishni ta’minlaydigan ekranli modullardan foydalangan holda quriladi, so‘ngra voqealarni kuzatib borish va yozib olish vaqtida qoidalar asosida ma’lumotni yuboradi yoki bloklaydi.

Lokal tarmoq, uning segmentlari va manbalariga kirishni boshqarish tarmoqlararo ekran orqali ta’minlanadi.

3.5 OSIning ikki va undan yuqori sathlarini tarmoq hujumlardan himoya qilish, hujumlarni aniqlash va oldini olish vositalari (IDPS) yordamida ta’minlanishi lozim.

3.6 IDPS vositasi tekshirish usuli va xatti-harakatlarni tahlil qilish usuli yordamida tarmoq hujumlari va hujumlarini aniqlashi va ularning harakatlarini oldini olish ta’minlanadi.

3.7 IDPS vositalaridan foydalanganda ularda ishlatiladigan hujum usulini tekshirish va ma’lumotlar bazalarining davriy yangilanishi ta’minlanishi kerak.

3.8 IDPS vositasidan lokal tarmoqqa internet tarmog‘idan ulanishda tarmoq hujumlariga qarshi himoya qilish uchun qo‘llanilishi lozim.

3.9 Proksi-serverlar yoki ilovalarni boshqarish funksiyalariga ega tarmoqlararo ekran transport va amaliy qatlam protokollari orqali trafik uzatilishini boshqarish uchun ishlatiladi.

3.10 Proksi-serverlar yoki tarmoqlararo ekran internetga lokal tarmoq ulanishining chegarasida o‘rnatiladi. Proksi-server yoki tarmoqlararo ekran sozlamalarida va axborot resurslari uchun zarur bo‘lgan trafik tarmoq protokollari orqali ta’minlanadi.

4. Tarmoqlararo ekran

4.1 Tarmoqlararo ekran ma’lumotlarini (paketlarni va ulanishlarni) OSIning turli

darajalarida (tarmoq sathidan dasturiy darajasiga qadar) belgilangan tarmoq xavfsizligi qoidalariga muvofiq filtrlashi kerak, shuningdek, himoyalangan tarmoq tuzilishi to‘g‘risidagi ma’lumotlarni tashqi foydalanuvchilardan yashirishi kerak.

4.2 Tarmoqlararo ekran lokal tarmoqning internetga ulanish nuqtasiga o‘rnatiladi.

4.3 Ushbu Nizomning 4.2-bandda ko‘rsatilgan tarmoqlararo ekran O‘z DSt 2815:2014 “Axborot texnologiyalari. Tarmoqlararo ekranlar. Ma’lumotlarga ruxsatsiz kirishdan himoya qilish darajasi bo‘yicha tasniflash” davlat standartiga muvofiq kamida 3-xavfsizlik sinfidan iborat bo‘lishi kerak.

4.4 Tarmoqlararo ekranni sozlashda quyidagi talablar bajarilishi shart:

- internet tarmog‘idan lokal tarmoqqa to‘g‘idan-to‘g‘i kirishlarni cheklash (blokirovka qilish);
- xodimlar uchun internet tarmog‘idan (masofadan) lokal tarmoqqa ruxsat etilmagan hamda himoyalanmagan ulanishlarni cheklash (blokirovka qilish);
- faqat xodimlarning ish stansiyalarini internetga ulanishini ta’minlash, shuningdek, kirishlarni boshqarish;
- ushbu talablarni bajarish uchun filtrlash qoidalariga muvofiq turli protokol, IP-manzillar, URL-manzillar orqali so‘rovlarni va trafikni filtrlash;
- tarmoq manzili translyatsiyasini (NAT) ta’minlash;
- ilovalarni nazorat qilish.

5. Tarmoqlararo ekranni o‘rnatish va ishlatish tartibi

5.1 Joriy etiladigan tarmoqlararo ekran quyidagi talablarni bajarishi shart:

- himoyalangan tarmoq yoki uning segmenti xavfsizligini va tashqi ulanishlar va aloqa seanslari ustidan to‘liq nazoratni ta’minlash;
- Siyosatni to‘liq va sodda amalga oshirish uchun kuchli va moslashuvchan boshqaruv vositalariga ega bo‘lishi;
- tarmoq tarkibi o‘zgarganda tizimni oddiy qayta konfiguratsiyalash;
- tarmoq foydalanuvchilari uchun uzluksiz ishlashiga va ularning huquqiy harakatlariga to‘sqinlik qilmaslik;
- tarmoqqa bo‘lgan so‘rovlar soni oshgan, tig‘iz vaqtda barcha kiruvchi va chiquvchi trafiklarni qayta ishlash uchun samarali va o‘z vaqtida ishlashi;
- har qanday ruxsatsiz ta’sirlardan o‘zini himoya qilish xususiyatlariga ega bo‘lishi.

5.2 Tarmoqlararo ekranni joriy etishdan oldin ushbu Nizomning 6-bo‘limiga muvofiq sinovlardan o‘tkazilishi kerak.

5.3 Tarmoqlararo ekranni ishlatish (texnik xizmat ko‘rsatish, sozlamalarini o‘zgartirish) Universitetda Tarmoqlarni boshqarish va texnik qo‘llab-quvvatlash sektori bosh mutaxassisi (keyingi o‘rinlarda – Lokal tarmoq administratori) va Departament xodimlari tomonidan amalga oshiriladi.

5.4 Tarmoqlararo ekranni ishlatishdan oldin ushbu Nizomning 4-bo‘limi va Siyosat talablariga muvofiq sozlanadi.

5.5 Tarmoqlararo ekranni ishlatishda quyidagilar ta’minlanishi kerak:

- tarmoqlararo ekran ishini muntazam ravishda monitoring qilish va diagnostika qilish, shuningdek, tarmoqlararo ekran tomonidan nazorat funksiyalarining bajarilishini nazorat qilish;

- ushbu Nizomning 7-bo‘limida ko‘rsatilgan holatlarda tarmoqlararo ekranning sozlamalarini o‘zgartirish;

- tarmoqlararo ekran sozlamalari va konfiguratsiyasini belgilangan filtrlash talablariga asosan ishlashini har kuni tekshirish;

- tarmoqlararo ekranning so‘nggi sozlamalarini saqlash;

- tarmoqlararo ekran ishlamay qolganda yoki boshqasiga almashtirilganda uning so‘nggi barcha sozlamalari va konfiguratsiyasini tiklash orqali sozlash.

5.6 Uzatiladigan trafik hajmi ko‘payganda yoki tarmoqlararo ekran nazoratini oshirish va boshqa maqsadlarda tarmoqlararo ekranning ish tartibiga o‘zgartirishlar kiritilishi mumkin.

5.7 Tarmoqlararo ekran ishlashiga o‘zgartirishlar kiritish ushbu Nizomning 5.3-bandida keltirilgan mas’ul xodimlar tomonidan amalga oshiriladi, shuningdek, zarurat tug‘ilganda tegishli xavfsizlik talablariga rioya qilgan holda uchinchi tomon tashkilotlari jalb qilinadi.

5.8 Tarmoqlararo ekranlarga xizmat ko‘rsatuvchi mas’ul xodimlar har kuni xavfsizlik jurnallarini va tarmoqlararo ekran hodisalarini kuzatib borishlari kerak.

5.9 Agar tashqi hujumlar aniqlansa, Universitetning axborot xavfsizligini ta’minlash masalalari bo‘yicha mas’ul xodimi (keyingi o‘rinlarda – Axborot xavfsizligi administratori) hamda Departament boshlig‘ini xabardor qilishlari shart.

6. Tarmoqlararo ekranni sinovdan o‘tkazish tartibi

6.1 Tarmoqlararo ekranni sinovdan o‘tkazishning maqsadi ushbu dasturiy-apparat vositaning (paket filtrlari, proksi-serverlari, dastur shlyuzlari) tartibga soluvchi me’yoriy hujjatlar talablarga muvofiqligini tasdiqlash, shuningdek, filtrlashning talab qilingan qoidalarini bajarilishini tekshirish hisoblanadi.

6.2 Tarmoqlararo ekranni sinovdan o‘tkazish uchun boshqaruv xavfsizligi stendi yaratilib, u Axborot xavfsizligi administratori va Departament boshlig‘iga mustaqil ravishda paket yaratishga (ulanishni o‘rnatishga) va tarmoqlararo ekran sozlamalarining sinov natijalariga (tarmoqlararo ekrani orqali paket o‘tganligi yoki ulanish o‘rnatilganligi) tahlil qilishga imkoniyatini beradi.

Eng oddiy sinov bu paket (ulanish) generatori va trafikni tekshirgichlarni o‘z ichiga oladi. Ulanish o‘rnatilishini tekshirish uchun paket generatori ulanishni o‘rnatishi kerak va trafik tekshirgichi har qanday o‘zboshimchalik bilan belgilangan port yoki dasturga xizmat ko‘rsatadigan universal server bo‘lishi kerak.

6.3 Sinov jarayonida Axborot xavfsizligi administratori va Departament boshlig‘i paketni uzatish yoki tarmoqlararo ekranni “turli tomonlarida” ulanishni o‘rnatish natijalarini yaratishi va tahlil qilishi kerak (ya’ni paket generatori va trafik analizatori turli yo‘nalishlarda joylashgan bo‘lishi kerak).

6.4 Tarmoqlararo ekran orqali o‘tkazilgan sinov trafiklari natijalarini tahlil qilish va ularning aniq talabga javob beradigan deb hisoblangan natijalar bilan taqqoslash

asosida tarmoqlararo ekran sinovdan o‘tgan xavfsizlik mexanizmining to‘g‘ri bajarilishi to‘g‘risida xulosa chiqariladi.

6.5 Tarmoqlararo ekran sinovi barcha monitoring funksiyalari va filtrlash qoidalari tasdiqlanmaguncha amalga oshiriladi. Tarmoqlararo ekran sinov muddati kamida bir oy bo‘lishi kerak.

6.6 Tarmoqlararo ekranlar barcha sinov operatsiyasidan muvaffaqiyatli o‘tgan taqdirda Mas’ul rahbarga xabar beriladi.

7. Tarmoqlararo ekran konfiguratsiyasiga o‘zgartirishlar kiritish tartibi

7.1 Tarmoqlararo ekran konfiguratsiyasiga quyidagi hollarda o‘zgartirishlar kiritiladi:

- Siyosat talablari o‘zgarishi munosabati bilan yoki Universitet rahbariyatining topshirig‘iga binoan, shuningdek, alohida ulanishlar va kirishlarga cheklovlarni o‘rnatish zaruriyati bilan filtrlash qoidalarini o‘zgartirish;
- lokal tarmoq konfiguratsiyasini o‘zgartirish, yangi dasturlar, qurilmalar yoki foydalanuvchilarni qo‘shish;
- muvaffaqiyatsizliklar yoki hujumchilarning aniqlanishi va h.k.;
- qo‘shimcha yoki yangi axborot xizmatlarining joriy etilishi.

7.2 Mas’ul xodimlar tarmoqlararo ekranning konfiguratsiyasida har bir o‘zgarish haqida Universitetda Axborot xavfsizligi administratoriga va Departament boshlig‘iga xabar berishlari shart.

7.3 Tarmoqlararo ekran sozlamalari va konfiguratsiyasiga kiritilgan o‘zgartirishlar Lokal tarmoq administratori hamda departament xodimlari tomonidan ushbu Nizomga ilova qilingan shaklda jurnallarda qayd etilishi kerak.

7.4 Axborot xavfsizligi administratori tarmoqlararo ekran konfiguratsiyasiga kiritilgan o‘zgartirishlarni har chorakda kamida bir marta qayd etish jurnallari orqali tekshirishi kerak.

8. Javobgarlik

8.1 Axborot xavfsizligi administratori va Departament boshlig‘i Lokal tarmoq administratori hamda Departament xodimlarining ushbu Nizomda belgilangan talablarga rioya qilishlari uchun javobgardir.

8.2 Ushbu Nizomda belgilangan talablarning buzilishi Universitetning ichki mehnat qoidalari va O‘zbekiston Respublikasining mehnat qonunchiligiga muvofiq intizomiy javobgarlikka tortilishga olib keladi.

Tarmoq infratuzilmasi va tarmoqlararo ekran darajasida axborot xavfsizligini ta’minlash to‘g‘risidagi Nizomga ilova

Tarmoqlararo ekran sozlamalariga kiritilgan o‘zgartirishlarni qayd qilish JURNALI

T/r	Sana va vaqt	Kiritilgan o‘zgartirish	O‘zgartirish kiritish sababi
1.			
2.			
3.			
4.			
5.			

Universitet axborot xavfsizligi
siyosatiga 3-ilova

Lokal tarmoq administratorining YO‘RIQNOMASI

1. Umumiy qoidalar

1.1 Ushbu yo‘riqnoma Universitet lokal tarmog‘ini boshqarish tartibi va qoidalarini, lokal tarmoq administratori vazifalarini, lokal tarmoqning uzluksiz ishlashini ta’minlash va uning axborot xavfsizligini tegishli darajada saqlash vazifalarini belgilash maqsadida ishlab chiqilgan.

1.2 Universitetda lokal tarmoqni boshqarish uchun javobgarlik Lokal tarmoq administratoriga, u ma’lum sabab bilan ish joyida bo‘lmaganligi vaqtida Departament boshlig‘i qarori bilan Departamentning boshqa xodimi zimmasiga yuklanadi.

1.3 Lokal tarmoq administratori lavozimiga tayinlanadigan nomzodlar Departament boshlig‘i tomonidan ushbu Departament xodimlari orasidan tanlanadi va Universitet rahbariyati buyrug‘i bilan tayinlanadi.

1.4 Lokal tarmoq administratorining huquq va majburiyatlari ushbu yo‘riqnoma bilan belgilangan va uning lavozim yo‘riqnomasiga qo‘shimcha tarzda keltirilgan.

Betobligi tufayli yoki mehnat ta’tili paytida lokal tarmoq administratorining ishda bo‘lmagan vaqt, ushbu yo‘riqnomada ko‘rsatilgan lokal tarmoq administratorining huquqlari va majburiyatlari Departamentning boshqa xodimi zimmasiga yuklatiladi.

1.5 Lokal tarmoq administratori AKT sohasida kamida 3 yil ish tajribasiga ega bo‘lishi kerak.

1.6 Lokal tarmoq administratorining o‘z majburiyatlarini bajarishi bilan bog‘liq talablari Universitetning lokal tarmog‘idan foydalanuvchi barcha xodimlar uchun majburiydir.

1.7 Lokal tarmoq administratori quyidagilarga asoslangan holda ish yuritadi:

- Universitet axborot xavfsizligi siyosati;
- Universitet rektorining buyruqlari va farmoyishlari;
- qonun hujjatlari, ichki mehnat qoidalari;
- lokal tarmoqni boshqarish va axborot xavfsizligini ta’minlash usullari va qo‘llanmalari, ilmiy va uslubiy materiallar;
- ushbu yo‘riqnomaga asosan.

2. Lokal tarmoq administratorining vazifalari

2.1 Lokal tarmoq administratori hamda Departament xodimlari quyidagilarni bilishi kerak:

- lokal tarmoqda axborot texnologiyalaridan mukammal va samarali foydalanish;
- lokal tarmoqning tarmoq qurilmalaridan foydalanish qo‘llanmalarini;
- lokal tarmoq infratuzilmasini loyihalash va sozlash, jumladan kalitlar, marshrutizatorlar, kirish nuqtalari va kabellar;
- lokal tarmoq foydalanuvchilari hisoblarini yaratish, o‘zgartirish va o‘chirish,

shuningdek, kirish, ruxsatlar va xavfsizlik sozlamalarini boshqarish;

- xavfsizlik devorlari, hujumlarni aniqlash tizimlari va antivirus yechimlari kabi xavfsizlik choralarini qo‘llash va saqlash;
- himoyalangan VPN-ulanishlarni tashkil etish tartibi va usullarini amaliyotda qo‘llash;
- lokal tarmoq xavfsizligini kuzatish va xavfsizlik hodisalariga javob berish;
- lokal tarmoq ish faoliyatini baholash uchun monitoring qilish vositalaridan foydalanish;
- lokal tarmoq apparat va dasturiy ta’minotining so‘nggi yangilanishlar bilan yangilanib turishini ta’minlash;
- ma’lumotlarning zaxira nusxasini yaratish va ularni tiklash rejalarini ishlab chiqish va saqlash;
- xodimlarga texnik yordam ko‘rsatish, ularga tarmoq bilan bog‘liq muammolarni bartaraf etishda tezkor yordam berish;
- lokal tarmoq konfiguratsiyasi, siyosati va protseduralarining batafsil yozuvlarini saqlash;
- LDAP yoki Active Directory kabi foydalanuvchi autentifikatsiya mexanizmlarini joriy qilish;
- ruxsatsiz kirishni cheklash uchun kirishni boshqarish siyosatlarini qo‘llash;
- lokal tarmoq muammolari, ulanish muammolari va uzilishlarni tekshirish, ularni tezkorlikda hal qilish;
- lokal tarmoqni kengaytirish, takomillashtirish bo‘yicha rejalarni ishlab chiqish va takliflar tayyorlash;
- dasturiy ta’minotlarni yangilash, qurilmalarni tozalash va zaxira nusxalarini yaratish kabi ishlarni muntazam rejalashtirish va tartibli bajarish;
- lokal tarmoq faoliyatini yaxshilash uchun mavjud konfiguratsiyasilar hamda sozlamalarni optimallashtirish;
- xodimlarning uchun lokal tarmoqdan to‘g‘ri va maqsadli foydalanish, shuningdek, lokal tarmoqda xavfsizlik talablariga rioya qilish bo‘yicha xabardorligini oshirish;
- lokal tarmoqning axborot xavfsizligini ta’minlashga qo‘yiladigan talablarni bajarish;
- mehnatni muhofaza qilish qoidalari, normalari, xavfsizlik choralari va yong‘indan himoya qilish talablarini bajarish.

2.2 Lokal tarmoq administratori hamda Departament xodimlari quyidagilarga majbur:

- lokal tarmoq tarkibiga kiruvchi texnik, dasturiy ta’minot, tarmoq resurslarining ishlashini nazorat qilish;
- lokal tarmoq tarkibiga kiruvchi texnik, dasturiy ta’minot, tarmoq resurslarining ishlashini (o‘rnatish, sozlash, boshqarish va texnik xizmat ko‘rsatish) nazorat qilish;
- lokal tarmoqni profilaktika qilish bo‘yicha rejalar va jadvallarni ishlab chiqish va amalga oshirish;
- himoyalangan VPN-ulanishlarini tashkil etish va ishlashini ta’minlash;

- lokal tarmoqni profilaktika qilish boʻyicha rejalar va jadvallarni ishlab chiqish va amalga oshirish;

- kabellar infratuzilmasini qoʻllab-quvvatlash boʻyicha ishlarni tashkil etish va amalga oshirish, shu jumladan, tarmoq obyektlari va axborotni qayta ishlash vositalarini lokal tarmoqqa ulash, kabel tizimidagi nosozliklarni aniqlash va tuzatish;

- lokal tarmoq ishidagi turli xil ogʻishlarni oʻz vaqtida bartaraf etish boʻyicha ishlarni aniqlash va amalga oshirish;

- lokal tarmoqdagi axborot xavfsizligini buzish bilan bogʻliq voqealarga tezkor va samarali javob berish;

- tegishli vakolatlar va tarmoq axborot tizimlari va resurslariga kirish huquqlarini berish bilan xodimlarning ish stansiyalarini lokal tarmoqqa ulash;

- axborotlashtirish obyektlarini lokal tarmoqqa ulash boʻyicha talablarga rioya qilish;

- lokal tarmoq faoliyati jurnallarining ma’lumotlarini tahlil qilish;

- himoya talablarining mumkin boʻlgan buzilishlarini aniqlash uchun lokal tarmoq faoliyati jurnallaridan ma’lumotlarni tahlil qilish;

- lokal tarmoq qurilmalarining jismoniy xavfsizligini nazorat qilish;

- ruxsatsiz shaxslarning lokal tarmoqqa ulanishiga va ishlashiga yoʻl qoʻymaslik;

- vaqti-vaqti bilan bir oyda kamida bir marta lokal tarmoqning tarmoq qurilmalarini ularning ishlashining toʻgʻriligini sinovdan oʻtkazgan holda nazorat tekshiruvlarini oʻtkazish. Ushbu tekshiruvlar va sinovlar har yili ishlab chiqiladigan texnik xizmat koʻrsatish jadvaliga muvofiq amalga oshiriladi;

- tarmoq qurilmalari dasturiy ta’minotining xavfsizligini, himoyasini va oʻz vaqtida yangilanishini ta’minlash;

- lokal tarmoq infratuzilmasini rivojlantirish va uning xavfsizlik darajasini oshirish boʻyicha takliflar tayyorlash va taqdim etish;

- lokal tarmoq qurilmalarining yakuniy sozlamalarini, shuningdek, tarmoq qurilmalarini (domen serveri va fayl serveri) zaxira nusxalarini muntazam ravishda zaxiralashni amalga oshirish;

- har oyda tegishliligi boʻyicha Axborot xavfsizligi administratori hamda Departament boshligʻiga lokal tarmoqning ishlashi va axborot xavfsizligi holati toʻgʻrisida axborot berish, shuningdek, favqulodda vaziyatlar va xodimlar tomonidan axborotni muhofaza qilish boʻyicha belgilangan talablarning buzilishi toʻgʻrisida darhol xabar berish;

- xodimlar tomonidan Siyosat talablarining lokal tarmoqdan foydalanishda belgilangan tartib doirasida nazoratni ta’minlash.

2.3 Lokal tarmoqni boshqarishga mas’ul boʻlgan hamda Universitetda mehnat faoliyatini olib borayotgan boshqa xodimlarga quyidagilar taqiqlanadi:

- oʻz ish stansiyalarini nazoratsiz, shu jumladan ish holatida qoldirish;

- foydalanuvchilarning qayd yozuvi ma’lumotlarini foydalanuvchidan boshqa har qanday kishiga yetkazish;

- lokal tarmoq resurslariga ruxsatsiz kirish, shu jumladan tegishli ruxsatlarsiz tizimlar yoki ma’lumotlarga kirishga urinish;

- tarmoqlararo ekran yoki tahdidlarni aniqlash tizimlari kabi xavfsizlik choralarini chetlab o‘tish, ularni qasddan o‘chirishga yoki urinish;

- lokal tarmoqda zararli dasturlar, viruslar yoki zararli dasturlarni tarqatish, shuningdek, bila turib qasddan joriy etish;

- mualliflik huquqi bilan himoyalangan materiallarni ruxsatsiz almashish kabi noqonuniy fayl almashish bilan shug‘ullanish;

- lokal tarmoq konfiguratsiyasiga ruxsatsiz o‘zgartirishlar kiritish yoki ruxsatsiz o‘zgartirishga urinish;

- lokal tarmoq orqali ish faoliyati bilan bog‘liq bo‘lmagan kontentga kirish, ularni yuklab olish yoki almashish;

- boshqa xodimlarni aldash yoki ruxsatsiz kirishga erishish uchun fishing yoki ijtimoiy muhandislik hujumlarini amalga oshirishga urinish;

- lokal tarmoq xavfsizligini buzish, uning ish faoliyatini to‘xtatish va boshqa maqsadlarda sodir etiladigan DoS, DDoS hujumlarida ishtirok etish yoki ularga yordam berish;

- lokal tarmoq yaxlitligini saqlash uchun lokal tarmoqqa shaxsiy yoki ruxsatsiz qurilmalarni ulash yoki foydalanish.

3. Lokal tarmoq administratorining huquqlari

3.1 Universitetda lokal tarmog‘ini boshqarish huquqi Lokal tarmoq administratori hamda Departament xodimlariga beriladi.

3.2 Lokal tarmoq administratori hamda Departament xodimlari quyidagi huquqlarga ega:

- lokal tarmoqning himoyalangan resurslariga ruxsatsiz kirishni amalga oshirgan yoki boshqa axborot xavfsizligi talablarini buzgan xodimlarni lokal tarmoqdan uzish;

- lokal tarmoq faoliyatiga oid har qanday tekshirishda qatnashish;

- lokal tarmoqqa nostandart dasturiy ta’minot va qurilmalarni o‘rnatishni taqiqlash;

- lokal tarmoqning rivojlanishi ta’minlaydigan qarorlari loyihalari bilan tanishish;

- lokal tarmoq ishini takomillashtirish va axborot xavfsizligini ta’minlash bo‘yicha takliflarni Axborot xavfsizligi administratori va Departament boshlig‘iga taqdim etish;

- rahbariyat bilan o‘rnatilgan tartibda lokal tarmoqdan foydalanish qoidalarini belgilash va ularga o‘zgartirishlar kiritish;

- tegishliligi bo‘yicha Universitet hisobidan muntazam ravishda o‘z malakasini oshirish.

4. Lokal tarmoq administratorining javobgarligi

4.1 Lokal tarmoq administratori quyidagilarga javobgardir:

- ushbu yo‘riqnomada nazarda tutilgan o‘z vazifalarini bajarmaganligi yoki lozim darajada bajarmaganligi;

- lokal tarmoqdan foydalanishda foydalanuvchilarning xatti-harakatlarini nazorat

qilish bo‘yicha u tomonidan olib borilayotgan ishlarning sifatsizligi;

- texnika xavfsizligi qoidalarini buzilishiga javobgardir.

Universitet axborot xavfsizligi
siyosatiga 4-ilova

Axborot tizimi administratori
YO‘RIQNOMASI

1. Umumiy qoidalar

1.1 Ushbu Yo‘riqnoma Universitetning axborot resurslarini boshqarish tartibi va qoidalarini, operatsion va to‘plangan ma’lumotlarning to‘liq hajmini dolzarb ish tartibida saqlab turish, shuningdek uning axborot xavfsizligini tegishli darajada saqlash va ruxsatsiz kirishdan himoya qilish bo‘yicha tizim administratorining vazifalarini belgilash maqsadida ishlab chiqilgan.

1.2 Tizim administratori lavozimiga tayinlanadigan nomzodlar Departament boshlig‘i tomonidan ushbu Departament xodimlari orasidan tanlanadi va Universitet rahbariyatining tegishli buyrug‘i bilan tayinlanadi.

1.3 Tizim administratorining huquqlari va majburiyatlari ushbu Yo‘riqnoma bilan belgilangan va uning lavozim yo‘riqnomasiga qo‘shimcha tarzda keltirilgan.

Tizim administratorining ma’lum sabab bilan ish joyida bo‘lmaganligi vaqtida Tizim administratorining ushbu Yo‘riqnomada belgilangan huquqlari, vazifalari va majburiyatlari Departament boshlig‘i qarori bilan Departamentning boshqa bir xodimi zimmasiga yuklanadi.

1.4 Tizim administratori AKT sohasida oliy ma’lumotga hamda kamida 3 yillik tajribaga ega bo‘lishi kerak.

1.5 Tizim administratorining talablari o‘z majburiyatlarini bajarish bilan bog‘liq talablari, Universitetning barcha xodimlari uchun majburiydir.

1.6 Tizim administratori o‘z faoliyatida quyidagilar asosida ish olib boradi:

- Universitetning axborot xavfsizligi siyosati;
- Universitet rektorining buyruqlari va farmoyishlari;
- qonun hujjatlari, ichki mehnat qoidalari;
- ma’lumotlar bazalarini saqlash, boshqarish va axborot xavfsizligini ta’minlash usullari va ko‘rsatmalari;
- ushbu Yo‘riqnomaga asosan.

2. Tizim administratorining vazifalari va majburiyatlari

2.1 Ma’lumotlar bazalarining normal ishlashi va axborot xavfsizligini ta’minlash uchun Tizim administratori quyidagilarni bajaradi:

- axborot tizimlarining, shu jumladan server uskunalari, tizimli va amaliy dasturlarning uzluksiz ishlashi;
- axborot tizimining serverlarini sozlash va boshqarish, server saqlash tizimi va ma’lumotlarni saqlash tizimining barcha xususiyatlarini ko‘rish va o‘zgartirish;
- axborot tizimi foydalanuvchilari uchun rollar/vakolatlarni yaratish va belgilash;
- serverni saqlash va ma’lumotlarni saqlash tizimlarining parametrlari va konfiguratsiyasini, shuningdek ularning ishlashi va nosozliklari jurnallarini tekshirish;

- axborot tizimining serverlaridan ma’lumotlarni zaxiralash va tiklash;

- ma’lumotlar bazasidagi ma’lumotlarning yaxlitligini tekshirish vositalaridan foydalangan holda ma’lumotlar bazasini tekshirish;

- ma’lumotlar bazalari uchun zaxira va tiklash tizimlarini sozlash;

- MBBT ishini nazorat qilish;

- ma’lumotlar bazasini o‘rnatish va sozlash;

- tegishli hujjatlarni rasmiylashtirish va jurnallarni to‘ldirish.

2.2 Tizim administratori:

- favqulodda vaziyatlarni o‘z ichiga olgan ma’lumotlarning oldingi talqinlarini tiklash;

- operatsiya bilan parallel ravishda ma’lumotlar bazalarini qayta tashkil etish;

- ma’lumotlar bazalarini ruxsatsiz kirishdan himoya qilish;

- MBBT parametrlarini o‘rnatish;

- MBBTning amaldagi holatini kuzatib borish;

- ma’lumotlar bazalari bilan ishlaydigan dasturlar uchun statistik ma’lumotlarni yig‘ish yoki taqdim etish vositalarining mavjudligini nazorat qilish;

- ma’lumotlar bazasining kelajakdagi joylashuvi parametrlarini o‘rnatish va u uchun yetarli darajada disk maydoni ajratish;

- ma’lumotlarning zaxira nusxasini yaratish;

- ma’lumotlar bazalari bilan ishlaydigan yoki ma’lumotlar bazalari bilan o‘zaro aloqada bo‘lgan dasturlardan foydalaniladigan bo‘limlar xodimlarining harakatlarini nazorat qilish;

- kerakli apparat va dasturiy ta’minot bazalarini o‘rnatish va sozlash bo‘yicha ishlarni tashkil etish hamda amalga oshirish;

- ma’lumotlar bazalari ishidagi turli xil og‘ishlarni o‘z vaqtida bartaraf etish bo‘yicha ishlarni aniqlash va amalga oshirish;

- ma’lumotlar bazalariga, shuningdek ruxsatsiz shaxslarning ma’lumotlar bazalariga ulanishga yo‘l qo‘ymaslik;

- MBBT dasturining xavfsizligini, himoyasini va o‘z vaqtida yangilanishini ta’minlash;

- ma’lumotlar bazasi infratuzilmasini rivojlantirish va uning xavfsizligi darajasini oshirish bo‘yicha takliflar tayyorlash va taqdim etish;

- ma’lumotlar bazasi va ma’lumotlar bazalarining zaxira nusxalarini yaratish bilan bir qatorda, ma’lumotlar bazasi va ma’lumotlar bazalarining yakuniy sozlamalarini muntazam ravishda zaxiralashni amalga oshirish;

- ma’lumotlar bazasi vositalari va jihozlarining jismoniy xavfsizligini nazorat qilish;

- ma’lumotlar bazalariga, shuningdek ruxsatsiz shaxslarning ma’lumotlar bazalariga ulanishga yo‘l qo‘ymaslikka majbur.

2.3 Tizim administratori quyidagilarni bilishi kerak:

- ma’lumotlar bazalarini saqlash uchun hujjatlarni ishlab chiqish va rasmiylashtirish bo‘yicha qoidalar, nizomlar;

- MBBT uchun normativ-texnik va loyihalash hujjatlari;

- ma’lumotlar bazasi dasturiy ta’minotining tarkibiy qismlari arxitekturasi;

- boshqariladigan axborot-kommunikatsiya tizimida profilaktika ishlarini olib borish qoidalari;
- Universitetda tarmoq texnologiyasini amalga oshirish xususiyatlari;
- boshqariladigan operatsion tizimning xususiyatlari;
- ma’lumotlar bazasi dasturiy ta’minotining tarkibiy qismlari arxitekturasi.

1.8 Tizim administratori quyidagilarga majbur:
- operatsion va to‘plangan ma’lumotlarning to‘liq hajmini dolzarb ish sharoitida saqlash, shuningdek axborotni ruxsatsiz kirishdan himoya qilish;
- tashkilotning tarkibiy bo‘linmalarining axborotga bo‘lgan ehtiyojlarini tahlil qilish;
- Universitetning manfaatdor bo‘linmalarining talabiga binoan yangi vazifalarni bajarish uchun dasturiy ta’minotni ishlab chiqish uchun texnik shartlarni tuzish;
- avtomatlashtirilgan axborotni qayta ishlash bilan bog‘liq hujjatlarni hisobga olish va saqlashni amalga oshirish;
- dasturiy vositalarni takomillashtirish bo‘yicha ishlar majmuini amalga oshirish;
- ma’lumotlarni qayta tiklash va qayta tashkil etishning zamonaviy usullarini qo‘llash;
- kasbiy vazifalarni bajarish uchun zarur bo‘lgan ma’lumotlarni mustaqil izlashni amalga oshirish;
- ma’lumotlarni zaxira qilish uchun zamonaviy dasturlardan foydalanish;
- ma’lumotlar bazalarini arxivlash;
- ma’lumotlar bazasini boshqarish uchun maxsus vositalar bilan ishlash;
- ma’lumotlar bazasi foydalanuvchilarining haqiqiyligini tekshirish;
- MBBT tarkibiy qismlarini yuklash;
- ma’lumotlarni turli xil saqlash vositalariga nusxalash;
- o‘zi xizmat ko‘rsatadigan apparat, dasturiy, apprat-dasturiy vositalarning doimiy yangilanishi, va versiyasi hamda sborkasini tegishli jadvallarga kiritib borish;
- mehnatni muhofaza qilish, xavfsizlik, ishlab chiqarish sanitariyasi va yong‘indan himoya qilish qoidalariga rioya qilish.

2.3 Tizim administratoriga quyidagilar taqiqlanadi:
- ishchi stansiyalarni qarovsiz (shu jumladan ish holatida) qoldirish;
- axborot xavfsizligi talablarini buzish.

3. Tizim administratorining huquqlari

3.1 Tizim administratori quyidagi huquqlarga ega:
- himoya qilinadigan resurslarga ruxsatsiz kirishni amalga oshirgan yoki boshqa axborot xavfsizligi talablarini buzgan Universitet xodimlarini axborot tizimidan uzib qo‘yish;
- ma’lumotlar bazalarini tekshirishda qatnashish;
- MBBT va ma’lumotlar bazalarining ishlashi bilan bog‘liq risklarni keltirib chiqarishi mumkin bo‘lgan nostandart dasturiy ta’minotni o‘rnatishni taqiqlash;
- tizim administratorning o‘z faoliyati, ma’lumotlar bazalarining ishlashini va rivojlanishini ta’minlaydigan qarorlari loyihalari bilan tanishish;

- o‘z vazifalarini takomillashtirish va axborot xavfsizligini ta’minlash bo‘yicha Departament boshlig‘iga takliflar kiritish;

- Departament boshlig‘i bilan kelishilgan holda, MBBTdan foydalanish qoidalarini belgilash, o‘zgartirish va boshqarish;

- Universitet hisobidan muntazam malaka oshirish.

4. Tizim administratorining javobgarligi

4.1 Tizim administratori quyidagi hollarda javobgar bo‘ladi:

- ushbu Yo‘riqnomada nazarda tutilgan o‘z vazifalarini bajarmaganligi yoki lozim darajada bajarmaganligi;

- ma’lumotlar bazalari bilan bog‘liq harakatlarni nazorat qilish bo‘yicha ularning ishlarining sifati, ularni himoya qilishning belgilangan darajasi va holati;

- texnika xavfsizligi qoidalarini buzganligi uchun javobgardir.

Universitet axborot xavfsizligi
siyosatiga 5-ilova

Axborot va kiberxavfsizlikni ta’minlash bo‘yicha mas’ul xodim YO‘RIQNOMASI

1. Umumiy qoidalar

1.1 Ushbu yo‘riqnoma Universitet infratuzilmasida axborot va kiberxavfsizlikni ta’minlashga, shuningdek axborot va kiberxavfsizlik insidentlariga javobgar bo‘lgan xodim (keyingi o‘rinlarda — axborot xavfsizligi administratori)ning majburiyatlarini belgilashga mo‘ljallangan.

1.2 Universitetda axborot xavfsizligini ta’minlash bo‘yicha ishlarni tashkil etish va muvofiqlashtirish Axborot xavfsizligi administratori zimmasiga yuklatiladi.

1.3 Axborot xavfsizligi administratori lavozimiga tayinlanadigan nomzodlar Departament boshlig‘i tomonidan ushbu Departament xodimlari orasidan tanlanadi va Universitet rahbariyatining tegishli buyrug‘i bilan tayinlanadi.

1.4 Universitetda axborot xavfsizligi administratorining huquqlari va majburiyatlari ushbu yo‘riqnomada belgilangan va lavozim yo‘riqnomasiga qo‘shimcha tarzda keltirilgan.

Axborot xavfsizligi administratori ma’lum sabab bilan ish joyida bo‘lmaganligi vaqtida uning ushbu Yo‘riqnomada belgilangan huquqlari, vazifalari va majburiyatlari Departament boshlig‘i qarori bilan Departamentning boshqa bir xodimi zimmasiga yuklanadi.

1.5 Axborot xavfsizligi administratori axborot va kiberxavfsizlik sohasida kamida 3 yil ish tajribasiga ega bo‘lishi kerak.

1.6 Axborot xavfsizligi administratorining o‘z vazifalarini bajarish bilan bog‘liq talablari Universitetning barcha xodimlari uchun majburiydir.

1.7 Axborot xavfsizligi administratori quyidagilarga asoslangan holda ish yuritadi:

- Universitetning axborot xavfsizligi siyosati;
- axborot xavfsizligi ta’minlash sohasidagi me’yoriy-huquqiy hujjatlar;
- Universitet rektorining buyruqlari va farmoyishlari;
- qonun hujjatlari, ichki mehnat qoidalari;
- ushbu yo‘riqnomaga asosan.

2. Axborot xavfsizligi administratorining vazifalari

2.1 Universitet axborot xavfsizligi administratorining asosiy vazifalari va funksiyalari quyidagilardan iborat:

- Universitetning axborot xavfsizligi siyosatini qayta ko‘rib chiqishda va ma’lumotlarning himoyasini ta’minlash bo‘yicha chora-tadbir rejalarini ishlab chiqishda qatnashish;

- axborot va kiberxavfsizlikni ta’minlash uchun Universitet tomonidan tasdiqlangan chora-tadbirlar rejalarini amalga oshirish;

- axborotlarni muhofaza qilish vositalari, antivirus serveriga xizmat koʻrsatish;
- lokal tarmoq hamda tizim administratorlari tomonidan ma’lumotlar himoyasini tashkil etish boʻyicha majburiyatlarini bajarishini muvofiqlashtirish va nazorat qilish;
- Universitetning axborot xavfsizligi vositalarining ishlashini nazorat qilish;
- Universitetda axborot xavfsizligi ichki va tashqi auditini tashkil etish va oʻtkazish, zaifliklar va axborot tarqalish kanallarini aniqlash;
- Axborot xavfsizligi holatini monitoring qilish va amalga oshirilayotgan chora-tadbirlar samaradorligini baholash;
- Universitetda axborot xavfsizligi tizimini takomillashtirish boʻyicha Departament boshligʻiga takliflar kiritish;
- lokal tarmoq va tizim administratorlari tomonidan aniqlangan axborot va kiberxavfsizlik insidentlari toʻgʻrisida ma’lumot olish, yigʻish, tahlil qilish va bartaraf etish;
- Departament boshligʻini hodisalar toʻgʻrisida oʻz vaqtida xabardor qilish;
- Universitet axborot infratuzilmasida sodir boʻlgan hodisalarni tahlil qilish va ular boʻyicha tekshirish oʻtkazishda ishtirok etish;
- oʻzi xizmat koʻrsatadigan apparat, dasturiy, apprat-dasturiy vositalarning doimiy yangilanishi, va versiyasi hamda sborkasini tegishli jadvalga kiritib borish;
- Universitet xodimlarini Axborot xavfsizligi siyosati talablari va ularni bajarish yuzasidan brifinglar oʻtkazish, bilimlari va amaliy koʻnikmalarini baholash.

3. Axborot xavfsizligi administratorining huquqlari

3.1. Axborot xavfsizligi administratori quyidagi huquqlarga ega:
- axborot xavfsizligini ta’minlash vositalarini loyihalashtirish, qabul qilish, foydalanishga topshirishda ishtirok etish;
- axborot xavfsizligi siyosatiga va axborot xavfsizligini ta’minlash bilan bogʻliq ichki normativ hujjatlarga, shu jumladan boʻlim xodimlari faoliyatini tartibga soluvchi hujjatlarga oʻzgartirishlar kiritish boʻyicha takliflar kiritish;
- Universitet xodimlaridan axborotni qayta ishlash texnologiyalarini qoʻllash va axborot resurslarining ishlashi boʻyicha ma’lumot olish;
- Universitet xodimlari tomonidan axborot xavfsizligi talablari bajarilishini nazorat qilish;
- Universitetda antivirus himoya vositalaridan foydalanish, shuningdek axborot xavfsizligining boshqa vositalaridan foydalanish bilan bogʻliq faoliyatni boshqarish;
- avariyalar va baxtsiz hodisalardan soʻng ish faoliyatini tiklash boʻyicha tadbirlarda qatnashish.

4. Axborot xavfsizligi administratorining javobgarligi

4.1 Axborot xavfsizligi administratori quyidagilarga javobgardir:
- ushbu yoʻriqnomada nazarda tutilgan oʻz majburiyatlarini bajarmaganligi yoki lozim darajada bajarmaganligi;
- foydalanuvchilarning xatti-harakatlarini, ularning himoyalanganlik holatini va saqlanishini boshqarish boʻyicha ishlarning sifatsizligi;

- himoya vositalarining ekspluatatsiyasi;
- axborotga kirish bo‘yicha vakolatlarni taqsimlash;
- kompyuter tizimlarini faoliyatini monitoringini o‘tkazish;
- axborot xavfsizligi siyosati bilan xodimlarni tanishtirish haqidagi jurnalni to‘ldirish;
- texnika xavfsizligi qoidalarini buzish.

Universitet axborot xavfsizligi
siyosatiga 6-ilova

Axborot xavfsizligini ta’minlash sektori va Raqamli ta’lim texnologiyalari departamentining Universitet infratuzilmasida axborot va kiberxavfsizlikni ta’minlash sohasidagi vazifalarini amalga oshirish to‘g‘risidagi NIZOM

1. Asosiy qoidalar

1.1 Ushbu Nizom Axborot xavfsizligini ta’minlash sektori va Raqamli ta’lim texnologiyalari departamentining axborot xavfsizligi sohasidagi vazifalari, huquqlari va majburiyatlarini taqsimlash maqsadida ishlab chiqilgan.

1.2 Universitetda axborot xavfsizligini ta’minlash bo‘yicha ishlarni tashkil etish va muvofiqlashtirish Axborot xavfsizligini ta’minlash sektoriga va texnik tatbiq qilish esa Departamentga yuklangan.

1.3 Departament va Axborot xavfsizligini ta’minlash sektori birgalikda Universitetda axborot xavfsizligini ta’minlash sohasida quyidagi keltirilgan hujjatlar asosida amalga oshiradi:

- Universitetning axborot xavfsizligi siyosati;
- axborot va kiberxavfsizlik sohasidagi normativ hujjatlar;
- Universitet raisining buyruqlari, farmoyishlari va ko‘rsatmalari;
- qonun hujjatlari, ichki mehnat qoidalari;
- ushbu Nizom.

1.5 Axborot xavfsizligini ta’minlash sektori va Departament xodimlari quyidagilar uchun javobgardirlar:

- ushbu Yo‘riqnomada nazarda tutilgan o‘z vazifalarini bajarmaslik yoki lozim darajada bajarmaslik;
- Universitetda axborot xavfsizligini ta’minlash bo‘yicha ishlarning sifati.

2. Asosiy vazifalar va funksiyalar

2.1 Axborot xavfsizligini ta’minlash bo‘yicha Axborot xavfsizligini ta’minlash sektorining asosiy vazifalari quyidagilardan iborat:

- Universitetda axborot xavfsizligini ta’minlash bo‘yicha yo‘nalishlarni shakllantirish, me’yoriy hujjatlar va chora-tadbirlar rejalarini ishlab chiqish;
- AXBTni joriy etish, ishlab chiqish va ishlatish uchun talablarni aniqlash;
- Universitetning axborot xavfsizligini ta’minlash bilan shug‘ullanuvchi mutaxassislar o‘rtasida vazifalarni taqsimlash;
- axborot xavfsizligini ta’minlash bo‘yicha chora-tadbirlar rejalarining bajarilishini nazorat qilish;
- O‘zbekiston Respublikasi Prezidentining 2011-yil 8-iyuldagi “Milliy axborot resurslarini muhofaza qilish bo‘yicha qo‘shimcha chora-tadbirlar to‘g‘risida”gi PQ-

1572-son qaroriga muvofiq akkreditatsiyadan o‘tgan tashkilotlar tomonidan Universitet axborotlashtirish obyektlarini attestatsiyadan o‘tkazish;

- himoya choralarining samaradorligini baholash, shuningdek, audit, ekspertiza va sertifikatlashtirish natijalari bo‘yicha aniqlangan kamchiliklarni bartaraf etish;

- Universitet xodimlarini axborot xavfsizligi masalalari bo‘yicha xabardor qilish, o‘qitish va Universitetda axborot xavfsizligini ta’minlash uchun mas’ul mutaxassislarni tayyorlash;

- Axborot xavfsizligi siyosatining 9-bo‘limiga muvofiq axborot xavfsizligi risklarini tahlil qilish va baholash;

- axborot xavfsizligi intsidentlariga javob berish, axborot xavfsizligi qoidalarining buzilishi holatlari yuzasidan rasmiy tekshiruvni tashkil etish;

- Universitetda axborot xavfsizligini ta’minlash uchun ichki qoidalarini ishlab chiqish va joriy etish;

- axborot xavfsizligi sohasidagi normativ-huquqiy bazani takomillashtirish bo‘yicha taklif tayyorlash va rahbariyatga taqdim etish;

- axborot xavfsizligi siyosatiga o‘zgartirish va qo‘shimchalar kiritish;

- axborot xavfsizligini ta’minlash bo‘yicha chora-tadbirlar rejalarini ishlab chiqish va amalga oshirish bo‘yicha ishlarni tashkil etish;

- konfidensial ma’lumotlar ro‘yxatini, unga kirish huquqiga ega bo‘lgan xodimlar ro‘yxatini va ularga kirish tartibini belgilash;

- himoya qilish obyektlari ro‘yxatini va ularning tasnifini, tahdid modellarini aniqlash;

- axborot tizimlari va boshqa himoya vositalaridan foydalanish imkoniyatiga ega bo‘lgan xodimlar ro‘yxatini tuzish va nazorat qilish;

- himoyalangan obyektlarga kirishni taqsimlash va kirishni nazorat qilishni o‘rnatish;

- ichki va tashqi axborot xavfsizligi auditini tashkil etish va o‘tkazish;

- Universitet rasmiy veb-sayti va boshqa veb-resurslarining axborot xavfsizligi talablariga muvofiqligini tekshirish;

- axborot xavfsizligi hodisalarini aniqlash va ularga javob qaytarish bo‘yicha ishlarni tashkil etish va muvofiqlashtirish;

- axborot xavfsizligi bilan bog‘liq hodisalarni tekshirishni tashkil etish;

- axborot xavfsizligi bilan bog‘liq hodisalarning takrorlanishining oldini olish bo‘yicha chora-tadbirlarni rejalashtirish va amalga oshirish;

- Universitet bo‘linmalari va xodimlariga axborot xavfsizligini ta’minlash masalalarida uslubiy va amaliy yordam ko‘rsatish;

- Universitet xodimlari tomonidan tizimni muhofaza qilish va axborot xavfsizligi bo‘yicha tashkiliy-ma’muriy hujjatlarni amalga oshirish talablariga rioya etilishi ustidan muntazam monitoringni tashkil etish;

- Universitet xodimlari uchun axborot xavfsizligi bo‘yicha brifinglar, treninglar va seminarlar tashkil etish va o‘tkazish.

2.2 Axborot xavfsizligini ta’minlash bo‘yicha Departamentning asosiy vazifalari quyidagilardan iborat:

- Universitetda axborot resurslari va tizimlarini texnik tashkil etish va himoya qilishni ta’minlash;

- axborot xavfsizligi tizimlarini joriy etish va rivojlantirish bo‘yicha amaliy tadbirlarni rejalashtirish va tashkil etish, shu jumladan axborot xavfsizligi vositalarini xarid qilish, sotib olish, o‘rnatish, sinovdan o‘tkazish va qabul qilishni tashkil etish;

- Universitetning axborot infratuzilmasini himoya qilish uchun foydalaniladigan xavfsizlik tizimi uchun mas’ul bo‘lgan xodimlarni aniqlash;

- texnik jihozlarni joylashtirish, kabel yo‘llari va muhandislik tizimlarini yotqizish, zaxiralash va arxivlash, shuningdek, axborot xavfsizligini ta’minlash va unga ishlov berishni boshqarish uchun dasturiy ta’minotning namunaviy nusxalarini yaratish va ulardan foydalanish bo‘yicha maxsus talablarning bajarilishini nazorat qilish;

- ma’lumotlarni qayta ishlash markazining ishlashi, shuningdek, axborot resurslari va tizimlari uchun serverlar va telekommunikatsiya uskunalarini sotib olish, yetkazib berish, o‘rnatish va texnik xizmat ko‘rsatish bo‘yicha uchinchi shaxslar bilan Universitet shartnomalariga muvofiqligini tekshirish.

3. Huquq va majburiyatlar

3.1 Axborot xavfsizligini ta’minlash sektori axborot xavfsizligini ta’minlash uchun quyidagi huquqlarga ega:

- Universitetning axborot xavfsizligini ta’minlash uchun joriy o‘zgartirishlar va yangi ichki qoidalarni qabul qilish;

- Universitet xodimlarini rahbariyat bilan kelishilgan holda axborot xavfsizligini ta’minlash jarayoniga jalb etish, ularning vazifalari va vakolatlarini belgilash;

- Universitet xodimlarini axborot infratuzilmasidan foydalanish qamrovi nuqtai nazaridan nazorat qilish, birinchi navbatda, maksimal vakolatlarga ega bo‘lgan xodimlar tomonidan axborot xavfsizligi talablari buzilishining oldini olish;

- o‘z vakolatlari doirasida boshqarish, saqlash va nazorat qilish usullari, vositalari va mexanizmlarini tanlash, amalga oshirish va qo‘llash;

- axborot xavfsizligi talablarining buzilishi bilan bog‘liq hodisalarni tekshirishni tashkil etish, axborot xavfsizligi talablarini buzganlik uchun qonunbuzarlarni javobgarlikka tortish bo‘yicha rahbariyatga takliflar kiritish.

3.2 Departament quyidagi huquqlarga ega:

- Universitet axborot xavfsizligi siyosatiga o‘zgartirishlar kiritish bo‘yicha takliflar tayyorlash va rahbariyatga kiritish;

- axborot tizimlarida texnik va dasturiy vositalarning ishlashi uchun shaxsiy javobgarlikni belgilash;

- Universitet axborot xavfsizligi siyosatida belgilangan axborot xavfsizligi talablariga rioya qilish bo‘yicha administratorlar tomonidan o‘z vazifalarini bajarishini nazorat qilish.

4. Javobgarlik

4.1 Departament va Axborot xavfsizligini ta’minlash sektori xodimlari ushbu Nizomning talablarini bajarish uchun javobgardir.

4.2 Departament va Axborot xavfsizligini ta’minlash sektori xodimlari o‘zlariga yuklangan vazifalarning sifatliligi uchun javobgardir.

Universitet axborot xavfsizligi
siyosatiga 7-ilova

Tizim va amaliy dasturlarni yangilash, shuningdek, ma’lumotlarning zaxira nusxalarini shakllantirish va tiklash bo‘yicha
NIZOM

1. Umumiy qoidalar

1.1 Tizim va amaliy dasturiy ta’minotni yangilash, shuningdek, ma’lumotlarni zaxiralash va tiklash to‘g‘risidagi ushbu Nizom quyidagilarni belgilaydi:

- qurilmalarning ishlamay qolishi, axborot xavfsizligi buzilishi, foydalanuvchilarning xatolari, favqulodda vaziyatlar (yong‘in, tabiiy ofatlar va boshqalar) natijasida to‘liq yoki qisman yo‘qolgan axborot resurslari yoki ularning qismlari ishini keyinchalik tiklash uchun ma’lumotlarni zaxira qilish tartibi;
- ma’lumotlarni zaxiralash, tizim va amaliy dasturlarni o‘rnatish, o‘zgartirishlar kiritish, sozlash va yangilash tartibi va mas’ul xodimlarning vazifalari;
- tizim va amaliy dasturiy ta’minotni yangilash uchun javobgarlik;
- zaxira nusxalash turlarining tasnifi;
- zaxira nusxa olish va qayta tiklash tartibi;
- zaxira nusxalanadigan ma’lumotlar ro‘yxati;
- zaxira nusxalarini o‘z ichiga olgan axborot tashuvchilarni hisobga olish, saqlash va hisobdan chiqarish tartibi;
- zaxiralash natijalarini boshqarish va javobgarlik.

1.2 Universitetda foydalaniladigan barcha dasturiy ta’minotlar Kiberxavfsizlik to‘g‘risidagi qonuni 19-moddasiga muvofiq sertifikatsiyadan o‘tgan bo‘lishi shart.

1.3 Ushbu Nizom quyidagi faoliyat turlarini tartibga soladi:

- dasturiy ta’minotni o‘rnatish, sozlash, yangilash, o‘zgartirish;
- dasturiy ta’minotni tekshirish va sinovdan o‘tkazish;
- zaxira nusxalarini saqlash va xavfsizligini ta’minlash;
- zaxira nazorati;
- dasturiy ta’minotni yangilash.

1.4 Zaxiralashning maqsadi – apparat, dasturiy ta’minot ishdan chiqqanda yoki favqulodda vaziyatlar yuzaga kelganda ma’lumotlarning yo‘qolishini oldini olish.

1.5 Ushbu Nizom tizim va amaliy dasturiy ta’minotga nisbatan qo‘llaniladi.

1.6 Mazkur Nizom talablariga rioya etilishini nazorat qilish Departament boshlig‘i zimmasiga yuklanadi.

2. Ma’lumotlarni zaxiralash, tizim va amaliy dasturlarni o‘rnatish, o‘zgartirishlar kiritish, sozlash va yangilash tartibi va mas’ul xodimlarning vazifalari

2.1 Dasturiy ta’minotni o‘rnatish, o‘zgartirish, sozlash va yangilash ishlari quyidagi maqsadda amalga oshiriladi:

- dasturiy ta’minotning normal ishlashini ta’minlash;

- dasturiy ta’minot faoliyatida aniqlangan xatoliklar yoki buzilishlarni bartaraf etish;

- dasturiy ta’minotning vazifalari va funksiyalariga o‘zgartirishlar kiritish;

- dasturiy ta’minotning zaif tomonlarini bartaraf etish;

- dasturiy ta’minotning ishlash parametrlarini o‘zgartirish.

2.2 Ma’lumotlarni zaxiralash, tizim va amaliy dasturlarni o‘rnatish, o‘zgartirishlar kiritish, sozlash va yangilash uchun Universitetda Departamentning Tarmoqlarni boshqarish va texnik qo‘llab-quvvatlash sektori bosh mutaxassisi (keyingi o‘rinlarda – Lokal tarmoq administratori) va Departament xodimlari mas’ul bo‘ladi.

2.3 Lokal tarmoq administratori hamda Departament xodimlarining tizim va amaliy dasturlarni yangilash, shuningdek, ma’lumotlarning zaxira nusxalarini shakllantirish va tiklash bo‘yicha vazifalariga quyidagilar kiradi:

- operatsion tizimlarni (masalan, Windows, Linux) o‘rnatish, sozlash va boshqarish;

- yangi ishlab chiqilgan, o‘zgartirilgan yoki sotib olingan dasturiy ta’minotni o‘rnatish;

- foydalanuvchilarning hisoblarini yaratish, o‘zgartirish, bloklash, parollarni boshqarish;

- tizimlarning faoliyatini nazorat qilish, monitoring tizimlarini ishlatish va xato yoki muammolarni aniqlash;

- dasturiy ta’minotni sozlash;

- dasturiy ta’minotni sozlamalariga o‘zgartirish kiritish;

- dastur yoki axborot tizimining ba’zi vazifa va funksiyalarini o‘zgartirish zarurati tug‘ilganda, shuningdek, dastur ishida aniqlangan xatoliklarni bartaraf etish uchun dasturiy ta’minotning manba kodiga o‘zgartirishlar kiritish;

- mavjud qurilmaga o‘rnatilishidan oldin yangi ishlab chiqilgan dasturiy ta’minotni yoki o‘zgartirilgan dasturiy ta’minotni sinovdan o‘tkazish (ishga tushirish);

- ishlab chiqaruvchilarning dasturiy ta’minot yangilanishlarini kuzatib borish;

- dasturiy ta’minotni yangilash;

- o‘rnatish va sozlashdan so‘ng dasturiy ta’minotning to‘g‘ri ishlashini tekshirish, sozlamalarga o‘zgartirishlar kiritish va dasturiy ta’minotni yangilash.

2.4 Dasturiy ta’minotni o‘rnatish quyidagi hollarda amalga oshiriladi:

- axborot tizimini yoki obyektni foydalanishga topshirishda;

- bo‘linmalarning arizasi asosida;

- almashtirishda, yangisini o‘rnatishda yoki mavjud qurilmani qayta o‘rnatishda.

2.5 O‘zgarishlar va dasturiy ta’minotni yangilash quyidagi hollarda amalga oshiriladi:

- dasturiy ta’minot ishlab chiqaruvchisining yangi versiyasi yoki yangilanishlarining paydo bo‘lishi;

- aniqlangan zaifliklarni yoki dasturiy ta’minotdagi xatolarni bartaraf etish zarurati;

- dasturiy ta’minot vazifalari va funksiyalarini o‘zgartirish zarurati.

2.6 Yangilanadigan asosiy dasturlarga quyidagilar kiradi:

- ish stansiyalar va serverlarning operatsion tizimlari, MBBT, log-fayllar;

- axborot tizimlari va resurslari, korporativ elektron pochta va boshqa veb-ilovalar uchun dasturiy ta’minot;

- axborot xavfsizligi va tarmoq qurilmalari uchun dasturiy ta’minot.

2.7 Ishlab chiqaruvchi muhim deb hisoblagan o‘zgarishlar va yangilanishlar o‘z navbatida qo‘llash tartibini belgilash kerak. Muhim sozlamalar yoki yangilanishlarni qo‘llash zarurligi to‘g‘risida xabar olingan kundan boshlab 3 (uch) kun ichida obyektga javobgar administrator tomonidan yangilanish bo‘yicha qaror qabul qilinadi. Bunday yangilanishlarni o‘rnatishdan bosh tortgan taqdirda, aniqlangan zaifliklarni yoki xatoliklarni bartaraf etish uchun yetarli choralar ko‘rilishi shart.

2.8 Dasturiy ta’minot va tizim dasturiy ta’minotidagi yangilanishlar to‘g‘risida ma’lumot manbai dasturiy ta’minot ishlab chiqaruvchisi, internet saytlari bo‘lishi mumkin. Yangilanishlar haqidagi ma’lumotlarning yana bir manbai bu zaiflikni aniqlash va boshqarish tizimining natijalari, xavfsizlik skanerlarining natijalari bo‘lishi mumkin.

2.9 Korporativ elektron pochta dasturiy ta’minotini yangilash zarurligi to‘g‘risida qaror Universitetning axborot-kommunikatsiya texnologiyalarini joriy etish va raqamlashtirish bo‘yicha mas’ul rahbari (keyingi o‘rinlarda – Mas’ul rahbar) tomonidan qabul qilinadi. Ushbu yangilanishlar ish vaqtidan tashqarida (serverning haddan tashqari yuklanishi bo‘lmasligi uchun) amalga oshirilishi kerak. Yangilanishdan so‘ng serverlar yoki vositalarning normal ishlashini, yangilangan dasturiy ta’minotni, ularga o‘rnatilgan dasturiy ta’minotni va ma’lumotlarning yaxlitligini baholash uchun barcha tekshiruvlar va testlar o‘tkazilishi kerak.

2.10 Tizim dasturiy ta’minotini, axborotni muhofaza qilish vositalarini va tarmoq qurilmalarini yangilash tizim administratorlari tomonidan avtomatik ravishda yangilaydigan qilib sozlanishi kerak.

2.11 Ilova dasturiy ta’minotiga o‘zgartirishlar, uni ishlab chiquvchi tomonidan o‘zgartirilganda, Universitetning funksional imkoniyatlariga o‘zgartirish kiritish zarurati yoki axborot resurslarini yanada rivojlantirish zarurati bilan bog‘liq holda kiritiladi.

2.12 Axborot tizimlari va resurslari uchun ularni dasturiy ta’minotini o‘zgartirish bo‘yicha quyidagi talablar bajarilishi kerak:

- o‘zgartirilgan dasturiy ta’minot yoki axborot tizimining barcha mavjud va yangi funksiyalarining ishlashini tekshirish alohida sinov serverida amalga oshirilish;

- o‘zgartirilgan dasturiy ta’minotni to‘liq tekshirilgandan so‘ng ish vaqtidan tashqari vaqtda o‘rnatish;

- o‘zgartirilgan dasturiy ta’minotni o‘rnatishda axborot tizimi ma’lumotlar bazasidagi barcha ma’lumotlarning xavfsizligini ta’minlash;

- o‘rnatishdan so‘ng, serverlarning normal ishlashini, ularga o‘rnatilgan o‘zgartirilgan dasturiy ta’minotni va axborot tizimi ma’lumotlarining xavfsizligini baholash uchun barcha tekshiruvlar va sinovlarni o‘tkazish.

2.13. Quyidagi dasturiy ta’minot majburiy yangilanishi kerak:

- domen boshqaruvchisi serverining operatsion tizimlari, fayl serveri, axborot tizimlarining ma’lumotlar bazalari serverlari va axborot tizimining dastur serverlari, lokal elektron pochta serverlari, boshqa axborot almashish tizimlari;

- axborot tizimlari ma’lumotlar bazasi serverlarining ma’lumotlar bazasi;

- axborot tizimlarining ilovalari (dasturiy dasturlari);

- axborot xavfsizligi vositalari va xavfsizlik serverlarining operatsion tizimi uchun dasturiy ta’minot;

- ishchi stansiyasining operatsion tizimlari.

2.14. Universitetning muhim uskunalari bo‘yicha dasturiy ta’minot yangilanishini qabul qilishdan oldin ushbu Nizomning 3-bo‘limiga muvofiq sinov uskunalarida yangilangan dasturiy ta’minotning ishlashini sinash va tekshirish bo‘yicha choralar ko‘rilishi mumkin.

2.15. Muhim uskunalar bo‘yicha dasturiy ta’minotni yangilash ishlamaydigan vaqtlarda amalga oshiriladi.

2.16. Ishlab chiqaruvchi yoki ishlab chiqaruvchi dasturiy ta’minotni avtomatik yangilash uchun tuzilgan tashkilot uskunasi uchun har bir yangilashdan so‘ng ushbu Nizomning 3.13-bandi talablariga muvofiq uskunaning to‘g‘ri ishlashi tekshirilishi kerak.

2.17. Yangilangan dasturiy ta’minot yoki tegishli ilovalarning ishlashida og‘ishlar aniqlansa zavod sozlamalariga qaytish yoki dasturiy ta’minotning oldingi dasturiy ta’minot versiyasini tiklash yoki dasturiy ta’minotning oxirgi saqlangan ishchi versiyasini tiklash kerak.

Bunday holda, ushbu Nizomning 3-bo‘limi talablariga muvofiq yangilangan dasturiy ta’minotni sinovdan o‘tkazgandan va tekshirishdan so‘ng dasturiy ta’minotni keyingi yangilash amalga oshirilishi yoki dasturiy ta’minotni yangilashni taqiqlash to‘g‘risida qaror qabul qilinishi kerak.

2.18. Operatsion dasturiy ta’minotga o‘zgartirishlar (manba kodidagi o‘zgarishlar) quyidagi hollarda kiritilishi mumkin:

- dasturiy ta’minotning ishlashini takomillashtirish zarurati — dasturiy ta’minotning vazifalari va funksiyalariga o‘zgartirishlar yoki qo‘shimchalar kiritish, mahsuldorlikni, ishonchlilikni oshirish yoki axborotni qayta ishlash jarayonlarini o‘zgartirish va boshqalar;

- dasturiy ta’minotning ishlashida aniqlangan xatolar yoki buzilishlarni, shuningdek, dasturiy ta’minotda aniqlangan zaifliklarni bartaraf etish.

2.19. Dasturiy ta’minotga o‘zgartirishlar quyidagi hollarda kiritiladi:

- Universitet iltimosiga binoan dasturiy ta’minotni ishlab chiquvchi (ishlab chiqaruvchi) tomonidan;

- dastlabki kod mavjud bo‘lsa.

3. Dasturiy ta’minotni tekshirish va sinovdan o‘tkazish

3.1. Xarid qilingan, yangi ishlab chiqilgan yoki o‘zgartirilgan dasturiy ta’minotni Universitetning uskunalariga o‘rnatishdan oldin uni tekshirish (sinovdan o‘tkazish) kerak.

Universitetning axborot tizimlari uchun qo‘shimcha ishlab chiqilgan dasturiy ta’minot sinovdan o‘tkazilishi kerak. Foydalanish muddati axborot tizimini ishlab chiqish uchun texnik shartlarda belgilanadi.

3.2. Dasturiy ta’minotni tekshirish (testdan o‘tkazish)dan maqsad dasturiy ta’minotning ishlashi va axborot xavfsizligiga qo‘yiladigan talablarni ishlab chiqish sifati va bajarilishini baholashdan iborat.

3.3. Dasturiy ta’minotni tekshirish va sinovdan o‘tkazishda quyidagilar tekshiriladi:

- ishlab chiqilgan (o‘zgartirilgan) dasturiy ta’minotning axborot tizimini yaratish yoki ishlab chiqish (modernizatsiya qilish) uchun ishlab chiqish yoki texnik shartlarga qo‘yiladigan talablarga muvofiqligi;
- dasturiy ta’minot orqali barcha talab qilinadigan vazifalar va funksiyalarni bajarish;
- dasturiy ta’minot bilan bog‘liq ilovalarning ishlashi;
- dasturiy ta’minot tomonidan barcha jarayonlarni bajarishda xatolarning yo‘qligi;
- dasturiy ta’minotni ishlatish va ishlatishning soddaligi va qulayligi;
- uning ishlashi davomida dasturiy ta’minot tomonidan yaratilgan ortiqcha yukning yo‘qligi;
- ishlab chiquvchi tomonidan e’lon qilinmagan potensial xavfli funksionallikning yo‘qligi va boshqalar.

Dasturiy ta’minotni sinovdan o‘tkazishda ishlashi, zarur yoki ortib borayotgan yuk (so‘rovlar, so‘rovlar va boshqalar) mavjud bo‘lganda uning ishlashi va axborot tizimining ishonchliligi qo‘shimcha ravishda tekshiriladi va sinov paytida aniqlanmagan xato va kamchiliklar aniqlanadi.

3.4. Tekshirilayotgan dasturiy ta’minotdagi quyidagi jarayonlar e’lon qilinmagan funksionallik deb hisoblanadi:

- fayl tizimiga, ma’lumotlar bazalariga, elektron pochtaga va dasturiy ta’minotning funksionalligi bilan bog‘liq bo‘lmagan boshqa ma’lumotlarga kirishga urinishlar;
- uchinchi tomon tarmoq manzillari va domen nomlariga hujjatsiz qo‘ng‘iroqlar;
- zararli dasturiy ta’minotning tizimli qo‘ng‘iroqlari;
- dasturiy ta’minotni o‘rnatish natijasida fayl tizimidagi potensial xavfli o‘zgarishlar;
- operatsion muhit konfiguratsiyasidagi o‘zgarishlar (masalan, yangi avtomatik yuklangan dasturlarning paydo bo‘lishi);
- axborot xavfsizligi vositalarini yoki axborotni himoya qilish funksiyalarini o‘chirish va hokazo.

3.5. Dasturiy ta’minotni sinovdan o‘tkazish administratorlar tomonidan amalga oshiriladi.

3.6. Sinovdan o‘tkazilayotgan har bir dasturiy ta’minot uchun dasturiy ta’minotni sinovdan o‘tkazish bo‘yicha ishlarning tartibi va mazmunini belgilovchi test metodologiyasi tayyorlanadi.

3.7. Dasturiy ta’minotni sinovdan o‘tkazish uchun Universitetda foydalanishda bo‘lgan asbob-uskunalar bilan bog‘liq bo‘lmagan virtual muhit bo‘lgan sinov dastgohi yaratiladi.

3.8. Dasturiy ta’minotni sinovdan o‘tkazish axborot xavfsizligi administratori bilan kelishilgan holda, mavjud uskunada faqat ish vaqtidan tashqarida o‘tkazilishi mumkin.

3.9. Ishlab chiqish sifatini baholash va axborot xavfsizligini ta’minlash uchun ishlab chiqilgan dasturiy ta’minot qo‘shimcha ravishda dastlabki kod tahlilidan o‘tkazilishi mumkin.

Dasturiy ta’minotdagi xatolar va zaifliklarni aniqlash uchun manba kodini tahlil qilish amalga oshiriladi. Ushbu tahlil alohida mutaxassis dasturchi tomonidan qo‘lda va/yoki manba kod analizatori (ixtisoslashtirilgan dasturiy ta’minot) yordamida amalga oshiriladi.

Manba kodini tahlil qilish axborot xavfsizligi administratori tomonidan amalga oshiriladi.

3.10. Sinov yoki sinovdan o‘tkazish jarayonida aniqlangan har qanday izohlar dasturiy ta’minotga tegishli o‘zgartirish va qo‘shimchalar kiritish uchun ishlab chiquvchiga taqdim etiladi.

Dasturiy ta’minotga o‘zgartirish va qo‘shimchalar kiritilgandan so‘ng, agar kerak bo‘lsa, u qayta sinovdan o‘tkaziladi, sinov muddati uzaytirilishi mumkin;

3.11. Dasturiy ta’minot muvaffaqiyatli sinovdan o‘tkazilgandan yoki sinovdan o‘tkazilgandan so‘ng uni mavjud uskunaga o‘rnatishga (ishga tushirishga) ruxsat beriladi.

3.12. Dasturiy ta’minotni sinovdan o‘tkazishni muvaffaqiyatli yakunlash natijalari bo‘yicha dalolatnoma tuziladi, uni sinovdan o‘tkazishda foydalanish jarayonida ishtirok etuvchi mutaxassislar imzolaydilar.

3.13. Dasturiy ta’minot yangilanishini sinovdan o‘tkazish deyarli yaratilgan sinov uskunasida amalga oshiriladi, mavjud muhim uskunalarda avtomatik yangilanishlar o‘chiriladi.

Dasturiy ta’minot yangilanishi sinov uskunasiga kelgandan so‘ng, u tekshiriladi (sinovdan o‘tkaziladi):

- yangilangan dasturiy ta’minot va tegishli ilovalarni ishga tushirish;
- talab qilinadigan jarayonlarning qotib qolmasligi yoki bajarilmasligini tekshirish;
- antivirus yangilanishlarni boshqarish;
- ma’lumotlar xavfsizligini tekshirish;
- e’lon qilinmagan funksionallik deb hisoblanishi mumkin bo‘lgan xavfli yangilanish faoliyatini kuzatish va qidirish va h.k.

Ushbu tekshirish har bir yangilash uchun amalga oshirilishi kerak.

3.14. Yangilangandan keyin sinov uskunasining normal ishlashini baholash kamida 12 soat bo‘lishi kerak.

3.15. Universitetning axborot tizimini yaratish yoki ishlab chiqish (modernizatsiya qilish) uchun dasturiy ta’minot sinovdan o‘tkazilgandan so‘ng ushbu axborot tizimi O‘zbekiston Respublikasi Prezidentining 2020-yil 15-iyundagi PQ-

4751-son qaroriga muvofiq texnik shartlar talablariga muvofiqligi va axborot xavfsizligi talablariga muvofiqligi bo‘yicha ekspertizadan o‘tkazilishi shart.

Ko‘rsatilgan ekspertiza axborot xavfsizligi administratori tomonidan tashkil etilgan va amalga oshiriladigan axborot tizimini joriy etishdan oldin amalga oshirilishi lozim.

4. Zaxira nusxalash turlarining tasnifi

4.1 Zaxiralanadigan ma’lumotlar turlariga ko‘ra quyidagilarga bo‘linadi:

- operatsion tizimlar va yordamchi dasturlar;
- amaliy (ixtisoslashtirilgan) dasturiy ta’minot;
- ma’lumotlar.

4.2 Zaxira ma’lumotlarini saqlash joylari:

- serverlar;
- ish stansiyalar;
- qattiq disklar yoki qattiq disklarning bo‘sh joylari.

4.3 Zaxiralash usullari:

- klonlash (point-in-time), ya’ni jildlarning (klonlarning) bir nechta fizik nusxalarini yaratish;
- tezkor nusxani yaratish (snapshot), ya’ni diskning mantiqiy nusxasini, uning obrazini yaratish;
- nusxalash.

4.4 Saqlangan ma’lumotlarning to‘liqligi bo‘yicha:

- to‘liq zaxira (Full backup) – barcha ma’lumotlarni zaxira nusxasini yaratish, texnologik qurilmalarni to‘liq tiklash uchun zarur;
- qo‘shimcha zaxira – (Incremental backup) avvalgi to‘liq yoki qo‘shimcha zaxiralashdan keyin o‘zgartirilgan barcha ma’lumotlarning zaxira nusxasini yaratish (Differensial zaxiradan farqli o‘laroq o‘zgargan yoki yangi fayllar eskilarini almashtirmaydi va mustaqil xotiraga yoziladi);
- Differensial zaxira – (Differential backup) avvalgi to‘liq zaxiralashdan keyin o‘zgartirilgan barcha ma’lumotlarning zaxira nusxasini yaratish.

4.5 Tashuvchiga kirish usuliga ko‘ra:

- onlayn zaxira (Online backup) – doimiy ulangan (to‘g‘ridan-to‘g‘ri yoki tarmoq orqali) zaxira arxivini yaratish;
- avtonom zaxira – (Offline backup) foydalanishdan oldin o‘rnatilishi kerak bo‘lgan zaxira nusxasini olinadigan muhitda yoki kartridjda saqlash.

4.6 Zaxira vaqti bo‘yicha:

- real vaqtda zaxira nusxalari – ma’lumotlar tizimda paydo bo‘lganda to‘g‘ridan-to‘g‘ri zaxiralash-ko‘paytirish, tarqatish va hokazo.
- rejalashtirilgan zaxira nusxalari – ma’lumotlar oldindan belgilangan vaqtlarda zaxiralanadi.

4.7 Zaxira nusxasi to‘plami bo‘yicha:

- sutkalik to‘plam, nusxa ko‘chirish oyning 1-sanasi va yakshanba kunidan tashqari har sutkaning yuklamalar nisbatan kam bo‘lgan soatlarida amalga oshiriladi;

- haftalik to‘plam, nusxa ko‘chirish oyning har yakshanbasining yuklamalar nisbatan kam bo‘lgan soatlarida amalga oshiriladi, agar oyning 1-sanasiga to‘g‘ri kelmasa;

- oylik to‘plam, nusxa ko‘chirish har oyning 1-sanasida, sutkaning yuklamalar nisbatan kam bo‘lgan soatlarida amalga oshiriladi, agar u 1-yanvarga to‘g‘ri kelmasa;

- yillik to‘plam, nusxa ko‘chirish 1-yanvarda amalga oshiriladi va 3 yil saqlanadi.

5. Zaxira nusxa olish va qayta tiklash tartibi

5.1 Zaxira nusxa olish tartibi

5.1.1 Axborot quyidagi ma’lumotlar asosida zaxiralanadi: zaxira qilinadigan ma’lumotlarning tarkibi va hajmi, zaxiralash vaqti va nusxalarning saqlash muddati.

5.1.2 Zaxira tizimi muhim ma’lumotlarni saqlash uchun yetarli ishlashni ta’minlashi kerak.

5.1.3 Inson omilini kamaytirish va zararni minimallashtirish maqsadida zaxira olish va qayta tiklash tizimini nazorat qiluvchi xodimlarning minimal aralashuvini hisobga olgan holda avtomatlashtirish kerak.

5.1.4 Zaxira nusxa oluvchi quyidagilarni ta’minlashi kerak:

- zaxira tizimini ishga tushirish;

- zaxira tizimining konfiguratsiyasiga sezilarli o‘zgarishlar kiritish;

- zaxira jurnalini tahlil qilish, zaxira sozlamalariga o‘zgartirish kiritish zarurligini kuzatib borish;

- zaxira nusxalash yoki jihozlarni nazorat qilish;

- zaxira nusxalash natijalarini boshqarish;

- zaxira nusxalarini o‘z ichiga olgan saqlash vositalarini saqlash tartibi va shartlarini bajarish;

- zaxira nusxalaridan ma’lumotlarni qayta tiklash.

5.1.5 Zaxira nusxa olingandan so‘ng, ushbu Nizomning 7-bo‘limiga muvofiq barcha zaxira jarayonlari natijalari kuzatilishi kerak.

5.1.6 Axborotning zaxira nusxasi uchun mas’ul bo‘lgan shaxs ushbu Nizomning 6-bo‘limi talablariga muvofiq nusxa ko‘chirilgan nusxaning xavfsizligini ta’minlashi shart.

5.1.7 Zaxira tizimi ishlamay qolganda, zaxira qilinadigan ma’lumotlarning kunlik nusxasi uni saqlash uchun disk hajmining zarur hajmiga ega bo‘lgan serverlarning fayl tizimlari vositalari yordamida amalga oshiriladi.

5.1.8 Agar zaxira tizimi mavjud bo‘lmasa, zaxira nusxasi virtual zaxira serverida amalga oshiriladi.

5.2 Axborotni tiklash tartibi

5.2.1 Zaxira nusxalaridan ma’lumotlarni qayta tiklash axborot tizimining yoki uning tarkibiy qismining ishlash qobiliyati yo‘qolgan taqdirda amalga oshiriladi va Axborot xavfsizligi administratori hamda Bo‘lim boshlig‘i nazoratida amalga oshiriladi.

5.2.2 Zaxira nusxasini tiklash jarayonida zaxira tizimiga biriktirilgan hujjatlarda va axborot tizimining dasturiy ta’minotini ishlab chiquvchi hujjatida tasvirlangan zaxira nusxalaridan ma’lumotlarni tiklash bo‘yicha ko‘rsatmalarga amal qilish kerak.

5.2.3 Ma’lumotlarni tiklash rejada belgilangan muddat ichida amalga oshiriladi.

5.2.4 Zaxira ma’lumotlarining tiklanishini tekshirish tartibi ular tiklangandan so‘ng darhol amalga oshiriladi.

5.2.5 Qayta tiklanganidan so‘ng zaxiralangan ma’lumotlarni tekshirishda quyidagilar amalga oshiriladi:

- barcha tiklash jarayonlarining to‘g‘riligini tekshirish, ya’ni amalga oshirilgan jarayonlar ro‘yxati va ularni amalga oshirishda xatoliklar mavjud emasligi;
- ko‘chirilgan ma’lumotlar, fayllar, kataloglar ro‘yxati;
- tiklangan fayllar hajmi, ya’ni ma’lumotlarning yaxlitligi tegishli ilovalardagi fayllarni navbatma-navbat ochish orqali baholanadi;
- qayta tiklangan ma’lumotlarda virusga qarshi vositalar yordamida zararli dasturlarning yo‘qligini tekshirish.

5.2.6 Zaxiralangan ma’lumotlarning tiklanishining to‘g‘riligini tekshirish bo‘yicha belgilangan jarayonlar Axborot xavfsizligi administratori hamda Departament boshlig‘i tomonidan amalga oshiriladi.

5.2.7 Agarda xatolik aniqlansa hamda zarurat tug‘ilganda Axborot xavfsizligi administratori va Departament boshlig‘i bu haqda Mas’ul rahbarga darhol xabar beradi.

5.3 Zaxira nusxalanadigan ma’lumotlar ro‘yxati

5.3.1 Quyidagilar zaxira nusxalanadi:

- texnologik qurilmalarning ishlashini tiklash uchun zarur bo‘lgan ma’lumotlar (operatsion tizimlar, amaliy dasturlar, tizim konfiguratsiyasi);
- ishchi ma’lumotlar (ma’lumotlar bazalari, fayllar).

5.3.2 Universitetda zaxira nusxalanadigan ma’lumotlar ro‘yxati ushbu Nizom ilovasida (1-jadval) keltirilgan.

5.3.3 Ushbu ro‘yxat yangi axborot tizimlari hamda resurslari va/yoki vositalari paydo bo‘lishi bilan o‘zgartirilishi va to‘ldirilishi mumkin.

5.3.4 Ushbu ro‘yxatga o‘zgartirish va qo‘shimchalar kiritish bo‘yicha takliflar Axborot xavfsizligi administratori hamda Departament boshlig‘i tomonidan tayyorlanadi Mas’ul rahbarga taqdim etiladi.

6. Zaxira nusxalarini o‘z ichiga olgan axborot tashuvchilarni hisobga olish, saqlash va hisobdan chiqarish tartibi

6.1 Zaxira nusxalarini saqlash xavfsizligi uchun quyidagi choralar ko‘rilishi kerak:

- zaxira nusxalarini saqlash ruxsatsiz shaxslar kirishi cheklangan server xonasida joylashgan ma’lumotlarni saqlash tizimida amalga oshiriladi;
- saqlash tizimidagi ma’lumotlarning yaxlitligini tekshirish;
- saqlangan zaxira nusxalarining xavfsizligi uchun ma’lumotlarni saqlash tizimida RAID-dan foydalanish;

- faqat tizim administratori ma’lumotlarni saqlash tizimiga mantiqiy kirish huquqiga ega;

- ma’lumotlarni saqlash tizimiga kirishda tizim administratorining ikki faktorli autentifikatsiyasidan foydalanish;

- saqlash tizimining axborot vositalarini hisobga olish.

6.2 Zaxira nusxasini saqlaydigan ma’lumot tashuvchilarga, ushbu ma’lumotlarning eng yuqori konfidensiallik darajasiga qarab, konfidensiallik darajasi belgilanadi.

6.3 Zaxira vositalarini yozib olish va belgilash kerak (nusxa ko‘chirish sanasi, resurs nomi, saqlash muddati, nusxalari soni, jildning raqami va boshqalar).

6.3 Zaxira vositalarini hisobga olish, mobil qurilmalar, ma’lumotlarni saqlash qurilmalari bilan ishlash Siyosatning 10-ilovasi “Mobil, ma’lumot saqlovchi va tashuvchi qurilmalar bilan ishlashda axborot xavfsizligini ta’minlash bo‘yicha yo‘riqnoma”ga asosan amalga oshiriladi.

Zaxira nusxalarini tashuvchi vositalar Siyosatning 14-ilovasi “Axborot aktivlarini boshqarish tartibi”da keltirilgan. Axborot aktivlarini boshqarish tartibi talablariga muvofiq axborot aktivlari sifatida belgilanadi.

6.4 Zaxira vositalarni hisobdan chiqarish va yo‘q qilish Siyosatning 10-ilovasi “Mobil, ma’lumot saqlovchi va tashuvchi qurilmalar bilan ishlashda axborot xavfsizligini ta’minlash bo‘yicha yo‘riqnoma”da keltirilgan tashqi tashuvchi vositalari, mobil qurilmalar, ma’lumotlarni saqlash qurilmalari bilan ishlashda xavfsizlikni ta’minlash bo‘yicha yo‘riqnomaga muvofiq amalga oshiriladi.

7. Zaxiralash natijalarini boshqarish

7.1 Barcha zaxira jarayonlari natijalarini nazorat qilish Axborot xavfsizligi administratorlari hamda Departament boshlig‘i tomonidan amalga oshiriladi.

7.2 Ushbu Nizomning ilovasida keltirilgan 1-jadvalda ko‘rsatilgan zaxira qilingan ma’lumotlarning qolgan qismi uchun zaxira jarayonlari natijalarini boshqarish zaxira nusxasi yaratilgandan so‘ng darhol amalga oshiriladi.

7.3 Axborot resurslari va korporativ elektron pochta xabarlarining zaxira nusxalarini yaratish jarayonlari natijalarini nazorat qilish 1-jadvalda ko‘rsatilgan zaxira tizimlari tomonidan amalga oshiriladi.

7.4 Zaxira nusxalarini boshqarish vaqtida quyidagilar tekshiriladi:

- barcha nusxalarning ko‘chirish jarayonlari to‘g‘riligi, ya’ni nusxalashda xatolik mavjud emasligi;

- nusxalangan ma’lumotlar, fayllar, kataloglar ro‘yxati;

- ko‘chirilgan fayllar hajmiga mos kelishi;

- virusga qarshi vositalar tomonidan zararli dasturlarning yo‘qligini tekshirish.

7.5 Agar xatolik aniqlansa tegishliligi bo‘yicha Lokal tarmoq administratorlari hamda Departament xodimlari Axborot xavfsizligi administratori yoki Departament boshlig‘ini darhol xabardor qiladi.

7.6 Agar zaxira olishda xatolar kuzatilsa, zaxira nusxa olish takroran amalga oshiriladi. Agar yana xatolar yuzaga kelsa, uning sabablari aniqlanadi: zaxira

tizimining noto‘g‘ri ishlashi yoki noto‘g‘ri sozlanganligi, zaxira nusxasi tashuvchisining to‘lganligi yoki ishdan chiqqanligi bo‘yicha ularni bartaraf etish choralari ko‘riladi.

8. Hodisalar jurnallarini yuritish va ularning saqlanishini ta’minlash

8.1 Universitetda quyidagi maqsadlarda hodisalar jurnallari (loglar)ni yig‘ish, qayta ishlash va saqlash amalga oshirilishi kerak:

- axborot xavfsizligini nazorat qilish (axborot xavfsizligi buzilishi hodisalarini aniqlash);
- foydalanuvchilar, jumladan imtiyozli foydalanuvchilar (ma’muriy harakatlar) harakatlarini hisobga olish (huquq buzilishi holatlarini aniqlash uchun);
- o‘zaro aloqada bo‘lgan axborot tizimlari so‘rovlarini to‘g‘ri qayta ishlanishini tekshirish;
- ishlash holatini nazorat qilish – muhim tizimlarda xatoliklar va nosozliklarni qayd qilish.

8.2 Quyidagi muhofaza obyektlarida voqealar majburiy ravishda jurnalga yozilishi (loglanishi) shart:

- tashkilotning barcha axborot tizimlari va resurslari;
- korporativ (mahalliy) tarmoqning yadro kommutatorlari.

8.3 Axborot tizimlari va resurslarda quyidagi hodisalar loglanishi kerak:

1) Autentifikatsiya va avtorizatsiya voqealari (oddiy va imtiyozli foydalanuvchilar):

- foydalanuvchilarning tizimga kirishi/chiqishi (autentifikatsiya);
- muvaffaqiyatsiz kirish urinishlari;
- foydalanuvchi akkaunti bloklanishi;
- parolni tiklash yoki o‘zgartirish;
- taqiqlangan resurslarga kirishga urinishlar.

2) Foydalanuvchi harakatlari:

- fayllar, ma’lumotlar yoki yozuvlarni ko‘rish, yaratish, o‘zgartirish, o‘chirish;
- muhim dastur va skriptlarni ishga tushirish;
- tizim yoki ilovalar sozlamalarini o‘zgartirish;
- konfidensial ma’lumotlar bilan bog‘liq harakatlar.

3) Ma’muriy va imtiyozli harakatlar:

- akkauntlar yaratish, o‘chirish, o‘zgartirish;
- kirish huquqlarini belgilash yoki o‘zgartirish;
- xavfsizlik siyosatlarini sozlash;
- tizim xizmatlarini qayta ishga tushirish;
- xizmatlarni yoqish/o‘chirish;
- serverni yoqish/o‘chirish;
- tizimni qayta ishga tushirish.

4) Tarmoq hodisalari:

- tarmoqqa ulanishlar (SSH, RDP, VPN va boshqalar);
- portlarning ochilishi/yopilishi;

- kiruvchi/chiquvchi ulanishlar.

5) Xatolik va nosozliklar:

- operatsion tizimdagi xatoliklar;
- ilova xatoliklari;
- ma’lumotlar bazasi boshqaruv tizimi (SGBD) xatoliklari;
- serverlarning ortiqcha yuklanishi yoki resurs yetishmovchiligi (CPU, RAM, disk).

8.4 Hodisalar jurnallari (log fayllar) ma’lumotlar bazasi, operatsion tizim va ilovalar bilan birgalikda “Universitetning zaxira nusxa olish ro‘yxati” jadvaliga muvofiq, belgilangan muddatlar va ijrochilar tomonidan zaxira olinadi.

8.5 Yadro kommutatorlaridan hodisalar jurnallarini zaxiralash yoki elektron arxivlash Axborot texnologiyalari departamenti tarmoq administratorlari tomonidan har oyda amalga oshiriladi.

8.6 Tarmoqlararo ekranda quyidagi hodisalar loglanadi:

- ruxsat berilgan va rad etilgan ulanish urinishlari (normal yoki siyosatga zid faollikni aniqlash);
- tarmoqlararo ekran konfiguratsiyasi va siyosat o‘zgarishlari (filtrlash qoidalari, NAT, marshrutlash sozlamalari);
- foydalanuvchi (administrator) autentifikatsiyasi va harakatlari (muvaffaqiyatli/muvaffaqiyatsiz kirish, parolni taxmin qilish, CLI buyruqlari, qayta yuklash);
- tizim hodisalari (qurilmani ishga tushirish/to‘xtatish, xizmat xatoliklari, firmware yangilanishi).
- VPN funksiyasi (masofaviy kirish uchun VPN shlyuzi) bo‘lsa, quyidagilar ham loglanadi:
- VPN sessiyalarining ulanishi/uzilishi;
- tunellar o‘rnatilishidagi xatoliklar;
- ishlatilgan protokollar va parametrlari.

8.7 IDPS tizimida (tarmoqlararo ekranga integratsiyalangan yoki alohida):

- aniqlangan tarmoq hujumlari va anomaliyalar;
- IDPSning javob harakatlari (ulanishni bloklash, TCP sessiyani uzish, tugunni ajratish, ogohlantirish);
- IDPS qoidalari va signaturalarining yangilanishi.

8.8 Axborot xavfsizligi vositalaridan loglarni zaxiralash har oyda Axborot xavfsizligi departamenti tomonidan amalga oshiriladi. Har 6 oyda elektron arxivlash amalga oshirilishi kerak (agar xotira to‘lsa, bu muddat qisqartirilishi mumkin).

Ushbu bo‘limda keltirilgan barcha hodisalar jurnallari (loglar) kamida **1 yil** davomida saqlanishi shart.

9. Javobgarlik

9.1 Tizim va dasturiy ta’minotni yangilash uchun javobgarlik Lokal tarmoq administratori hamda Departament xodimlariga yuklatiladi.

9.2 Lokal tarmoq administratori hamda Departament xodimlari tomonidan tizim va dasturiy ta’minotni yangilash bo‘yicha talablarning bajarilishini nazorat qilish Axborot xavfsizligi administratori hamda Departament boshlig‘i tomonidan amalga oshiriladi.

9.3 Lokal tarmoq administratori hamda Departament xodimlari ushbu yo‘riqnomada nazarda tutilgan talablarning bajarmaganligi yoki lozim darajada bajarmaganligi uchun javobgardir.

9.4 Ushbu Nizomda belgilangan talablarning bajarilmasligi Universitetning ichki mehnat qoidalari va O‘zbekiston Respublikasining mehnat qonunchiligiga muvofiq intizomiy javobgarlikka tortilishga olib keladi.

Tizim va amaliy dasturlarni yangilash, hamda
ma’lumotlarni zaxiralash va tiklash to‘g‘risidagi
Nizomga ilova

1-jadval. **Zaxira nusxalanadigan ma’lumotlar**
RO‘YXATI

T/r	Zaxiralanadigan ma’lumot	Zaxiralash turlari	Zaxira nusxa yaratish davriyligi	Javobgar
1	**buxdu.uz**			
1.1	Veb-sayt ma’lumotlar bazalari, fayllar, MBBT jurnali, log-fayllar	**Arxivlash (zaxiralash)** ma’lumotlarni qayta ishlash markazi zaxira serverining alohida ma’lumotlarni saqlash tizimiga (RAID massivi) fayl nusxalari shaklida zaxiralanadi. **Zaxiralangan ma’lumotlarni saqlash joyi:** alohida ma’lumotlarni saqlash tizimi. (NAS) **Zaxiralash tizimi:** MY SQL **Zaxiralash turi:** zaxira nusxasini olish, onlayn zaxira nusxasi	Har kuni kechasi avtomat ravishda qo‘shimcha nusxa, Haftada bir marta kechasi avtomat ravishda to‘liq nusxa	Universitetning Raqamli ta’lim texnologiyalari departamenti xodimlari, Arsenal-D
2	**moodle.buxdu.uz**			
2.1	Tizimining ma’lumotlar bazalari, fayllar, server sozlamalar fayli, MBBT jurnali, log-fayllar	**Arxivlash (zaxiralash)** ma’lumotlarni qayta ishlash markazi zaxira serverining alohida ma’lumotlarni saqlash tizimiga (RAID massivi) fayl nusxalari shaklida zaxiralanadi. **Zaxiralangan ma’lumotlarni saqlash joyi:** alohida ma’lumotlarni saqlash tizimi. (NAS) **Zaxiralash tizimi:** MY SQL, PostgreSQL **Zaxiralash turi:** zaxira nusxasini olish, onlayn zaxira nusxasi	Har kuni kechasi avtomat ravishda qo‘shimcha nusxa, Haftada bir marta kechasi avtomat ravishda to‘liq nusxa	Universitetning Raqamli ta’lim texnologiyalari departamenti xodimlari
3	**hemis.buxdu.uz**			
3.1	Tizimining ma’lumotlar bazalari, fayllar, server sozlamalar fayli, MBBT jurnali, log-fayllar	**Arxivlash (zaxiralash)** ma’lumotlarni qayta ishlash markazi zaxira serverining alohida ma’lumotlarni saqlash tizimiga (RAID massivi) fayl nusxalari shaklida zaxiralanadi. **Zaxiralangan ma’lumotlarni saqlash joyi:** alohida ma’lumotlarni saqlash tizimi. (NAS)	Har kuni kechasi avtomat ravishda qo‘shimcha nusxa,	Universitetning Raqamli ta’lim texnologiyalari departamenti xodimlari

		Zaxiralash tizimi: MY SQL, PostgreSQL **Zaxiralash turi:** zaxira nusxasini olish, onlayn zaxira nusxasi	Haftada bir marta kechasi avtomat ravishda to‘liq nusxa	
4	**masofaviy.buxdu.uz**			
4.1	Tizimining ma’lumotlar bazalari, fayllar, server sozlamalar fayli, MBBT jurnali, log-fayllar	**Arxivlash (zaxiralash)** ma’lumotlarni qayta ishlash markazi zaxira serverining alohida ma’lumotlarni saqlash tizimiga (RAID massivi) fayl nusxalari shaklida zaxiralanadi. **Zaxiralangan ma’lumotlarni saqlash joyi:** alohida ma’lumotlarni saqlash tizimi. (NAS) **Zaxiralash tizimi:** MY SQL, PostgreSQL **Zaxiralash turi:** zaxira nusxasini olish, onlayn zaxira nusxasi	Har kuni kechasi avtomat ravishda qo‘shimcha nusxa, Haftada bir marta kechasi avtomat ravishda to‘liq nusxa	Universitetning Raqamli ta’lim texnologiyalari departamenti xodimlari
5	**student.buxdu.uz**			
5.1	Tizimining ma’lumotlar bazalari, fayllar, server sozlamalar fayli, MBBT jurnali, log-fayllar	**Arxivlash (zaxiralash)** ma’lumotlarni qayta ishlash markazi zaxira serverining alohida ma’lumotlarni saqlash tizimiga (RAID massivi) fayl nusxalari shaklida zaxiralanadi. **Zaxiralangan ma’lumotlarni saqlash joyi:** alohida ma’lumotlarni saqlash tizimi. (NAS) **Zaxiralash tizimi:** MY SQL, PostgreSQL **Zaxiralash turi:** zaxira nusxasini olish, onlayn zaxira nusxasi	Har kuni kechasi avtomat ravishda qo‘shimcha nusxa, Haftada bir marta kechasi avtomat ravishda to‘liq nusxa	Universitetning Raqamli ta’lim texnologiyalari departamenti xodimlari
6	**uniwork.buxdu.uz**			
6.1	Tizimining ma’lumotlar bazalari, fayllar, server sozlamalar fayli, MBBT jurnali, log-fayllar	**Arxivlash (zaxiralash)** ma’lumotlarni qayta ishlash markazi zaxira serverining alohida ma’lumotlarni saqlash tizimiga (RAID massivi) fayl nusxalari shaklida zaxiralanadi. **Zaxiralangan ma’lumotlarni saqlash joyi:** alohida ma’lumotlarni saqlash tizimi. (NAS) **Zaxiralash tizimi:** MY SQL **Zaxiralash turi:** zaxira nusxasini olish, onlayn zaxira nusxasi	Har kuni kechasi avtomat ravishda nusxa olish Haftada bir marta kechasi avtomat ravishda to‘liq nusxa	Universitetning Raqamli ta’lim texnologiyalari departamenti xodimlari
7	**citrus.buxdu.uz**			
7.1	Tizimining ma’lumotlar bazalari, fayllar, server	**Arxivlash (zaxiralash)** ma’lumotlarni qayta ishlash markazi zaxira serverining alohida ma’lumotlarni saqlash tizimiga (RAID massivi) fayl nusxalari shaklida zaxiralanadi.	Har kuni kechasi avtomat ravishda nusxa olish	Universitetning Raqamli ta’lim texnologiyalari

	sozlamalar fayli, MBBT jurnali, log-fayllar	**Zaxiralangan ma’lumotlarni saqlash joyi:** alohida ma’lumotlarni saqlash tizimi. (NAS) **Zaxiralash tizimi:** MY SQL **Zaxiralash turi:** zaxira nusxasini olish, onlayn zaxira nusxasi	Haftada bir marta kechasi avtomat ravishda to‘liq nusxa	departamenti xodimlari
8	**journal.buxdu.uz**			
8.1	Tizimining ma’lumotlar bazalari, fayllar, server sozlamalar fayli, MBBT jurnali, log-fayllar	**Arxivlash (zaxiralash)** ma’lumotlarni qayta ishlash markazi zaxira serverining alohida ma’lumotlarni saqlash tizimiga (RAID massivi) fayl nusxalari shaklida zaxiralanadi. **Zaxiralangan ma’lumotlarni saqlash joyi:** alohida ma’lumotlarni saqlash tizimi. (NAS) **Zaxiralash tizimi:** MY SQL **Zaxiralash turi:** zaxira nusxasini olish, onlayn zaxira nusxasi	Har kuni kechasi avtomat ravishda nusxa olish Haftada bir marta kechasi avtomat ravishda to‘liq nusxa	Universitetning Raqamli ta’lim texnologiyalari departamenti xodimlari
9	**srep.buxdu.uz**			
9.1	Tizimining ma’lumotlar bazalari, fayllar, server sozlamalar fayli, MBBT jurnali, log-fayllar	**Arxivlash (zaxiralash)** ma’lumotlarni qayta ishlash markazi zaxira serverining alohida ma’lumotlarni saqlash tizimiga (RAID massivi) fayl nusxalari shaklida zaxiralanadi. **Zaxiralangan ma’lumotlarni saqlash joyi:** alohida ma’lumotlarni saqlash tizimi. (NAS) **Zaxiralash tizimi:** MY SQL **Zaxiralash turi:** zaxira nusxasini olish, onlayn zaxira nusxasi	Har kuni kechasi avtomat ravishda nusxa olish Haftada bir marta kechasi avtomat ravishda to‘liq nusxa	Universitetning Raqamli ta’lim texnologiyalari departamenti xodimlari
10	**pedskills.buxdu.uz**			
10.1	Tizimining ma’lumotlar bazalari, fayllar, server sozlamalar fayli, MBBT jurnali, log-fayllar	**Arxivlash (zaxiralash)** ma’lumotlarni qayta ishlash markazi zaxira serverining alohida ma’lumotlarni saqlash tizimiga (RAID massivi) fayl nusxalari shaklida zaxiralanadi. **Zaxiralangan ma’lumotlarni saqlash joyi:** alohida ma’lumotlarni saqlash tizimi. (NAS) **Zaxiralash tizimi:** MY SQL **Zaxiralash turi:** zaxira nusxasini olish, onlayn zaxira nusxasi	Har kuni kechasi avtomat ravishda nusxa olish Haftada bir marta kechasi avtomat ravishda to‘liq nusxa	Universitetning Raqamli ta’lim texnologiyalari departamenti xodimlari
11	**Universitetning korporativ elektron pochtasi**			

11.1	Tizim ma’lumotlar bazasi, fayllar, server sozlamalar fayli, MBBT jurnali, log-fayllar	**Arxivlash (zaxiralash)** ma’lumotlarni qayta ishlash markazi zaxira serverining alohida ma’lumotlarni saqlash tizimiga (RAID massivi) fayl nusxalari shaklida zaxiralanadi. **Zaxiralangan ma’lumotlarni saqlash joyi:** alohida ma’lumotlarni saqlash tizimi. (NAS) **Zaxiralash tizimi:** MY SQL **Zaxiralash turi:** zaxira nusxasini olish, onlayn zaxira nusxasi	Har kuni kechasi avtomat ravishda qo‘shimcha nusxa, Haftada bir marta kechasi avtomat ravishda to‘liq nusxa	Universitetning Raqamli ta’lim texnologiyalari departamenti xodimlari, Arsenal-D
12	**Fayl serverlar**			
12.1	Serverning barcha ma’lumotlari, fayllar, server sozlamalar fayli va Active Directory ma’lumotlari, log-fayllar	**Arxivlash (zaxiralash)** ma’lumotlarni qayta ishlash markazi zaxira serverining alohida ma’lumotlarni saqlash tizimiga (RAID massivi) fayl nusxalari shaklida zaxiralanadi. **Zaxiralangan ma’lumotlarni saqlash joyi:** alohida ma’lumotlarni saqlash tizimi. **Zaxiralash tizimi:** Windows Server Backup **Zaxiralash turi:** to‘liq zaxira nusxasini olish, onlayn zaxiralash	Har kuni kechasi avtomat ravishda nusxa olish	Universitetning Raqamli ta’lim texnologiyalari departamenti xodimlari
13	**Ishchi stansiyalar**			
13.1	Zaxiralanmaydi			
14	**Server uskunalari**			
14.1	Zaxiralanmaydi			
15	**Ichki telefon tarmog‘i**			
15.1	Zaxiralanmaydi			
16	**Kirish chiqishni nazorat qilish tizimi**			
16.1	Tizimining ma’lumotlar bazalari, fayllar, server sozlamalar fayli, MBBT jurnali, log-fayllar	**Arxivlash (zaxiralash)** ma’lumotlarni qayta ishlash markazi zaxira serverining alohida ma’lumotlarni saqlash tizimiga (RAID massivi) fayl nusxalari shaklida zaxiralanadi. **Zaxiralangan ma’lumotlarni saqlash joyi:** alohida ma’lumotlarni saqlash tizimi. (NAS) **Zaxiralash tizimi:** MY SQL **Zaxiralash turi:** zaxira nusxasini olish, onlayn zaxira nusxasi	Har kuni kechasi avtomat ravishda nusxa olish Haftada bir marta kechasi avtomat ravishda to‘liq nusxa	Universitetning Raqamli ta’lim texnologiyalari departamenti xodimlari
17	**Videokuzatuv tizimi**			

17.1	Tizimining ma’lumotlar bazalari, fayllar, server sozlamalar fayli, MBBT jurnali, log-fayllar	**Arxivlash (zaxiralash)** ma’lumotlarni qayta ishlash markazi zaxira serverining alohida ma’lumotlarni saqlash tizimiga (RAID massivi) fayl nusxalari shaklida zaxiralanadi. **Zaxiralangan ma’lumotlarni saqlash joyi:** alohida ma’lumotlarni saqlash tizimi. (NAS) **Zaxiralash tizimi:** MY SQL **Zaxiralash turi:** zaxira nusxasini olish, onlayn zaxira nusxasi	Har kuni kechasi avtomat ravishda nusxa olish Haftada bir marta kechasi avtomat ravishda to‘liq nusxa	Universitetning Raqamli ta’lim texnologiyalari departamenti xodimlari

Universitet axborot
xavfsizligi siyosatiga 8-ilova

Parolli himoya bo‘yicha YO‘RIQNOMA

1. Umumiy qoidalar

1.1 Ushbu Yo‘riqnoma axborotlashtirish obyektlariga kirishda xodimlarning parol bilan himoyalanishi va autentifikatsiyasiga qo‘yiladigan talablarni, qoidalarini va ishlatish tartibini belgilaydi.

1.2 Ushbu Yo‘riqnoma parol bilan himoya qilishni va axborotlashtirish obyektlariga kirishning boshqa identifikatorlarini shakllantirish, boshqarish, shuningdek, ushbu obyektlarga kirish huquqiga ega bo‘lgan barcha xodimlarga nisbatan qo‘llaniladi.

2. Atamalar va ta’riflar

2.1 Ushbu Yo‘riqnomada quyidagi atamalar va ularning ta’riflari qo‘llaniladi:

autentifikatsiya – subyekt haqiqiyligini tasdiqlash;

initsializatsiya paroli – foydalanuvchiga dastlabki kirish uchun berilgan parol;

parol – foydalanuvchini tasdiqlash uchun foydalaniladigan konfidensial belgilar to‘plami;

parol bilan himoya qilish – tizimga va uning resurslariga parollar orqali kirish jarayonini boshqarish;

parol komprometatsiyasi – parolning sir saqlanmasligi, oshkor qilinishi;

qayd yozuvi – axborot tizimlari va manbalariga kirishda foydalaniladigan foydalanuvchi identifikatori.

3. Umumiy talablar

3.1 Xodimlarining quyidagi axborotlashtirish obyektlariga kirishini ta’minlash uchun parolni himoya qilish va autentifikatsiyadan foydalanish kerak:

3.1.1 Qayd yozuvi va parolga asoslangan bir faktorli autentifikatsiya:

- ish stansiyalari, lokal tarmoq, server qurilmalari, axborot xavfsizligi vositalari, tarmoq qurilmalari, korporativ elektron pochta – xodimlar, Universitetning axborot xavfsizligini ta’minlash masalalari bo‘yicha mas’ul xodimi (keyingi o‘rinlarda – Axborot xavfsizligi administratori), Raqamli ta’lim texnologiyalari departamenti boshlig‘i (keyingi o‘rinlarda – Departament boshlig‘i), Tarmoqlarni boshqarish va texnik qo‘llab-quvvatlash sektori bosh mutaxassisi (keyingi o‘rinlarda – Lokal tarmoq administratori) va Raqamli ta’lim texnologiyalari departamenti (keyingi o‘rinlarda – Departament) xodimlari tomonidan;
- Universitet axborot tizimlari – tegishli ruxsat turlariga ko‘ra Universitet xodimlari, talabalar, shuningdek, internet foydalanuvchilari tomonidan.

3.1.2 Universitetda Edo.ijro.uz va E-xat tizimdagi harakatlarini ERI yordamida tasdiqlashdagi ikki faktorli autentifikatsiyadan foydalaniladi.

3.1.3 Xodimlarni Universitet binosiga kirish-chiqishi Face ID tizimi hamda ID-karta orqali foydalaniladigan autentifikatsiya orqali nazorat qilinadi.

3.2 Keyinchalik joriy etilishi mumkin bo‘lgan axborot tizimlari uchun ikki faktorli autentifikatsiyani joriy etish Axborot xavfsizligi administratorlari hamda Bo‘lim boshlig‘i uchun ustuvor vazifa bo‘lishi kerak.

3.3 Xodimlarning parollari konfidensial ma’lumot bo‘lib, ularni oshkor qilish yoki birovga berish mumkin emas. Parol xavfsizligini ta’minlash uchun uning egasi javobgardir.

4. Parollarni xavfsiz saqlashga qo‘yilgan talablar

4.1 Shaxsiy parolini sir saqlash uchun foydalanuvchi shaxsan javobgardir. Parolni kompрometatsiya qilish, shuningdek, parolni jamoat joylarida saqlash taqiqlanadi.

4.2 Xodim o‘z parollarini qog‘ozda saqlashga faqat parol egasi tomonidan shaxsiy muhr bilan muhrlangan qutida yoki bo‘linma boshlig‘i seyfida saqlashga ruxsat etiladi.

4.3 Zarurat tug‘ilganda (xizmat safari, ta’til va boshqalar), Axborot xavfsizligi administratori tomonidan amalga oshiriladigan tekshirishda foydalanuvchi parolini talab qiladigan bo‘lsa, uning parolini oshkor qilishga ruxsat beriladi.

Parolni berish fakti foydalanuvchi tomonidan Axborot xavfsizligi administratori hamda Departament boshlig‘iga yetkazish kerak. Ishlab chiqarish yoki tekshirish ishlarining oxirida foydalanuvchilar mustaqil ravishda kompрometatsiyaga uchragan parollarni darhol majburiy ravishda o‘zgartirishlari shart.

4.4 Favqulodda vaziyatlar, shuningdek, foydalanuvchi qayd yozuvi va parollarni o‘zgartirishga texnologik ehtiyoj tug‘ilgan taqdirda tizim administratorlariga parollarni o‘zgartirishga ruxsat beriladi. Bunday hollarda parollari o‘zgartirilgan foydalanuvchilar o‘zlarining parollari o‘zgartirilganligini bilgandan so‘ng darhol yangi parol yaratishga majburdirlar.

4.5 Agar foydalanuvchi uzoq vaqt ishda bo‘lmagan taqdirda (xizmat safari, kasallik va boshqalar) uning qayd yozuvi bloklanadi, zarur hollarda ushbu foydalanuvchi resurslariga nisbatan boshqa foydalanuvchilarning kirish huquqlari o‘zgartiriladi. Universitetda Departament boshlig‘i va Lokal tarmoq administratorlariga foydalanuvchi uzoq vaqt davomida yo‘qligi to‘g‘risida xabar berilishi kerak.

4.6 Parol egalari yuqorida sanab o‘tilgan talablardan xabardor bo‘lishlari va ushbu talablarga javob bermaydigan parollardan foydalanish, shuningdek, parol ma’lumotlarini oshkor qilish mas’uliyati haqida ogohlantirishlari lozim.

4.7 Serverlar, tarmoq qurilmalari va axborotni muhofaza qilish vositalariga qo‘yilgan parollar xavfsiz joyda, yong‘inga qarshi seyfda saqlanishi kerak. Ushbu parollarga kirish Universitetda Axborot xavfsizligi administratori va Departament boshlig‘i tomonidan amalga oshiriladi.

5. Parol yaratish jarayonlarini tashkiliy va texnik jihatdan ta’minlash

5.1 Universitetda ishga yangi qabul qilingan xodimlar uchun ish stansiyalar, lokal tarmoq va elektron pochta xizmatlaridan foydalanish, shuningdek, axborot tizimlari va resurslariga kirish uchun yangi foydalanuvchi qayd yozuvi va ishga tushirish parollari yaratiladi.

5.2 Lokal tarmoq hamda korporativ elektron pochta xizmatidan foydalanish uchun yangi foydalanuvchi qayd yozuvi va boshlang‘ich parollar Universitetda Lokal tarmoq administratori va Departament xodimlari tomonidan yaratiladi tegishli domen serveriga kiritiladi.

5.3 Initsializatsiya qilingan parolni yaratishda ushbu Yo‘riqnomaning 7-bo‘limida belgilangan parollarni yaratish talablari va qoidalari bajarilishi kerak.

5.4 Ish stansiyalariga kirish uchun boshlang‘ich parol agar xodim yangi bo‘lsa, xodimning shaxsan o‘ziga taqdim etiladi. Boshqa holatlarda boshlang‘ich parol xodimning korporativ elektron pochta qutisiga yuboriladi.

6. Parollarni o‘zgartirish va bekor qilish jarayoni

6.1 Parol shakllangandan so‘ng, yangi xodim ushbu Yo‘riqnomaning 7-bo‘limida belgilangan parollarni ishlab chiqarish talablari va qoidalariga rioya qilgan holda o‘z parolini kiritishi shart.

6.2 Xodimlar ish stansiyalari va lokal tarmoqqa kirishdagi parollarini 3 (uch) oyda bir marotaba o‘zgartirishlari kerak. Ushbu talab Universitetda alohida Active Directory xizmatini sozlash orqali bajarilishi kerak.

Active Directory foydalanuvchi tomonidan vaqti-vaqti bilan parolni o‘zgartirish talablariga va Yo‘riqnomaning 7-bo‘limida belgilangan talablarga muvofiq kiritilgan parolni murakkablik talabiga javob berishi kerak.

6.3 Begona shaxslarning serverlarga, tarmoq qurilmalariga va axborotni muhofaza qilish vositalariga kirishini cheklash, ularga kirish parollari, shuningdek, ularga masofadan kirishni ta’minlaydigan ish stansiyalari, ularning ishlashi tizim va lokal tarmoq administratorlari tomonidan hamkorlikda shakllantiriladi hamda foydalaniladi.

Belgilangan parollar rejaga asosan o‘zgartirish o‘zaro kelishgan holda tizim va lokal tarmoq administratorlari tomonidan har 30 kunda bir marta amalga oshirilishi kerak.

6.4 Lokal tarmoq administratori hamda Departament xodimlari tomonidan o‘z vaqtida parollarni o‘zgartirish talabining bajarilishi Axborot xavfsizligi administratori hamda Departament boshlig‘i tomonidan nazorat qilinadi.

6.5 Mas’ul xodimlarning axborot tizimlariga kirishi parol asosida amalga oshiriladi, uning rejadagi o‘zgarishi mas’ul xodimlarning o‘zlari tomonidan 30 kun ichida kamida bir marta amalga oshiriladi. Bu talab nazorat tizimini tartibga solish va axborot tizimlariga kirishni nazorat qilish bilan ta’minlanishi lozim.

6.6 Agar parol kompрometatsiyaga uchragan deb gumon qilingan bo‘lsa, xodim darhol Universitetda Lokal tarmoq administratoriga yoki Departament xodimlaridan biriga xabar berishi shart. Rejadan tashqari parolni o‘zgartirish belgilangan xodimlar tomonidan amalga oshiriladi.

6.7 Xodimning qayd yozuvini o‘chirish orqali kirishni blokirovka qilish uning vakolatlari tugatilgan taqdirda (ishdan bo‘shatish, boshqa ishga o‘tish va h.k.) amalga oshiriladi va ushbu xodimning tizimdagi so‘nggi sessiyasi tugagandan so‘ng darhol amalga oshirilishi shart.

6.8 Barcha foydalanuvchilar uchun parollarning rejadan tashqari to‘liq o‘zgarishi Universitetda Lokal tarmoq administratori va Departament xodimlari tomonidan amalga oshiriladi.

6.9 Axborotlashtirish obyektlariga uch marotaba muvaffaqiyatsiz parol kiritilsa kirish bloklanishi kerak.

Ish stansiyasi sozlamalari, agar foydalanuvchi 5 daqiqa davomida ishchi holatida bo‘lmasa blok holatiga, 30 daqiqada uxlash rejimiga va 120 daqiqada gibernatsiya holatiga o‘tishi avtomatlashtirilgan tarzda bo‘lishi kerak.

7. Parolni yaratish talablari

7.1 Univesitetda parol generatorlari boshlang‘ich parollarni yaratish uchun texnik yordam sifatida ishlatiladi. Parol generatori sifatida “Password Generator 1.25” dasturiy ta’minotidan foydalaniladi.

7.1.1 Axborotlashtirish obyektlariga kirish uchun parollarni shakllantirishda quyidagi talablarga javob berish kerak:

- parol kamida 8 ta belgilardan iborat bo‘lishi;
- parol belgilarida katta va kichik harflar, raqamlar va maxsus belgilardan iborat bo‘lishi;
- parolda oson hisoblanadigan belgilar kombinatsiyalari (ismlar, familiyalar, tug‘ilgan kunlar va boshqalar), shuningdek, umumiy qabul qilingan qisqartmalardan iborat bo‘lmasligi;
- parolni o‘zgartirganda, yangi qiymat kamida 6 holatda avvalgisidan farq qilishi lozim.

7.2 Lokal tarmoq administratori hamda Bo‘lim xodimlarining paroli kichik va katta harflar, raqamlar va maxsus belgilar yordamida kamida 12 ta belgi bo‘lishi kerak.

7.3 Parollarni generatsiyalash va tarqatish jarayonlari Lokal tarmoq administratori va Departament xodimlari tomonidan amalga oshiriladi. Ushbu vazifalar Axborot xavfsizligi administratori tomonidan nazorat qilinadi.

8. Parollar bilan ishlashda xodimlar va mas’ul xodimlarning harakatlarini nazorat qilish

8.1 Parollar bilan ishlashda xodimlar va mas’ul xodimlarning harakatlari ustidan nazorat Axborot xavfsizligi administratori tomonidan Departament boshlig‘i bilan hamkorlikda amalga oshiriladi.

8.2 Parollar bilan ishlashda xodimlar, Lokal tarmoq administratori hamda Departament xodimlari harakatlari ustidan tashkiliy va texnik nazorat Axborot xavfsizligi administratori tomonidan har 6 oyda bir marta amalga oshiriladi.

8.3 Parollar bilan ishlashda xodimlar va mas’ul xodimlarning harakatlari ustidan nazorat quyidagilar asosida amalga oshiriladi:

- ushbu Yo‘riqnomaning 7-bo‘limiga muvofiq parollarni yaratishga qo‘yiladigan talablar;

- ushbu Yo‘riqnomaga muvofiq parollarni saqlash talablari;

- ushbu Yo‘riqnomaning 9-bo‘limiga muvofiq parol egalarining majburiyatlari.

8.4 Nazorat Active Directory xizmati sozlamalarini, axborot tizimlari va resurslarida foydalanuvchi kirishini nazorat qilish to‘g‘riligini tekshirish asosida amalga oshiriladi.

Foydalanuvchilarning parollari xavfsizligini ta’minlash uchun tasodifiy tekshirish (so‘rov, so‘rovnoma, tekshirish) amalga oshiriladi.

Axborot xavfsizligi administratori hamda Departament boshlig‘i xodimlar tomonidan kiritgan parolning murakkabligi va saqlanish holatini tekshiradi.

8.5 Ushbu Yo‘riqnoma talablari buzilgan taqdirda Axborot xavfsizligi administratori yoki Departament boshlig‘i takroran buzilishning oldini olish maqsadida tegishli xodimlarga ogohlantirish berishi shart.

Xodim tomonidan ushbu Yo‘riqnoma talablari muntazam yoki qo‘pol ravishda buzilgan taqdirda, buzg‘unchiga nisbatan tegishli choralar ko‘rish uchun Lokal tarmoq administratori va Departament xodimlari Axborot xavfsizligi administratorini va Departament boshlig‘ini xabardor qilishlari kerak.

Departament boshlig‘i universitet rahbariyatiga ushbu yo‘riqnoma talablarini qo‘pol ravishda buzgan xodimga nisbatan chora ko‘rishni so‘rab rasmiy murojaat kiritish huquqiga ega.

9. Foydalanuvchilarning vazifalari

9.1 Xodimlar quyidagilarga majbur:

- turli axborotlashtirish obyektlariga kirishda har bir qayd yozuvlari uchun turli parollarni qo‘llash;

- Lokal tarmoq administratori yoki Departament xodimlaridan biriga kirishni blokirovka qilish uchun ularning paroli buzilganligi to‘g‘risida xabar berish;

- parol xavfsizligini ta’minlash;

- begona shaxslarga va xodimlarga shaxsiy parolni oshkor qilmaslik.

9.2 Xodimlar o‘z parollarini himoya qilish bo‘yicha yetarli choralarni qo‘llashlari shart, shu jumladan:

- shaxsiy parolni yodda saqlash va boshqa xodimlarni bilmasligini ta’minlash;

- shaxsiy parolni faqatgina tarkibiy bo‘linma rahbaridan tashqari har qanday vaziyatda hech kimga bermaslik;

- paroldan foydalanganda (masalan, uni kiritish), uning buzilish ehtimolini istisno qilish uchun zarur choralarni ko‘rish (masalan, kiritilgan parolni vizual ko‘rish imkoniyatini istisno qilish).

9.3 Xodim tomonidan ishlatilgan parollardan Universitetdan tashqaridagi tizimlarda (masalan, internet-saytlarda, internet-do‘konlarda, elektron to‘lov tizimlarida va boshqalarda) foydalanish taqiqlanadi.

9.4 Lokal tarmoq administratori yoki Departament xodimlariga xodimlarning parollarini aniq matnda yoki xesh qiymatlari shaklida saqlash, shuningdek, parollarni umumiy resurslarga joylashtirish yoki tashqi elektron pochta orqali

yuborish taqiqlanadi (parollarni faqat korporativ elektron pochta orqali xodimning o‘ziga yuborishdan tashqari).

9.5 Lokal tarmoq administratori va Departament xodimlarining parollarni saqlash bo‘yicha majburiyatlari:

- xodimlarni – parollarni himoya qilish, parollarning xavfsizligini ta’minlash va parolni buzish uchun javobgar bo‘lishi to‘g‘risida ogohlantirish;
- xodimlar tomonidan parollar buzilgan taqdirda, ushbu Yo‘riqnoma talablarini buzganlik holatlari bo‘yicha Axborot xavfsizligi administratori yoki Departament boshlig‘iga zudlik bilan xabar berish.

10. Javobgarlik

10.1 Parollarni generatsiya qiladigan Lokal tarmoq administratori va Departament xodimlari ushbu Yo‘riqnomaning talablarini bajarish uchun javobgardir.

10.2 Xodimlar ushbu Yo‘riqnoma talablariga muvofiq o‘zlarining parollari xavfsizligini ta’minlash uchun javobgardir.

10.3 Ushbu Yo‘riqnomada belgilangan talablarning bajarilmasligi Universitetning ichki mehnat qoidalari va O‘zbekiston Respublikasining mehnat qonunchiligiga muvofiq intizomiy javobgarlikka tortilishga olib keladi.

Antivirus himoyasi bo‘yicha YO‘RIQNOMA

1. Umumiy qoidalar

1.1 Ushbu Yo‘riqnoma axborot-kommunikatsiya tizimlarini zararli dasturlarning xatti-harakatlaridan himoya qilishni ta’minlashni tashkil etish talablarini belgilaydi.

1.2 Ushbu Yo‘riqnoma Universitetda axborot-kommunikatsiya tizimidan foydalanuvchi barcha xodimlar uchun majburiydir.

2. Atamalar va ta’riflar

2.1 Ushbu Yo‘riqnomada quyidagi atamalar va ularning ta’riflari qo‘llaniladi:

virusga qarshi dastur – viruslarni aniqlash uchun mo‘ljallangan va ularni yo‘q qilish taklifini berishi mumkin bo‘lgan yoki yo‘q qiluvchi dastur;

zararlovchi dastur – apparat, dasturiy-apparat yoki dasturiy usulda amalga oshirilgan va biror-bir ruxsat etilmagan yoki jinoyatkorona harakatlarni bajarish uchun mo‘ljallangan dastur;

dasturiy virus, virus – boshqa dasturlarga o‘zining o‘zgartirilgan nusxalarini qo‘yish yo‘li bilan o‘z-o‘zidan ko‘payadigan, uni o‘zgartiradigan, zararlangan dasturni ochishda amalga oshadigan maxsus ishlab chiqilgan zararlovchi dastur;

antivirusni boshqarish vositasi – parametrlarni markazlashtirilgan boshqarish, antivirus vositalari va antivirus himoyasi sohasidagi intsidentlarni yangilashning avtomatlashtirilgan tizimi.

3. Umumiy talablar

3.1 Axborot xavfsizligini ta’minlash uchun Universitetda faqat litsenziyalangan antivirus vositalaridan foydalanishga ruxsat beriladi.

Ish stansiyalari va serverlarda o‘rnatilgan antivirus dasturlari uchun markazlashtirilgan boshqaruv tizimidan foydalanish kerak.

3.2 Ish stansiyalari va serverlarda o‘rnatilgan barcha antivirus dasturlarini boshqarish va yangilashni boshqarishning markazlashtirilgan tizimidan foydalanishni tashkil etish Universitetda Raqamli ta’lim texnologiyalari departamenti Tarmoqlarni boshqarish va texnik qo‘llab-quvvatlash sektori bosh mutaxassisi (keyingi o‘rinlarda – Lokal tarmoq administratori) va Raqamli ta’lim texnologiyalari departamenti (keyingi o‘rinlarda – Departament) xodimlarining ustuvor vazifalaridan biri bo‘lishi kerak.

3.3 Markazlashtirilgan antivirus tizimi Universitetning o‘z binolarida joylashgan serverlariga o‘rnatiladi. Markazlashtirilgan antivirus tizimi ish stansiyalar va serverlarda o‘rnatilgan antiviruslarning ishlashi va boshqarilishini

markazlashtirilgan nazorat qilish, shuningdek, ularning antivirus ma’lumotlar bazalarini markazlashtirilgan ravishda yangilashni ta’minlaydi.

3.4 Barcha ish stansiyalari, serverlar va tarmoq trafigi majburiy antivirus nazorati ostida bo‘ladi.

4. Antivirus muhofazasi tadbirlarini tashkil etish

4.1 Virusga qarshi tizimni boshqarish va xizmat ko‘rsatish Lokal tarmoq administratori hamda Bo‘lim xodimlari tomonidan amalga oshiriladi.

4.2 Ish stansiyalari va serverlarda antivirus vositalarini o‘rnatish va sozlash Universitetda Lokal tarmoq administratori va Departament xodimlari tomonidan amalga oshiriladi.

4.4 Agar tarmoqlararo ekran vositasi sozlamalarida trafikni boshqarish funksiyasi mavjud bo‘lsa, yoqilishi kerak.

4.5 Disklar va ish stansiyalari fayllarni antivirus bilan tekshirish har kuni avtomatik ish stansiyalarini ishga tushirishda va serverlar qayta ishga tushirilganda amalga oshirilishi kerak.

4.6 Antivirus ma’lumotlar bazasi muntazam ravishda avtomatik rejimda yangilanib turishi kerak, buni Lokal tarmoq administratori hamda Departament xodimlari antivirus dasturiy ta’minotini ishlab chiqaruvchisi yangilanish serverlariga kirishni sozlashi kerak. Agar antivirus vositalari ishlab chiqaruvchisi yangilanish serverlariga kirishni sozlash imkonsiz bo‘lsa, Lokal tarmoq administratori hamda Departament xodimlari haftada bir marta viruslar ma’lumotlar bazasini yangilash paketlarini o‘rnatishi, ularning antivirus paketiga ulanishini nazorat qilishi va ish stansiyalari va serverlarini viruslarga tekshirishi kerak.

4.7 Lokal tarmoq orqali, shuningdek, tashuvchida qabul qilingan va uzatiladigan har qanday ma’lumotlar (har qanday formatdagi matnli fayllar, ma’lumotlar va fayllar) majburiy antivirus nazoratidan o‘tishi lozim.

4.8 Tizim va amaliy dasturiy ta’minotni o‘rnatish (o‘zgartirish) Lokal tarmoq administratori hamda Departament xodimlari tomonidan Universitetning axborot xavfsizligini ta’minlash masalalari bo‘yicha mas’ul xodimi (keyingi o‘rinlarda – Axborot xavfsizligi administratori) va Departament boshlig‘i nazoratida amalga oshirilishi kerak. O‘rnatilgan (o‘zgartirilishi mumkin bo‘lgan) dasturiy ta’minot tegishliligi bo‘yicha Lokal tarmoq administratori hamda Departament xodimlari tomonidan oldindan tekshirilishi zarur. Dastur o‘rnatgandan (o‘zgartirgandan) so‘ng darhol antivirus tekshiruvi o‘tkazilishi kerak.

4.9 Xodimlarga mustaqil ravishda ish stansiyalariga dasturiy ta’minotni o‘rnatishning oldini olish uchun ularga ishchi (administrator bo‘lmagan) foydalanuvchi sifatida kirish huquqi berilishi kerak.

5. Virusdan himoya qilish ishlarining ishtirokchilariga qo‘yiladigan talablar

5.1 Ish stansiyalari va serverlarni o‘rnatilgan antivirus dasturisiz ishlatish taqiqlanadi. Antivirus dasturini doimo yangilab turish kerak.

5.2 Agar zararli dastur mavjudligiga shubha tug‘ilsa (dasturlarning noto‘g‘ri ishlashi, grafik va ovozli effektlarining paydo bo‘lishi, ma’lumotlarning buzilishi, yo‘qolgan fayllar, tizim xatosi haqidagi xabarlarning tez-tez paydo bo‘lishi), foydalanuvchining o‘zi yoki Lokal tarmoq administratori va Departament xodimlari bilan birgalikda o‘z ish stansiyasida antivirus nazoratini amalga oshirishi kerak.

5.3 Ish stansiyalarida viruslarni yuqtirgan fayllar antivirus tekshiruvi vaqtida aniqlangan bo‘lsa, xodimlar:

- ish stansiyasining ishini to‘xtatib qo‘yish;
- virusni yuqtirgan fayllar aniqlanganligi to‘g‘risida Lokal tarmoq administratoriga yoki Departament xodimlariga, shuningdek, ushbu fayllardan o‘z ishlarida foydalanadigan foydalanuvchilarni darhol xabardor qilishi shart;
- undan keyingi foydalanish tahlilini o‘tkazish;
- zararlangan fayllarni zararsizlantirish yoki yo‘q qilish;
- agar antivirus dasturi zararsizlantira olmagan yangi virus aniqlansa, virus bilan zararlangan faylni Axborot xavfsizligi administratoriga va/yoki Departament boshlig‘iga taqdim etish.

5.4 Xodimlarga ish stansiyasidan Axborot xavfsizligi administratori va Departament boshlig‘i roziligisiz quyidagilar taqiqlanadi:

- antivirus himoya vositalari sozlamalari va konfiguratsiyasini o‘zgartirish;
- virusga qarshi himoya vositalarini olib tashlash yoki tizimga qo‘shish;
- ish stansiyasida o‘rnatilgan antivirus himoyasi vositalarida tekshirmasdan turib saqlash vositalaridan foydalanish;
- elektron pochta orqali kelgan noma’lum dasturlarni ishga tushirish.

5.5 Xodimlar quyidagilarga majbur:

- noma’lum, shubhali yoki ishonchsiz manbalardan olingan elektron pochta xabarlariga qo‘shimchalarni ochmaslik. Bunday biriktirilgan fayllar tezda o‘chirilishi kerak;
- noma’lum yoki shubhali manbalardan ma’lumotlarni yuklamaslik;
- mantiqiy disklarga kirishni bekor qilish;
- noma’lum yoki shubhali manbalardan foydalanishdan oldin uni viruslardan tekshirish;
- har kuni, ish stansiyasini dastlabki yuklashda, xodim antivirus monitor mavjudligiga ishonch hosil qilish va agar mavjud bo‘lmasa, Lokal tarmoq administratorini yoki Departament xodimlarini xabardor qilish;
- Lokal tarmoq administratori yoki Departament xodimlaridan tizimda virus mavjudligi to‘g‘risida, shuningdek, virusga shubha tug‘ilganda xabarnoma olingandan so‘ng, ish stansiyasini rejadan tashqari antivirus tekshiruvini mustaqil ravishda amalga oshirish.

6. Virusdan himoya qilish ishlarida ishtirokchilarning javobgarligi

6.1 Lokal tarmoq administratori hamda Departament xodimlari ushbu Yo‘riqnomaning talablariga muvofiq virusga qarshi nazoratni tashkil etish uchun javobgardir.

6.2 Ushbu Yo‘riqnomaning talablariga rioya qilish uchun javobgarlik barcha mas’ul xodimlarga yuklatilgan.

6.3 Virusga qarshi himoya holatini, shuningdek, virusga qarshi kurashning belgilangan tartibiga rioya etilishini va xodimlar tomonidan ushbu Yo‘riqnoma talablariga rioya qilinishini vaqti-vaqti bilan monitoring qilish Axborot xavfsizligi administratori hamda Departament boshlig‘i tomonidan amalga oshiriladi.

6.4 Ushbu Yo‘riqnomada belgilangan talablarning bajarilmasligi Universitetning ichki mehnat qoidalari va O‘zbekiston Respublikasining mehnat qonunchiligiga muvofiq intizomiy javobgarlikka tortilishga olib keladi.

Mobil, ma’lumot saqlovchi va tashuvchi qurilmalar bilan ishlashda axborot xavfsizligini ta’minlash bo‘yicha YO‘RIQNOMA

1. Umumiy qoidalar

1.1 Ushbu Yo‘riqnoma Universitetda foydalaniladigan axborot tashuvchi vositalar, mobil qurilmalar, ma’lumotlarni saqlash moslamalari bilan ishlashda axborot xavfsizligini ta’minlash talablari va tartiblarini belgilaydi.

1.2 Axborot-kommunikatsiya tizimlarida, ish stansiyalari va lokal tarmoqda ma’lumotlarni qayta ishlash, qabul qilish, uzatish maqsadida mobil qurilmalar va qo‘shimcha ma’lumotlarni saqlovchi va tashuvchi tashqi qurilmalar foydalanishni anglatadi.

1.3 Foydalaniladigan axborot tashuvchi vositalar, mobil qurilmalar sifatida USB flesh-xotiralar, qattiq disklar va noutbuklardan (keyingi o‘rinlarda – Mobil qurilmalar) foydalaniladi.

2. Atamalar va ta’riflar

2.1 Ushbu Yo‘riqnomada quyidagi atamalar va ularning ta’riflari qo‘llaniladi:

2.1.1 **zararlovchi dastur** – apparat, dasturiy-apparat yoki dasturiy usulda amalga oshirilgan va biror-bir ruxsat etilmagan yoki jinoyatkorona harakatlarni bajarish uchun mo‘ljallangan dastur.

2.1.2 **nazorat qilinadigan hudud** – doimiy yoki bir martalik ruxsati bo‘lmagan begona shaxslar va transport vositalarining nazoratsiz bo‘lishi taqiqlangan joy (hudud, bino, binoning bir qismi).

Izoh – Nazorat qilinadigan hududning chegaralari quyidagilar bo‘lishi mumkin:

- tashkilotning nazorat qilinadigan hududi perimetri;
- himoyalanadigan bino yoki binoning himoyalanadigan qismini o‘rab olish konstruksiyalari, agar u himoya qilinmaydigan hududda joylashgan bo‘lsa.

2.1.3 **mobil qurilmalar** – smartfonlar, planshetlar, elektron kitoblar, telefonlar, shaxsiy raqamli yordamchilar, operatsion tizimga ega netbuklar va mobil tarmoqlarga, Wi-Fi va internetga ulanish imkonini beradigan mobil ilovalar, shuningdek, ish stansiyalari va boshqa shunga o‘xshash qurilmalar.

2.1.4 **ma’lumotlarni saqlash qurilmasi** – ma’lumotni zaxiralash va saqlash, shuningdek, uni tashish uchun foydalaniladigan ma’lumotni o‘qiydigan yoki yozadigan qurilma.

2.1.5 **ma’lumotlarni tashish qurilmasi** – oflayn rejimida saqlash uchun mo‘ljallangan qurilma. Ular quyidagi shaklda bo‘lishi mumkin: qattiq disklar (HDD), flesh-xotira (USB flash), optik lazer disklari (CD, DVD), disketalar.

3. Qo‘llash qoidalari va talablar

3.1 Universitetda xodimlarga tegishli bo‘lgan tashuvchi, saqlovchi va Mobil qurilmalardan foydalanish quyidagi hollarda taqiqlanadi:

- konfidensial muzokaralar va konfidensial xarakterdagi tadbirlar o‘tkaziladigan xonalarda;
- lokal tarmoq va axborot resurslariga ulanish uchun;
- masofadan foydalanuvchilarning Mobil qurilmalarini umumiy foydalanishdagi telekommunikatsiya tarmog‘i va internet orqali axborot resursiga va lokal tarmoqqa ulash;
- konfidensial yoki boshqa himoyalangan ma’lumotlarni, shu jumladan parollarni va boshqalarni tashuvchilar sifatida foydalanish.

3.2 Universitet hududida bir martalik ruxsatnomasi bo‘lgan uchinchi shaxslar tomonidan Mobil qurilmalardan foydalanishni taqiqlash choralari ko‘rilishi mumkin.

3.3 Universitet binolaridagi axborot-kommunikatsiya tizimida faqat Universitetning mulki bo‘lgan va ro‘yxatdan o‘tgan Mobil qurilmalar, ma’lumotlarni saqlovchi va tashuvchi tashqi qurilmalardan foydalanishga ruxsat beriladi.

Ma’lumotlarni tashuvchi, saqlovchi va mobil qurilmalarni qayd qilish jurnali Universitetning axborot xavfsizligini ta’minlash masalalari bo‘yicha mas’ul xodimi (keyingi o‘rinlarda – Axborot xavfsizligi administratori) tomonidan yuritiladi.

3.4 Hisobga olingan Mobil qurilmalarni haftasiga kamida bir marta virusga qarshi vositalar tomonidan zararli dastur bor-yo‘qligini aniqlash maqsadida tekshirib turilishi kerak.

3.5 Universitetda konfidensial ma’lumotlarni saqlash uchun Mobil qurilmalardan foydalanish taqiqlanadi.

3.6 Mobil qurilmalardan Universitetning axborot tizimlari va resurslariga ulanish uchun faqat boshqariladigan hudud doirasida foydalanish mumkin. Bunday holda, ularga qo‘yiladigan talablar ish stansiyalari bilan bir xil.

3.7 Mobil qurilmalar va ma’lumotlarni saqlovchi va tashuvchi tashqi qurilmalardan foydalanish vaqtida Universitet xodimlari quyidagi talablarni bajarishlari kerak:

- ulardan belgilangan maqsadlarda va faqat xizmat vazifalarini bajarishda foydalanish;
- ushbu Yo‘riqnomaning talablari buzilganligi ma’lum bo‘lsa, Raqamli ta’lim texnologiyalari departament boshlig‘i (keyingi o‘rinlarda – Departament boshlig‘i) va Axborot xavfsizligi administratoriga darhol xabar berish;
- Axborot xavfsizligi administratori va Departament boshlig‘iga Mobil qurilmalar, ma’lumotlarni saqlovchi va tashuvchi tashqi qurilmalarning yo‘qolishi (o‘g‘irlanishi) to‘g‘risida tezkorlikda xabar berish;
- Mobil qurilmalar, ma’lumotlarni saqlovchi va tashuvchi tashqi qurilmalarni jismoniy xavfsizligini har qanday oqilona usulda ta’minlash;
- Mobil qurilmalar va ma’lumotlarni saqlovchi va tashuvchi tashqi qurilmalarni boshqa shaxslarga bermaslik.

3.8 Hisobga olingan Mobil qurilmalar, ma’lumotlarni saqlovchi va tashuvchi tashqi qurilmalar mas’ul xodimlar tomonidan qarovsiz qoldirilishi taqiqlanadi.

3.9 Universitet hududidan tashqarida (xizmat safarlari, uchrashuvlar, muzokaralar va boshqalar) ishlatilganda Mobil qurilmalarning axborot va jismoniy xavfsizligini ta’minlash uchun quyidagi choralar qo‘llanilishi kerak:

- Mobil qurilmaga kirishda foydalanuvchi biometrik ma’lumotlari asosida kirish parolini o‘rnatish yoki autentifikatsiya vositalaridan foydalanish;
- Mobil qurilmaning ma’lum dasturlariga kirish uchun parolni o‘rnatish;
- Mobil qurilmada virusga qarshi himoya va shaxsiy tarmoqlararo ekranidan foydalanish.

4. Axborot tashuvchi vositalardan foydalanish qoidalari va talablari

4.1 Axborot tashuvchi vositalaridan foydalanish

4.1.1 Universitetning axborot infratuzilmasida faqat Universitetning mulki bo‘lgan va nazoratga olinadigan, ro‘yxatdan o‘tgan axborot tashuvchi vositalaridan foydalanishga ruxsat beriladi.

4.1.2 Axborot tashuvchi vositalar vaqti-vaqti bilan haftasiga kamida bir marta virusga qarshi dasturlar yordamida zararli dasturlarni tekshirilishi kerak.

4.1.3 Axborot tashuvchi vositalarni boshqariladigan hududdan olib chiqish Universitetning axborot-kommunikatsiya texnologiyalarini joriy etish va raqamlashtirish bo‘yicha mas’ul rahbari (keyingi o‘rinlarda – Mas’ul rahbar) hamda Departament boshlig‘i ruxsati bilan amalga oshiriladi.

Axborot tashuvchi qurilmalarni olib chiqish uchun ruxsatnomada quyidagilar ko‘rsatilishi kerak:

- qurilmadan foydalanadigan xodimning to‘liq F.I.Sh va lavozimi;
- qurilmaning modeli va qayd raqami;
- olib chiqish sababi (xizmat safarlar, uchrashuvlar, muzokaralar va boshqalar);
- ruxsatnomaning amal qilish muddati.

4.2 Konfidensial ma’lumotlarni saqlash uchun ishlatiladigan ma’lumotlarni saqlovchi tashqi qurilmalarni boshqariladigan hududdan tashqariga olib chiqishga yo‘l qo‘yilmaydi.

4.3 Mobil qurilmalardan foydalanish

4.3.1 Universitetda faqat Universitet mulki bo‘lgan va muntazam audit va nazorat ostida bo‘lgan Mobil qurilmalardan foydalanishga ruxsat beriladi.

4.3.2 Xodimlarga Mobil qurilmalardan foydalanishda faqat o‘z xizmat vazifalarini bajarish uchun ruxsat etiladi.

4.3.3 Mobil qurilmalar xodimlarga tarkibiy bo‘linmalar rahbarlarining tashabbusi bilan quyidagi hollarda beriladi:

- xodimning o‘z xizmat vazifalarini bajarish zarurati;
- xodim uchun ishlab chiqarish ehtiyojining paydo bo‘lishi.

4.3.4 Mobil qurilmalarning jismoniy xavfsizligini ta’minlash mobil qurilma foydalanuvchisiga yuklatiladi.

4.4 Konfidensial ma’lumotlarni saqlash uchun ishlatiladigan ma’lumotlarni tashuvchi, saqlovchi va mobil qurilmalarni boshqariladigan hududdan tashqariga ruxsatsiz olib chiqishga yo‘l qo‘yilmaydi.

Universitetning mulki bo‘lgan va ro‘yxatga olingan (nazorat qilinadigan) mobil qurilmalar, ma’lumotlarni saqlovchi va tashuvchi tashqi qurilmalarni harakatini (ro‘yxatga olish, xodimga biriktirish (ayrim hollarda qayta biriktirish, foydalanishdan chiqarish, tarkibini ishonchli tozalash, foydalanishdan chiqarish va yo‘q qilish) nazorat qilish Departament xodimlari tomonidan olib boriladi.

Mobil qurilmalar, ma’lumot saqlovchi va tashuvchi qurilmalarni harakatini nazorat qilish uchun lozim bo‘lgan “Universitet hududiga mobil qurilmalar, ma’lumot saqlovchi va tashuvchi qurilmalarni (ma’lumot to‘plagichlar, noutbuk va h.k.) olib kirish yoki hududdan olib chiqish uchun ruxsat berishga bildirgi” shakli 1-ilovaga muvofiq, “Mobil qurilmalar, ma’lumot saqlovchi va tashuvchi qurilmalarni yo‘q qilinganligi to‘g‘risidagi dalolatnoma” shakli 2-ilovaga muvofiq, “Mobil qurilmalar, ma’lumot saqlovchi va tashuvchi qurilmalarni hisobga olish jurnali” shakli 3-ilovaga muvofiq, “Konfidensial ma’lumotlar tashuvchilaridagi ma’lumotlarni yo‘q qilish bo‘yicha operatsiyalarni hisobga olish jurnali” shakli 4-ilovaga muvofiq keltirilgan.

Ish faoliyati bilan bog‘liq zarurat tufayli Mobil qurilmalar, ma’lumot saqlovchi va tashuvchi qurilmalarni harakati uchun ruxsat berish Mas’ul rahbarning yozma ruxsati bilan amalga oshiriladi.

4.5 Alohida grifli ma’lumotlarni tashuvchi, saqlovchi qurilmalarni ro‘yxatga olish, saqlash, foydalanish, bekor qilish hamda yo‘q qilish Universitetning Birinchi bo‘limi bosh mutaxassisi tomonidan Vakolatli organ talablari asosida amalga oshiriladi.

4.6 Konfidensial ma’lumotlarni saqlash uchun ishlatiladigan ma’lumotlarni tashuvchi, saqlovchi va mobil qurilmalar tegishliligi bo‘yicha Universitet logotipi va nomi bilan belgilab qo‘yiladi.

4.7 Konfidensial ma’lumotlarni saqlash uchun ishlatiladigan ma’lumotlarni tashuvchi, saqlovchi va Mobil qurilmalar Axborot xavfsizligi administratori hamda Departament boshlig‘i tomonidan inventarizatsiya qilinadi.

Axborot tashuvchisi va ularda markirovkaning mavjudligini tekshirish Axborot xavfsizligi administratori tomonidan Universitetda yiliga kamida bir marta amalga oshiriladi.

4.8 Universitet xodimlari axborot tashuvchi, saqlovchi va Mobil qurilmalardan foydalanishda quyidagi talablarga rioya qilishlari shart:

- vositalardan faqat o‘zlarining ish faoliyatiga oid vazifalarini bajarish uchun foydalanishi;
- Axborot xavfsizligi administratoriga va Departament boshlig‘iga ushbu Yo‘riqnoma talablarining buzilishining har qanday faktlari to‘g‘risida xabar berish;
- ma’lumotlarni tashuvchi, saqlovchi va Mobil qurilmalarni yo‘qotish (o‘g‘irlash) yoki ishlamay qolish faktlari to‘g‘risida Axborot xavfsizligi administratori va Departament boshlig‘iga xabar berish;
- axborot tashuvchi, saqlovchi va Mobil qurilmalarni jismoniy xavfsizligini barcha oqilona usullar bilan ta’minlash;

- axborot tashuvchi, saqlovchi va Mobil qurilmalarni boshqa shaxslarga bermaslik.

4.9 Axborot tashuvchi, saqlovchi va Mobil qurilmalarni vositalardan foydalanishda xodimlarga ularni xavfsizligini ta’minlash choralari ko‘rilmagan bo‘lsa, ularni qarovsiz qoldirish taqiqlanadi.

4.10 Agar ish stansiyani yoki serverni uchinchi shaxslar ta’mirlashni talab qilsa, ta’mirlashni boshlashdan oldin ma’lumotlarni tashuvchi, saqlovchi va Mobil qurilmalar ma’lumotlardan tozalanishi kerak. Ushbu ta’mirlash ishlari Universitetning Raqamli ta’lim texnologiyalari departamenti Tarmoqlarni boshqarish va texnik qo‘llab-quvvatlash sektori bosh mutaxassisi (keyingi o‘rinlarda – Lokal tarmoq administratori) va Departament xodimlari tomonidan nazorat qilinadi.

5. Axborot tashuvchi vositalarni hisobdan chiqarish va yo‘q qilish tartibi

5.1 Agar xodim ishdan bo‘shatilgan yoki boshqa ish joyiga o‘tkazilgan bo‘lsa, unga berilgan Universitetga tegishli bo‘lgan tashuvchi, saqlovchi va Mobil qurilmalar Universitetning Axborot xavfsizligi administratoriga va Departament boshlig‘iga topshirilishi shart.

5.2 Ishlamay qolgan yoki yo‘q qilishga mo‘ljallangan tashuvchi, saqlovchi va Mobil qurilmalar qulflanadigan metall shkaflarda (seyflarda) saqlanishi kerak.

5.3 Axborot tashuvchi vositalarni hisobdan chiqarish va yo‘q qilish bilan bog‘liq masalalarni ko‘rib chiqish uchun maxsus komissiya tuziladi (keyingi o‘rinlarda – Komissiya). Komissiya tarkibi kamida 3 (uch) kishidan iborat bo‘ladi.

Komissiya tarkibi Universitetda Axborot xavfsizligi administratori hamda Departament boshlig‘i tomonidan shakllantiriladi va Rektor buyrug‘i bilan tasdiqlanadi. Mas’ul rahbar Komissiya raisi hisoblanadi.

5.4 Komissiyaning axborot tashuvchi, saqlovchi va Mobil qurilmalardan foydalanishni bekor qilish to‘g‘risidagi qarori qabul qilinganidan so‘ng, ularni yo‘q qilinganligi to‘g‘risida dalolatnoma tuzish orqali amalga oshiriladi.

Universitetga tegishli ma’lumot saqlovchi va tashuvchi qurilmani yo‘q qilinganligi to‘g‘risida tuziladigan dalolatnoma shakli Yo‘riqnomaning 3-ilovasida keltirilgan.

5.5 Foydalanish uchun yaroqsiz bo‘lgan tashuvchi, saqlovchi va Mobil qurilmalarni formatlash va ularni jismoniy yo‘q qilish orqali tozalanishi kerak.

5.6 Konfidensial ma’lumotga ega bo‘lmagan tashuvchi, saqlovchi va Mobil qurilmalarni boshqa xodimga berishdan oldin ushbu qurilmalarda saqlanadigan barcha ma’lumotlarni uni formatlash orqali o‘chirib yo‘q qilinishi kerak.

5.7 Agar ma’lumotlarni tashuvchi, saqlovchi va Mobil qurilmalardan konfidensial ma’lumotlardan tozalash zarur bo‘lsa, axborotni kafolatlangan yo‘q qilish vositalaridan foydalanish va ushbu vositalarga ega bo‘lgan ixtisoslashtirilgan tashkilotlarning xizmatlariga murojaat qilish mumkin.

6. Javobgarlik

6.1 Ushbu Yo‘riqnoma talablarini buzganlik uchun Universitetning barcha xodimlari shaxsan javobgardirlar.

6.2 Ushbu Yo‘riqnomada belgilangan tashuvchi, saqlovchi va Mobil qurilmalardan foydalanish qoidalarini buzish Universitetning ichki mehnat qoidalari va O‘zbekiston Respublikasining mehnat qonunchiligiga muvofiq intizomiy javobgarlikka tortishga sabab bo‘ladi.

6.3 Axborot xavfsizligi administratori hamda Departament boshlig‘i Universitet xodimlari tomonidan ushbu Yo‘riqnoma talablarini bajarilishini nazorat qilinishi va ta’minlanishi uchun javobgardir.

Mobil qurilmalar, ma’lumot saqlovchi va tashuvchi qurilmalar bilan ishlashda axborot xavfsizligini ta’minlash bo‘yicha yo‘riqnomaga 1–ilova

Universitet binolariga mobil qurilma, ko‘chma ma’lumot tashish vositasini olib kirish, olib chiqish uchun xodimga ruxsat berish TALABNOMASI

Ish faoliyatidagi mavjud ehtiyojdan kelib chiqib, quyidagi xodimga mobil qurilma, ko‘chma ma’lumot tashish vositasini olib kirish, olib chiqish uchun ruxsat berishingizni so‘rayman:

_____,
to‘liq F.I.SH

_____ _____
(lavozimi) (bo‘limning nomi)

Tel.raqami_____,

_____
(mobil qurilma ko‘chma ma’lumot tashish vositasining nomi)

Bo‘linma rahbari: _____
tarkibiy bo‘linmaning nomi

20___-yil “ ” to‘liq F.I.SH

Kelishildi:

Raqamli ta’lim texnologiyalari departamenti boshlig‘i _____ _____
Imzo to‘liq F.I.SH

Axborot xavfsizligini ta’minlash masalalari bo‘yicha mas’ul _____ _____
Imzo to‘liq F.I.SH

Bino komendanti _____ _____
Imzo to‘liq F.I.SH

Mobil qurilmalar, ma’lumot saqlovchi va tashuvchi qurilmalar bilan ishlashda axborot xavfsizligini ta’minlash bo‘yicha yo‘riqnomaga 2–ilova

Yo‘q qilishga ruxsat beraman

_____ rahbari

_____

(lavozimi, unvoni, F.I.Sh.)

_____

20____ yil “___” _____

_____-sonli
Mobil qurilmalar, ma’lumot saqlovchi va tashuvchi qurilmalarni yo‘q qilinganligi to‘g‘risidagi
DALOLATNOMA

_____

(lavozimi, unvoni, F.I.Sh.)

_____

_____ tarkibidagi komissiya

_____ ga asos, yo‘q qilish uchun quyidagi axborot tashuvchi vositasini tanlab oldi:

T/R	Ro‘yxatga olish raqami	Konfidensiallik belgisi	Mobil qurilmalar, ma’lumot saqlovchi va tashuvchi qurilmalar	Tashuvchi turi	Tashuvchini yo‘q qilish bo‘yicha amalga oshirilgan harakat	Izoh

Jami bo‘lib ____ _____ axborot tashuvchi vositalari
(soni, yozuv bilan)
yo‘q qilindi.

Komissiya a’zolari: _____ _____
(imzo) (F.I.Sh.)

_____ _____
(imzo) (F.I.Sh.)

Mobil qurilmalar, ma’lumotlarni saqlovchi va tashuvchi tashqi qurilmalar bilan ishlashda axborot xavfsizligini ta’minlash bo‘yicha yo‘riqnomaga 3-ilova

Mobil qurilmalar, ma’lumot saqlovchi va tashuvchi qurilmalarni hisobga olish jurnali shakli

T/r	Sana	Ma’lumot tashuvchi, saqlovchi va mobil qurilmalarning xotira hajmi, nomi va seriya raqami	Ma’lumot tashuvchi, saqlovchi va mobil qurilmalarni qabul qilganlik haqida qaydnoma (qabul qiluvchi imzosi)	Ma’lumot tashuvchi, saqlovchi va mobil qurilmalarning topshirilganligi to‘g‘risidagi qaydnoma (oluvchining imzosi)	Ma’lumot tashuvchi, saqlovchi va mobil qurilmalarni saqlash joyi (seyf, shkaf, javon raqami)	Ma’lumot tashuvchi, saqlovchi va mobil qurilmalarni yo‘q qilish to‘g‘risidagi ma’lumot (administratorlarning imzosi, sanasi)	Izoh
1.							
2.							
3.							
4.							
5.							

Mobil qurilmalar, ma’lumotlarni saqlovchi va tashuvchi tashqi qurilmalar bilan ishlashda axborot xavfsizligini ta’minlash bo‘yicha yo‘riqnomaga 4-ilova

Konfidensial ma’lumotlar tashuvchilaridagi ma’lumotlarni yo‘q qilish bo‘yicha operatsiyalarni hisobga olish jurnali shakli

T/r	Xat raqami	Ma’lumotlar (model, o‘lcham, qattiq disk s/n)	Yo‘q qilinganligi sanasi	DBAN (versiyasi, o‘chirish algoritmi)	Mas’ul shaxslarning ismlari	imzo
1.						
2.						
3.						
4.						
5.						

Universitet axborot
xavfsizligi siyosatiga 11-ilova

Axborot manbalariga kirish matritsasini ishlab chiqish QOIDALARI

1. Umumiy qoidalar

1.1 Ushbu Qoidalar Universitetning axborot tizimlari va resurslariga kirish matritsasini ishlab chiqish tartibini tavsiflaydi.

1.2 Ushbu Qoidalarning talablari Universitetga tegishli axborot tizimlari va resurslari uchun majburiydir.

1.3 Axborot tizimlari va resurslariga kirish matritsasi, Universitet faoliyatining asosiy qismi bo‘lib, axborot tizimlari va resurslarining xavfsizligini ta’minlashda muhim ahamiyatga ega. Matritsa, kim qanday axborot tizimlari va resurslariga, qanday shartlarda va qanday maqsadlar uchun kirishi mumkinligini belgilaydi.

1.4 Axborot tizimlari va resurslaridan foydalanishni cheklash qoidalari (foydalanish siyosati) kirish matritsasida shakllantirilgan bo‘lib, unda qaysi subyektlarga (subyektlar guruhlariga), qaysi obyektlarga (obyektlar guruhlariga) kirish huquqlariga (o‘qish, yozish, ijro etish va boshqalar) ruxsat berilgan yoki taqiqlanganligini belgilaydi.

1.5 Kirish matritsasi Universitetning axborot tizimlari va resurslaridan foydalanish huquqini qo‘lga kiritgan xodimlar toifasini hamda ularning ma’lumotlarga kirish va ishlov berish huquqlari va vakolatlarini belgilaydi. Shuningdek, Universitetning xodimi bo‘lmagan, ammo axborot tizimidan yoki axborot resursidan foydalanishga huquqiga ega bo‘lgan shaxslar kiradi.

Kirish matritsasi asosida foydalanuvchining axborot tizimlari va resurslaridan foydalanishi boshqariladi.

Foydalanuvchilar toifalari – bu xodimlarning birlashtirilgan guruhi bo‘lib funksional majburiyatlari, faoliyat turi, bajarilgan ishlari, lavozimi va boshqalar kiradi.

1.6 Kirish matritsasi Universitetning Raqamli ta’lim texnologiyalari departamenti Tarmoqlarni boshqarish va texnik qo‘llab-quvvatlash sektori bosh mutaxassisi (keyingi o‘rinlarda – Lokal tarmoq administratori) hamda Raqamli ta’lim texnologiyalari departamenti (keyingi o‘rinlarda – Departament) xodimlari tomonidan taqdim etilgan identifikatorlar asosida Universitetning axborot xavfsizligini ta’minlash masalalari bo‘yicha mas’ul xodimi (keyingi o‘rinlarda – Axborot xavfsizligi administratori) va Departament boshlig‘i tomonidan ishlab chiqiladi va amalga oshirilishi tashkil qilinadi.

2. Atamalar va ta’riflar

2.1 Ushbu Qoidalarda quyidagi atamalar va ularning ta’riflari qo‘llaniladi:

2.1.1 **kirish matritsasi** – foydalanishni boshqarish huquqlarini ko‘rsatadigan jadval;

2.1.2 **kirish huquqi** – obyektga uning vakolati doirasida kirish huquqini beradigan ruxsat.

2.1.3 **hujjatlashtirilgan axborot** – identifikatsiya qilish imkonini beradigan rekvizitlarga ega moddiy tashuvchida qayd etilgan axborot;

3. Kirish matritsasini ishlab chiqish uchun talablar

3.1 Axborot tizimlari va resurslariga kirmaydigan boshqa axborot resurslariga (fayllar, papkalar, qurilmalar, xizmatlar va alohida ma’lumotlar bazalariga) kirish matritsasi xodimlarning kirish darajasidan kelib chiqqan holda Axborot xavfsizligi administratori va Departament boshlig‘i tomonidan ishlab chiqiladi.

3.2 Axborot xavfsizligi administratori kirish matritsasida ko‘rsatilgan axborot tizimlari va resurslari ro‘yxatini yuritishi kerak.

Ko‘rsatilgan axborot tizimlari va resurslariga kirish matritsasi Universitetda Active Directory va boshqa tarmoqqa kirishni boshqarish xizmatlari orqali ta’minlanadi.

3.3 Axborot tizimlari va resurslaridan foydalanish matritsasini ishlab chiqish quyidagi tartibda amalga oshiriladi:

- Universitetdagi barcha mavjud axborot tizimlari va resurslar ro‘yxati shakllantiriladi. Bularga fayllar, papkalar, qurilmalar, axborot tizimlari va ularning ma’lumotlar bazalari, fayl serverlar, bulutli saqlash va boshqa ma’lumotlar omborlari kiradi;

- axborot tizimlari va resurslaridagi axborotlarning sezgirligi va ahamiyatiga qarab tegishli toifalarga ajratiladi. Bu axborot tizimlari va resurslariga kirish darajasini aniqlashga yordam beradi;

- har bir axborot tizimi va resursi uchun unga kirish huquqiga ega foydalanuvchilarning ro‘yxati tuziladi;

- foydalanuvchilarning ro‘yxati xodimlarning egallab turgan lavozimi, funksional majburiyatlari va vakolatlarini hisobga olgan holda, ularning kirish huquqlarini ko‘rsatgan holda foydalanuvchilar toifalariga bo‘linadi;

- axborotlarning toifalari va foydalanuvchilari rollariga mos keladigan turli kirish darajalari yoki ruxsatlar aniqlanadi;

- axborot tizimlari va resurslarining himoyalanganligini va kutilmagan hodisalar yoki favqulodda vaziyatlar sodir bo‘lganda foydalanish imkoniyatini ta’minlash uchun falokatlarni tiklash rejasi ishlab chiqiladi;

- ruxsat berish tartib-taomillarini amalga oshiriladi. Individual axborot tizimlari va resurslar uchun kirish matritsasi ularga berilgan huquqlarga muvofiq ma’lum bir foydalanuvchi uchun axborot tizimlari va resurslariga kirish jadvalini (belgilangan vaqt orasida axborot manbasiga kirish) ko‘rsatishi mumkin.

3.4 Axborot tizimlari va resurslaridan foydalanuvchilarga quyidagi huquqlar va vakolatlar berilishi mumkin:

- Read (R) – obyektdan ma’lumot olish;
- Write (W) – obyektdagi ma’lumotlarni yangilash;
- Append (A) – obyektga yangi ma’lumotlar qo‘shish;
- Execute (E) – obyektni bajariladigan kod sifatida talqin qilish;

- Delete (D) – obyektni o‘chirish;
- Get info (G) – obyekt haqida ma’lumot olish;
- Set info (S) – obyekt haqida ma’lumot o‘rnatish;
- Privilege (P) – obyektga kirish huquqlarini sozlash;
- Full (F) – obyektga nisbatan barcha huquqlar berilgan;
- (—) – obyektga nisbatan hech qanday huquq berilmagan.

3.5 Kirish matritsasini ishlab chiqishda quyidagi talablarni hisobga olish kerak:

- “Need-to-Know” (Bilish kerak) tamoyiliga ko‘ra foydalanuvchilarga faqat o‘z vazifalarini samarali bajarishlari uchun zarur bo‘lgan ma’lumotlargagina kirish huquqi berish;
- foydalanuvchilarga axborot tizimlari va resurslarida o‘z vazifalarini bajarish uchun kerak bo‘ladigan eng past darajadagi ruxsatlarni berish;
- muayyan sharoitlarda qo‘llaniladigan majburiy va tavsiya etilgan qoidalar o‘rtasidagi farqlar;
- “Taqiqlanmaguncha hamma narsaga ruxsat beriladi” degan zaif tamoyil asosida emas, balki “Hamma narsaga aniq ruxsat berilmaguncha umuman taqiqlanishi kerak” mazmundagi tamoyilga asoslanib qoidalarni shakllantirish;
- axborotni qayta ishlash vositalari tomonidan avtomatik ravishda hosil qilinadigan va foydalanuvchilarning ixtiyoriga binoan boshlangan ma’lumotlarning konfidensiallik darajasidagi o‘zgarishlar;
- axborot tizimi tomonidan avtomatik ravishda o‘rnatiladigan va tizim administrator tomonidan belgilanadigan foydalanuvchi huquqlarining o‘zgarishi;
- kuchga kirgunga qadar maxsus tasdiqlashni talab qiladigan va talab qilmaydigan qoidalar.

3.6 Kirish matritsasi asosida xodimlarga berilgan huquqlar va rollar to‘g‘risida axborot tizimlari va resurslariga kirishni farqlash tizimlari amalga oshiriladi.

3.7 Axborot tizimlari va resurslariga kirishda axborotni qayta ishlashning yangi vositalaridan foydalanishga ruxsat olish uchun quyidagi choralarni ko‘rish kerak:

- axborot tizimlari va resurslariga kirishda axborotni qayta ishlashning yangi vositalarini joriy etish Universitetning axborot-kommunikatsiya texnologiyalarini joriy etish va raqamlashtirish bo‘yicha mas’ul rahbari (keyingi o‘rinlarda – Mas’ul rahbar) tomonidan ma’qullangan bo‘lishi;
- joriy etilgunga qadar dasturiy ta’minotni tizimning boshqa tarkibiy qismlari bilan mosligini sinab ko‘rish;
- ish joyida axborotni qayta ishlash uchun shaxsiy texnik vositalardan (masalan, noutbuklar, uy kompyuterlari va boshqalar) foydalanishni taqiqlash.

3.8 Universitetning asosiy axborot tizimlari va resurslariga kirish matritsasi ushbu Qoidalarning ilovasida keltirilgan.

4. Javobgarlik

4.1 Kirish matritsasini ishlab chiqish uchun Axborot xavfsizligi administratori, amalga oshirish uchun esa Lokal tarmoq administratori hamda Departamentning barcha xodimlari javobgardir.

Axborot manbalariga kirish matritsasini
ishlab chiqish qoidalariga ilova

Universitetning asosiy axborot tizimlari va resurslariga kirish MATRITSASI

Bo‘linma nomi va mas’ul xodim lavozimi		buxdu.uz	moodle.buxdu.uz	hemis.buxdu.uz	masofaviy.buxdu.uz	student.buxdu.uz	uniwork.buxdu.uz	citrus.buxdu.uz	journal.buxdu.uz	srep.buxdu.uz	pedskills.buxdu.uz	Korporativ elektron pochta	Fayl serverlar	Ishchi stansiyalar	Server uskunalari	Ichki telefon tarmog‘i	Kirish chiqishni nazorat qilish tizimi	Videokuzatuv tizimi
Rektorat	Rektor	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	RWA DG
	O‘quv ishlari bo‘yicha prorektor	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	RWA DG
	Yoshlar masalalari va ma’naviy-ma’rifiy ishlar bo‘yicha birinchi prorektor	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	RWA DG
	Ilmiy ishlar va innovatsiyalar bo‘yicha prorektor	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	RWA DG
	Moliya-iqtisod ishlari bo‘yicha prorektor	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	RWA DG

Bo‘linma nomi va mas’ul xodim lavozimi		buxdu.uz	moodle.buxdu.uz	hemis.buxdu.uz	masofaviy.buxdu.uz	student.buxdu.uz	uniwork.buxdu.uz	citrus.buxdu.uz	journal.buxdu.uz	srep.buxdu.uz	pedskills.buxdu.uz	Korporativ elektron pochta	Fayl serverlar	Ishchi stansiyalar	Server uskunalari	Ichki telefon tarmog‘i	Kirish chiqishni nazorat qilish tizimi	Videokuzatuv tizimi
	Rektor yordamchisi	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	-
	Kotib-ish yurituvchi	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	-
	Universitet kengashi kotibi	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	RWA DG
	Xalqaro hamkorlik bo‘yicha prorektor	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	-
	Ilmiy kengashning ilmiy kotibi	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	RWA DG
	Universitet matbuot kotibi	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	RWA DG
	Talabalar orasida ijtimoiy-ma’naviy muhit barqarorligini ta’minlashga mas’ul bo‘lgan rektor maslahatchisi	R	-	-	-	-	-	RW	-	-	-	-	-	-	-	R	-	-

Bo‘linma nomi va mas’ul xodim lavozimi		buxdu.uz	moodle.buxdu.uz	hemis.buxdu.uz	masofaviy.buxdu.uz	student.buxdu.uz	uniwork.buxdu.uz	citrus.buxdu.uz	journal.buxdu.uz	srep.buxdu.uz	pedskills.buxdu.uz	Korporativ elektron pochta	Fayl serverlar	Ishchi stansiyalar	Server uskunalari	Ichki telefon tarmog‘i	Kirish chiqishni nazorat qilish tizimi	Videokuzatuv tizimi
	Universitet kengashi mutaxassisi	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	RWA DG
Rektor ofisi	Rektor ofisi boshlig‘i	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	RWA DG
	Yetakchi mutaxassis	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	-
Yoshlar ma’naviy yuksaltirishiga ko‘maklashish departamenti	Departament boshlig‘i	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	RWA DG
	Bosh mutaxassis	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	-
	Yetakchi mutaxassis	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	-
	Psixolog	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	-
Klub va to‘garaklar faoliyatini muvofiqlashtiruvchi sektor	Bosh mutaxassis	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	-
	Klub mudiri	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	-
Tyutorlar faoliyatini	Bosh mutaxassis	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	-
	Yetakchi mutaxassis	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	-

Bo‘linma nomi va mas’ul xodim lavozimi		buxdu.uz	moodle.buxdu.uz	hemis.buxdu.uz	masofaviy.buxdu.uz	student.buxdu.uz	uniwork.buxdu.uz	citrus.buxdu.uz	journal.buxdu.uz	srep.buxdu.uz	pedskills.buxdu.uz	Korporativ elektron pochta	Fayl serverlar	Ishchi stansiyalar	Server uskunalari	Ichki telefon tarmog‘i	Kirish chiqishni nazorat qilish tizimi	Videokuzatuv tizimi
muvofiqlashtiruvchi sektor	Tyutor	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	-
Talabalarni turar joy bilan ta’minlash sektori	Talabalar turar joyi direktori	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	-
	Bosh mutaxassis	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	-
	Yetakchi mutaxassis	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	-
O‘quv-uslubiy departament	Departament boshlig‘i	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	RWA DG
Akademik faoliyat va o‘quv normativ ta’minot sektori	Departament boshlig‘i o‘rinbosari-sektor mudiri	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	-
	Yetakchi mutaxassis	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	-
Malaka oshirish va amaliyot sektori	Bosh mutaxassis	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	-
	Yetakchi mutaxassis	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	-
Offis registrator va	Bosh mutaxassis	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	-
	Yetakchi mutaxassis	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	-

Bo‘linma nomi va mas’ul xodim lavozimi		buxdu.uz	moodle.buxdu.uz	hemis.buxdu.uz	masofaviy.buxdu.uz	student.buxdu.uz	uniwork.buxdu.uz	citrus.buxdu.uz	journal.buxdu.uz	srep.buxdu.uz	pedskills.buxdu.uz	Korporativ elektron pochta	Fayl serverlar	Ishchi stansiyalar	Server uskunalari	Ichki telefon tarmog‘i	Kirish chiqishni nazorat qilish tizimi	Videokuzatuv tizimi
talabalar bilan ishlash sektori	Mutaxassis	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	-
Ta’lim kredit tizimini boshqarish sektori	Bosh mutaxassis	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	-
	Yetakchi mutaxassis	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	-
Ilmiy tadqiqot va innovatsion faoliyatni rivojlantirish departamenti	Departament boshlig‘i	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	RWA DG
	Bosh mutaxassis	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	-
	Yetakchi mutaxassis	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	-
	Ilmiy-texnik va patent materiallariga ishlov beruvchi	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	-
Ilmiy-innovatsion ishlanmalarni tijoratlashtirish bo‘limi	Bosh mutaxassis	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	-
	Yetakchi mutaxassis	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	-
Talabalarning ilmiy tadqiqot faoliyatini	Bosh mutaxassis	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	RWA DG
	Yetakchi mutaxassis	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	-

Bo‘linma nomi va mas’ul xodim lavozimi		buxdu.uz	moodle.buxdu.uz	hemis.buxdu.uz	masofaviy.buxdu.uz	student.buxdu.uz	uniwork.buxdu.uz	citrus.buxdu.uz	journal.buxdu.uz	srep.buxdu.uz	pedskills.buxdu.uz	Korporativ elektron pochta	Fayl serverlar	Ishchi stansiyalar	Server uskunalari	Ichki telefon tarmog‘i	Kirish chiqishni nazorat qilish tizimi	Videokuzatuv tizimi
tashkil etish sektori																		
Axborot-resurs markazi	Direktor	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	-
	Direktor muovini	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	-
Ilmiy-uslubiy va axborot-ma’lumot bo‘limi	Bo‘lim mudiri	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	-
	Yetakchi mutaxassis	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	-
	Uslubchi	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	-
	Bibliograf 1-toifa	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	-
	Kutubxonachi 1-toifa	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	-
Axborot — kutubxona resurslari bilan xizmat ko‘rsatish bo‘limi (abonimentlarga xizmat ko‘rsatish, o‘quv zallari	Bo‘lim mudiri	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	-
	Bosh kutubxonachi	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	-
	Bibliograf 1-toifa	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	-
	Kutubxonachi 1-toifa	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	-

Bo‘linma nomi va mas’ul xodim lavozimi		buxdu.uz	moodle.buxdu.uz	hemis.buxdu.uz	masofaviy.buxdu.uz	student.buxdu.uz	uniwork.buxdu.uz	citrus.buxdu.uz	journal.buxdu.uz	srep.buxdu.uz	pedskills.buxdu.uz	Korporativ elektron pochta	Fayl serverlar	Ishchi stansiyalar	Server uskunalari	Ichki telefon tarmog‘i	Kirish chiqishni nazorat qilish tizimi	Videokuzatuv tizimi
va kitob saqlashni inobatga olgan holda)																		
Elektron axborot resurslari bo‘limi	Bo‘lim mudiri	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	-
	Axborot kutubxona texnologiyalari bo‘yicha yetakchi mutaxassis	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	-
	Kutubxonachi 1-toifa	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	-
Axborot — kutubxona resurslarini butlash, kataloglashtirish va tizimlashtirish bo‘limi	Bo‘lim mudiri	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	-
	Axborot kutubxona texnologiyalari bo‘yicha yetakchi mutaxassis	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	-
	Bibliograf 1-toifa	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	-
	Kutubxonachi 1-toifa	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	-

Bo‘linma nomi va mas’ul xodim lavozimi		buxdu.uz	moodle.buxdu.uz	hemis.buxdu.uz	masofaviy.buxdu.uz	student.buxdu.uz	uniwork.buxdu.uz	citrus.buxdu.uz	journal.buxdu.uz	srep.buxdu.uz	pedskills.buxdu.uz	Korporativ elektron pochta	Fayl serverlar	Ishchi stansiyalar	Server uskunalari	Ichki telefon tarmog‘i	Kirish chiqishni nazorat qilish tizimi	Videokuzatuv tizimi
Moliyalashtirish, iqtisodiy rivojlanishni rejalashtirish departamenti	Departament boshlig‘i	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	-
	Bosh mutaxassis	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	-
	Yetakchi mutaxassis	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	-
Buxgalteriya	Bosh buxgalter	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	-
	Bosh buxgalter o‘rinbosari	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	-
	Buxgalter	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	-
	G‘aznachi	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	-
	Xarid bo‘yicha bosh mutaxassis	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	-
To‘lov-kontrakt asosida o‘qitish bo‘yicha shartnomalarni rasmiylashtirish va hisobga olish guruhi	Buxgalter	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	-

Bo‘linma nomi va mas’ul xodim lavozimi		buxdu.uz	moodle.buxdu.uz	hemis.buxdu.uz	masofaviy.buxdu.uz	student.buxdu.uz	uniwork.buxdu.uz	citrus.buxdu.uz	journal.buxdu.uz	srep.buxdu.uz	pedskills.buxdu.uz	Korporativ elektron pochta	Fayl serverlar	Ishchi stansiyalar	Server uskunalari	Ichki telefon tarmog‘i	Kirish chiqishni nazorat qilish tizimi	Videokuzatuv tizimi
Inson resurslarini boshqarish departamenti	Departament boshlig‘i	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	RWA DG
	Bosh mutaxassis	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	-
	Kadrlar bo‘yicha menedjer	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	-
Birinchi bo‘lim	Bosh mutaxassis	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	-
Harbiy hisobga olish sektori	Bosh mutaxassis	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	-
	Yetakchi mutaxassis	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	-
Arxiv	Mutaxassis	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	-
Marketing va karyera bo‘limi	Bo‘lim boshlig‘i	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	RWA DG
	Yetakchi mutaxassis	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	-
	Mutaxassis	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	-
Xalqaro hamkorlik departamenti	Departament boshlig‘i	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	RWA DG
	Bosh mutaxassis	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	-
	Yetakchi mutaxassis	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	-

Bo‘linma nomi va mas’ul xodim lavozimi		buxdu.uz	moodle.buxdu.uz	hemis.buxdu.uz	masofaviy.buxdu.uz	student.buxdu.uz	uniwork.buxdu.uz	citrus.buxdu.uz	journal.buxdu.uz	srep.buxdu.uz	pedskills.buxdu.uz	Korporativ elektron pochta	Fayl serverlar	Ishchi stansiyalar	Server uskunalari	Ichki telefon tarmog‘i	Kirish chiqishni nazorat qilish tizimi	Videokuzatuv tizimi
Xalqaro loyihalar va investitsiyalar sektori	Bosh mutaxassis	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	-
	Yetakchi mutaxassis	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	-
Xalqaro reytinglar bilan ishlash sektori	Bosh mutaxassis	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	-
	Yetakchi mutaxassis	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	-
Raqamli ta’lim texnologiyalari departamenti	Departament boshlig‘i	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
Raqamli ta’lim texnologiyalarini joriy etish va axborot xavfsizligini ta’minlash sektori	Bosh mutaxassis	RWAE DGS	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWAE DGS	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-		-	RWAE DGS
	Muhandis-dasturchi	RWAE DGS	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWAE DGS	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	RWAE DGS
	Ma’lumotlar bazasi administratori	RWAE DGS	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWAE DGS	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	RWAE DGS
	Tizim administratori	RWAE DGS	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWAE DGS	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	RWAE DGS

Bo‘linma nomi va mas’ul xodim lavozimi		buxdu.uz	moodle.buxdu.uz	hemis.buxdu.uz	masofaviy.buxdu.uz	student.buxdu.uz	uniwork.buxdu.uz	citrus.buxdu.uz	journal.buxdu.uz	srep.buxdu.uz	pedskills.buxdu.uz	Korporativ elektron pochta	Fayl serverlar	Ishchi stansiyalar	Server uskunalari	Ichki telefon tarmog‘i	Kirish chiqishni nazorat qilish tizimi	Videokuzatuv tizimi
	Veb dizayner	RWAE DGS	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWAE DGS	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	RWAE DGS
	Kontent-menedjer	RWAE DGS	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWAE DGS	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	RWAE DGS
	Tarmoq administratori	RWAE DGS	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWAE DGS	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	RWAE DGS
Tarmoqlarni boshqarish va texnik qo‘llab-quvvatlash sektori	Tarmoq administratori	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	-
	Bosh mutaxassis	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	RWA DG
	Muhandis-dasturchi	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	-
	Muhandis-elektronchi	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	-
	O‘qitish texnik vositalarini qo‘llab quvvatlash	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	-

Bo‘linma nomi va mas’ul xodim lavozimi		buxdu.uz	moodle.buxdu.uz	hemis.buxdu.uz	masofaviy.buxdu.uz	student.buxdu.uz	uniwork.buxdu.uz	citrus.buxdu.uz	journal.buxdu.uz	srep.buxdu.uz	pedskills.buxdu.uz	Korporativ elektron pochta	Fayl serverlar	Ishchi stansiyalar	Server uskunalari	Ichki telefon tarmog‘i	Kirish chiqishni nazorat qilish tizimi	Videokuzatuv tizimi
	bo‘yicha muhandis																	
Tahririy-nashriyot bo‘limi	Muharrir	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	-
	Musahhih	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	-
	Texnik muharrir	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	-
	Bo‘lim boshlig‘i	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	-
Ta’lim sifatini nazorat qilish departamenti	Bosh mutaxassis	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	-
	Departament boshlig‘i	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	RWA DG
	Yetakchi mutaxassis	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	-
Ta’lim jarayonlari monitoringi sektori	Bosh mutaxassis	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	-
	Yetakchi mutaxassis	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	-
	Mutaxassis	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	-

Bo‘linma nomi va mas’ul xodim lavozimi		buxdu.uz	moodle.buxdu.uz	hemis.buxdu.uz	masofaviy.buxdu.uz	student.buxdu.uz	uniwork.buxdu.uz	citrus.buxdu.uz	journal.buxdu.uz	srep.buxdu.uz	pedskills.buxdu.uz	Korporativ elektron pochta	Fayl serverlar	Ishchi stansiyalar	Server uskunalari	Ichki telefon tarmog‘i	Kirish chiqishni nazorat qilish tizimi	Videokuzatuv tizimi
Bilim va malakalarni baholash sektori	Bosh mutaxassis	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	-
	Yetakchi mutaxassis	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	-
Magistratura bo‘limi	Bo‘lim boshlig‘i	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	RWA DG
	Bosh mutaxassis	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	-
	Yetakchi mutaxassis	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	-
Sirtqi(maxsus sirtqi) va masofaviy ta’lim bo‘limi	Bo‘lim boshlig‘i	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	RWA DG
	Bosh mutaxassis	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	-
	Yetakchi mutaxassis	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	-
	Mutaxassis	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	-
Binolarni saqlash va obodonlashtirish departamenti	Muhandis	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	-
	Texnik	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	-
	Katta tovarshunos	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	-
	Ombor mudiri	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	-

Bo‘linma nomi va mas’ul xodim lavozimi		buxdu.uz	moodle.buxdu.uz	hemis.buxdu.uz	masofaviy.buxdu.uz	student.buxdu.uz	uniwork.buxdu.uz	citrus.buxdu.uz	journal.buxdu.uz	srep.buxdu.uz	pedskills.buxdu.uz	Korporativ elektron pochta	Fayl serverlar	Ishchi stansiyalar	Server uskunalari	Ichki telefon tarmog‘i	Kirish chiqishni nazorat qilish tizimi	Videokuzatuv tizimi
	Departament boshlig‘i	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	-
	Bosh energetik	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	-
	Bosh muhandis	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	-
	Mexanik	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	-
Qurilish ta’mirlash sektori	Yetakchi mutaxassis	R	-	-	-	-	-	-	-	-	-	-	-	-	-	R	-	-
	Bosh mutaxassis	R	-	-	-	-	-	-	-	-	-	-	-	-	-	R	-	-
Fuqaro va mehnat muhofazasi sektori	Texnika va yong‘in xavfsizligi muhandisi	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	-
	Favqulodda holatlarni oldini olish profilaktikasi va fuqaro muhofazasi bo‘yicha muhandis	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	-
Muzey	Muzey direktori	R	-	-	-	-	-	-	-	-	-	-	-	-	-	R	-	-
	Fond saqlovchi	R	-	-	-	-	-	-	-	-	-	-	-	-	-	R	-	-
	Ekskursovod	R	-	-	-	-	-	-	-	-	-	-	-	-	-	R	-	-

Bo‘linma nomi va mas’ul xodim lavozimi		buxdu.uz	moodle.buxdu.uz	hemis.buxdu.uz	masofaviy.buxdu.uz	student.buxdu.uz	uniwork.buxdu.uz	citrus.buxdu.uz	journal.buxdu.uz	srep.buxdu.uz	pedskills.buxdu.uz	Korporativ elektron pochta	Fayl serverlar	Ishchi stansiyalar	Server uskunalari	Ichki telefon tarmog‘i	Kirish chiqishni nazorat qilish tizimi	Videokuzatuv tizimi
	Muzey kuzatuvchisi	R	-	-	-	-	-	-	-	-	-	-	-	-	-	R	-	-
	Ilmiy xodim	R	-	-	-	-	-	-	-	-	-	-	-	-	-	R	-	-
	Muzey mutaxassisi	R	-	-	-	-	-	-	-	-	-	-	-	-	-	R	-	-
	Muzey kuzatuvchisi	R	-	-	-	-	-	-	-	-	-	-	-	-	-	R	-	-
Fakultetlar	Dekan	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	RWA DG
	Dekan o‘rinbosari	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	-
	Yoshlar bilan ishlash bo‘yicha dekan o‘rinbosari	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	-
	Sirtqi (Maxsus sirtqi) ta’lim bo‘yicha dekan o‘rinbosari	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	-
	Menejer	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	-
Kafedralar	Kafedra mudiri	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	RWA DG
	Professor	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	-
	Dotsent	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	-

Bo‘linma nomi va mas’ul xodim lavozimi		buxdu.uz	moodle.buxdu.uz	hemis.buxdu.uz	masofaviy.buxdu.uz	student.buxdu.uz	uniwork.buxdu.uz	citrus.buxdu.uz	journal.buxdu.uz	srep.buxdu.uz	pedskills.buxdu.uz	Korporativ elektron pochta	Fayl serverlar	Ishchi stansiyalar	Server uskunalari	Ichki telefon tarmog‘i	Kirish chiqishni nazorat qilish tizimi	Videokuzatuv tizimi
	Katta o‘qituvchi	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	-
	Assistent o‘qituvchi	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	-
	Laboratoriya mudiri	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	-
	Kabinet mudiri	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	-
	Laborant	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	-
	Ishlab chiqarish ta’limi ustasi	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	-
Qo‘shma ta’lim dasturlarini muvofiqlashtirish bo‘limi	Bo‘lim boshlig‘i	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	RWA DG
	Bosh mutaxassis	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	-
	Yetakchi mutaxassis	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	-
	Tyutor	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	-
Yuridik bo‘lim	Yuridik bo‘lim boshlig‘i	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	RWA DG
	Yuristkonsult	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	-
	Bo‘lim boshlig‘i	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	-

Bo‘linma nomi va mas’ul xodim lavozimi		buxdu.uz	moodle.buxdu.uz	hemis.buxdu.uz	masofaviy.buxdu.uz	student.buxdu.uz	uniwork.buxdu.uz	citrus.buxdu.uz	journal.buxdu.uz	srep.buxdu.uz	pedskills.buxdu.uz	Korporativ elektron pochta	Fayl serverlar	Ishchi stansiyalar	Server uskunalari	Ichki telefon tarmog‘i	Kirish chiqishni nazorat qilish tizimi	Videokuzatuv tizimi
Ichki audit, moliya nazorat va uslubiy ko‘rsatma berish bo‘limi	Auditor	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	-
Korrupsiyaga qarshi kurashish “Komplaens nazorat” tizimini boshqarish bo‘limi	Bo‘lim boshlig‘i	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	RWA DG
	Bosh mutaxassis	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	-
Rektor ijro apparati	Ijro apparati boshlig‘i	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	RWA DG
Nazorat va ijro intizomi sektori	Bosh mutaxassis	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	-
	Bosh mutaxassis-rektor ijro apparati boshlig‘i o‘rinbosari	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	-
	Yetakchi mutaxassis	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	-
	Bosh mutaxassis	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	-

Bo‘linma nomi va mas’ul xodim lavozimi		buxdu.uz	moodle.buxdu.uz	hemis.buxdu.uz	masofaviy.buxdu.uz	student.buxdu.uz	uniwork.buxdu.uz	citrus.buxdu.uz	journal.buxdu.uz	srep.buxdu.uz	pedskills.buxdu.uz	Korporativ elektron pochta	Fayl serverlar	Ishchi stansiyalar	Server uskunalari	Ichki telefon tarmog‘i	Kirish chiqishni nazorat qilish tizimi	Videokuzatuv tizimi
Murojaatlar sektori	Yetakchi mutaxassis	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	-
Devonxona	Bosh mutaxassis	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	-
	Yetakchi mutaxassis	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	-
Fan va ta’lim mukammallik markazi	Markaz boshlig‘i	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	RWA DG
	Bosh mutaxassis	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	-
	Yetakchi mutaxassis	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	-
Xotin-qizlar bilan ishlash bo‘limi	Yetakchi mutaxassis	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	-
	Bo‘lim boshlig‘i	R	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RW	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	RWA DG	-	R	-	RWA DG
Boshqalar	Universitet xodimi bo‘lmagan shaxslar (masalan: autsorsing xizmati xodimlari)	R	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
	Internet foydalanuvchilari	R	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
	Boshqalar	R	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-

Foydalanish uchun ruxsat etilgan dasturiy ta’minotlar
RO‘YXATI

1. Universitetda operatsion tizim va uning tarkibiy qismlarini, ish stansiyalari bo‘yicha dasturiy ta’minotni o‘rnatish va yangilash ishlari Universitetda Raqamli ta’lim texnologiyalari departamenti Tarmoqlarni boshqarish va texnik qo‘llab-quvvatlash sektori bosh mutaxassisi (keyingi o‘rinlarda – Lokal tarmoq administratori) hamda Raqamli ta’lim texnologiyalari departamenti (keyingi o‘rinlarda – Departament) xodimlari tomonidan amalga oshiriladi. Boshqa xodimlarga ish stansiyalarda operatsion tizim, dasturiy ta’minotlarni mustaqil ravishda o‘rnatishga yo‘l qo‘yilmaydi.

2. Universitetda ruxsat etilgan dasturiy ta’minotlar ro‘yxati Universitetning axborot-kommunikatsiya texnologiyalarini joriy etish va raqamlashtirish bo‘yicha mas’ul rahbari (keyingi o‘rinlarda – Mas’ul rahbar) tomonidan tasdiqlanadi.

3. Ruxsat etilgan dasturiy ta’minotlar ro‘yxatiga qo‘shimcha o‘zgartirishlar kiritish zarurati tug‘ilganda Universitetning axborot xavfsizligini ta’minlash masalalari bo‘yicha mas’ul xodimi (keyingi o‘rinlarda – Axborot xavfsizligi administratori) hamda Departament boshlig‘i tomonidan ruxsat etilgan dasturiy ta’minotlarning yangi ro‘yxati shakllantiriladi va qayta tasdiqlash uchun tegishliligi bo‘yicha rahbariyatga kiritiladi.

Shuningdek, Siyosatning 15-bo‘limida keltirilgan Siyosatni qayta ko‘rib chiqish va yangilash tartibiga asosan Universitetda ruxsat etilgan dasturiy ta’minotlar ro‘yxatiga tegishli o‘zgartirishlar kiritilishi va qayta tasdiqlanishi mumkin.

4. Universitet xodimlaring ish stansiyalarida o‘rnatilishi ruxsat etilgan dasturiy ta’minotlar ro‘yxati 1-jadvalga, Universitet serverlariga o‘rnatilgan dasturlar ro‘yxati 2-jadvalga muvofiq keltirilgan.

5. Qo‘shimcha (maxsus, sinovdan o‘tkazadigan) dasturiy ta’minotni o‘rnatish foydalanuvchilarning asosli yozma talabiga binoan amalga oshiriladi.

6. Universitetda ma’lum bir vazifani bajarishga ixtisoslashgan ish stansiyalar uchun barcha istisnolar Axborot xavfsizligi administratori hamda Departament boshlig‘i bilan yozma ravishda kelishiladi va Rektor buyrug‘i bilan rasmiylashtiriladi.

7. Universitetda Axborot xavfsizligi administratori hamda Departament boshlig‘i Mas’ul rahbar bilan o‘rnatilgan tartibda kelishgan holda boshqa shunga o‘xshash dasturiy ta’minotni ishlab chiqaruvchilar tomonidan yangilanishlar chiqarilishini to‘xtatgan, shuningdek, funksional jihatdan ustun bo‘lgan yoki ro‘yxatda ko‘rsatilganlardan pastroq narxga ega bo‘lgan yangi dasturlar paydo bo‘lganda foydalanishga ruxsat berish huquqiga ega.

8. Universitetda ish faoliyatini olib borayotgan rahbar va xodimlarga ish stansiyalar “foydalanuvchi” huquqlari bilan beriladi.

9. Lokal tarmoq va Axborot xavfsizligi administratorlari, Departament boshlig‘i hamda xodimlariga ish stansiyalarida “administrator” huquqlari beriladi.

10. Universitetda foydalanishda bo‘lgan ish stansiyalar va serverlarda o‘rnatilishi ruxsat etilgan dasturiy mahsulotlar yuzasidan nazorat tegishliligi bo‘yicha Axborot xavfsizligi administratori hamda Departament boshlig‘i tomonidan doimiy ravishda amalga oshiriladi.

11. Universitetda litsenziyalangan dasturiy ta’minotlardan foydalanish bo‘yicha zaruriy choralar ko‘rilgan bo‘lishi shart.

1-jadval. **Universitet xodimlaring ish stansiyalarida o‘rnatilishi ruxsat etilgan dasturiy ta’minotlar ro‘yxati**

T/r	Dasturiy mahsulot tavsifi	Dasturiy mahsulot nomi	Dasturiy mahsulot versiyasi*	Dasturiy mahsulot ishlab chiqaruvchisi
1.	Operatsion tizimlar	Windows 8.1	6.3 (9600)	Microsoft Corporation
		Windows 10	21H2 (19043)	
		Windows 11	21H2 (22000.51)	
		Ubuntu Linux LTS	16.04	Ochiq kodli
		Debian	8	
		CentOS	RHEL 8	
		MacOS	10.12	Apple
2.	Virusdan himoyalovchi dasturlar	Kaspersky Endpoint Security	10	Laboratoriya Kasperskogo
		ESET Endpoint Antivirus	10	ESET
		ESET Endpoint Security	10	
3.	Ofis paketlari	MS Office	2016-2021	Microsoft Corporation
		Microsoft 365	E3	
		LibreOffice	7.1.0 (10)	The Document Foundation
		Apache OpenOffice	4.1.9	Apache Software Foundation
		WPS Office	11 (14732)	Kingsoft Office Software Corporation
4.	Arxivlovchi dasturlar	WinRAR	6.02	RARLAB
		7-Zip	23.01	Igor Pavlov
		WinZip	25 (14245)	Corel Corporation
		TAR	1.32	Ochiq kodli
5.	Internet brauzerlar	Internet Explorer	11	Microsoft Corporation
		Microsoft Edge	94	
		Mozilla Firefox	116	Mozilla
		Google Chrome	114	Google
		Yandex Browser	21	Yandex
		Brauzer E-IMZO	3.40.1	Yangi texnologiyalar markazi
6.	Elektron pochta dasturlari	E-xat	4.0.6.58	UNICON-SOFT
		Microsoft Outlook	2016	Microsoft Corporation
		Mozilla Thunderbird	115	MZLA Technologies Corporation
		Kerio Connect Client	9.2.1 (2397)	Kerio Technologies
7.	PDF fayllarni ko‘rish va tahrirlash uchun dasturlar	Adobe Acrobat reader	23	Adobe
		Adobe Acrobat Pro DC	2023.001.20143	
		Acrobat reader	11.0.23	

T/r	Dasturiy mahsulot tavsifi	Dasturiy mahsulot nomi	Dasturiy mahsulot versiyasi*	Dasturiy mahsulot ishlab chiqaruvchisi
		PDF-XChange Viewer	8.0.336.0	Tracker Software Products
		Foxit Reader	9.7.1.29511	Foxit Corporation
		Nitro Pro	13.70.0.30	Nitro Software
		ABBYY FineReader	15	ABBYY
8.	Grafik dasturlar	Adobe Photoshop	20.0	Adobe
		CorelDRAW	22	Corel
		AutoCAD	24.0	Autodesk
9.	Rasmlarni ko‘rish uchun dasturlar	FastStone Image Viewer	7.4	FastStone Soft
		Picasa	3.9.141.259	Google
		Microsoft Picture Manager	14.0.4750.1000	Microsoft Corporation
10.	Videopleyerlar	Windows Media Player	12	Microsoft Corporation
		K-Lite Codec Pack	15.3.5	Codec Guide
		Pot player	1.7.20977	Kakao
		The KMPlayer	4.2.1.2	Pandora TV
11.	Audiopleyer	AIMP	4.60.2170	AIMP DevTeam
12.	Fayl menedjerlar	Total commander	9.22a	Kristian Gisler
		FarManager	3.0.5511	FAR Group
		PuTTY	0.79	Simon Tatham
		WinSCP	6.1.2	Martin Prikril
		Filezilla	3.65.0	Tim Kosse
		Bitvise SSH Client	9.31	Bitvise Limited
13.	Messenjerlar	HUMO Messenger	3.7.4	UNICON-SOFT
		Telegram	4.11	Pavel Durov
14.	Elektron imzo uchun dastur	E-IMZO	4.21	Yangi texnologiyalar markazi
15.	Buxgalteriya hisobot va tahlili uchun dasturlar	1C	8	1C Company
		eStat	4.0	Statistika agentligi
		Norma Hamkor	7.6.1	Norma
		UzAsbo	1.0.8	Axborot texnologiyalari markazi
16.	Video konferensiya dasturi	Zoom	5.16.2 (22807)	Zoom Video Communications
		Microsoft Teams	1.6.00.364	Microsoft Corporation
		Google Meet	17	Google
		Skype for business	16.0.4849.1000	Microsoft Corporation
17.	VPN-ulanish uchun dasturlar	Kerio VPN client	9.2.9-3171	Kerio Technologies
		OpenVPN client	2.6.3	OpenVPN
		Palo Alto client	5.2.4	Palo Alto
18.	Yordamchi dasturlar	Microsoft .Net Framework	4.8	Microsoft Corporation
		Microsoft Silverlight	5	
19.	Dasturlash tillari	Java	8.0	Oracle Corporation
		VueJS	2.7	Evan You
		Visual Studio	17.0	Microsoft Corporation
		Python	3.10.10	Python Software Foundation

T/r	Dasturiy mahsulot tavsifi	Dasturiy mahsulot nomi	Dasturiy mahsulot versiyasi*	Dasturiy mahsulot ishlab chiqaruvchisi
		C++	23	Joint Technical Committee
		C#	11.0	Microsoft Corporation
		Html 5	5.3	Web Hypertext Application Technology Working Group
		CSS	3	World Wide Web Consortium
		Java Script	13	Brendan Eyx
		PHP	7.3	Rasmus Lerdorf
		MySQL	8.2.0	MySQL AB
20.	IP-telefon	MicroSIP	3.21.3	MDev Group

**Izoh: Dasturlar versiyasi va sborkasi hamda litsenziya to‘g‘risidagi ma’lumotlar Administratorlar tomonidan doimiy yangilab borilganligi bois qo‘lda to‘ldirib boriladi.*

2-jadval.

Universitet serverlariga o‘rnatilgan dasturiy ta’minotlar ro‘yxati

T/r	Dasturiy mahsulot tavsifi	Dasturiy mahsulot nomi	Dasturiy mahsulot versiyasi	Dasturiy mahsulot ishlab chiqaruvchisi
1.	Server uchun operatsion tizimlar	Microsoft Windows Server 2019, 2022	10.0 (17763), 20348.1906 (21H2)	Microsoft Corporation
		CentOS	RHEL 8	Ochiq kodli
		Debian	10, 11, 12	
		Ubuntu	18, 20, 22, 23	
2.	Internet-trafikni tarqatish dasturi (proksi-server)	FortiGate 100F	5.4.0	Fortinet Technologies
		Palo Alto	9.1.5	Palo Alto Networks
		Kerio Control	9.2.9 (3171)	Kerio Technologies
3.	Virusdan himoyalovchi dastur	ESET Endpoint Antivirus	10	ESET
		ESET Server Security for Microsoft Windows Server	10.0.12014.0	
4.	“ESET Endpoint” dasturlarini boshqarish	ESET Security Management Center	10	ESET
5.	Virtualizatsiya tizimi uchun dastur	VMware ESXI	6.7.0	VMware
6.	IP-telefon tizimi	Kerio Operator	2.6.4	Kerio Technologies
7.	Fayl menedjerlar	Total commander	9.22a	Kristian Gisler
		FarManager	3.0.5511	FAR Group
8.	Arxivlovchi dasturlar	WinRAR	6.02	RARLAB
		7-Zip	23.01	Igor Pavlov

T/r	Dasturiy mahsulot tavsifi	Dasturiy mahsulot nomi	Dasturiy mahsulot versiyasi	Dasturiy mahsulot ishlab chiqaruvchisi
9.	Zaxira nusxa oluvchi dasturlar	Rsync	3.2.2	Wayne Davison

**Izoh: Dasturlar versiyasi va sborkasi hamda litsenziya to‘g‘risidagi ma’lumotlar Administratorlar tomonidan doimiy yangilab borilganligi bois qo‘lda to‘ldirib boriladi.*

Universitet axborot xavfsizligi
siyosatiga 13-ilova

Internet tarmog‘i resurslaridan foydalanish va korporativ elektron pochta bilan ishlash bo‘yicha YO‘RIQNOMA

1. Asosiy qoidalar

1.1 Ushbu Yo‘riqnoma Universitet xodimlarining internet tarmog‘i resurslaridan foydalanish va korporativ elektron pochta bilan ishlash tartibi va talablarini belgilaydi.

1.2 Universitet binosidagi lokal tarmoqlar orqali xodimlarga faqatgina o‘zlarining xizmat vazifalarini bajarish uchun tashqi axborot manbalariga to‘g‘ridan-to‘g‘ri internetga ulanish imkoniyati beriladi.

Xodimlarga internetdan foydalanish imkoniyati Universitetda Raqamli ta’lim texnologiyalari departamenti Tarmoqlarni boshqarish va texnik qo‘llab-quvvatlash sektori bosh mutaxassisi (keyingi o‘rinlarda – Lokal tarmoq administratori) hamda Raqamli ta’lim texnologiyalari departamenti (keyingi o‘rinlarda – Departament) xodimlari tomonidan “shaffof” proksi-server orqali tashkil etiladi.

Universitetning barcha xodimlari Universitet aloqa kanallari orqali o‘tadigan va/yoki Universitetga tegishli qurilmalarga kelib tushgan har qanday turdagi ma’lumotlar Universitetning mulki ekanligini tan oladi, unga kirish va tahlil qilish Universitet manfaatlariga javob berishi shart.

1.3 Korporativ elektron pochta tizimida Universitetning barcha xodimlariga elektron pochta qutisi ochib beriladi.

Korporativ elektron pochta xizmatlari Universitet xodimlariga faqat o‘zlarining xizmat vazifalarini bajarishlari uchun beriladi. Korporativ elektron pochta xizmatlaridan shaxsiy maqsadlarda foydalanish qat’iyan taqiqlanadi.

1.4 Internetga kirish va korporativ elektron pochtaga ulanishni amalga oshiradigan xodimlarning ro‘yxati Universitetning axborot xavfsizligini ta’minlash masalalari bo‘yicha mas’ul xodimi (keyingi o‘rinlarda – Axborot xavfsizligi administratori) hamda Raqamli ta’lim texnologiyalari departamenti (keyingi o‘rinlarda – Departament) boshlig‘i tomonidan shakllantiriladi va Universitetning axborot-kommunikatsiya texnologiyalarini joriy etish va raqamlashtirish bo‘yicha mas’ul rahbari (keyingi o‘rinlarda – Mas’ul rahbar) tomonidan belgilanadi.

Mas’ul rahbarning roziligisiz qo‘shimcha ravishda internetga ulanishni mustaqil ravishda tashkil etish va korporativ elektron pochtaga ulanish taqiqlanadi.

1.5 Tezkor xabar almashish tizimlaridan (messenjerlardan) foydalanish huquqi o‘zlarining ish faoliyatiga oid vazifalarini bajarish uchun ishlab chiqarish ehtiyojiga ega bo‘lgan xodimlargagina beriladi. Ushbu xodimlarning ro‘yxati Universitetda Mas’ul rahbar tomonidan belgilanadi.

Universitetning barcha xodimlari o‘z tashkilotida o‘rnatilgan tartibda ro‘yxati shakllantirilgan va tasdiqlangan har qanday konfidensial ma’lumotni ruxsat etilmagan messenjerlardan, shuningdek, internetdagi boshqa ma’lumotlar almashish tizimlari

(tezkor xabar almashish tizimlari, ijtimoiy tarmoqlar va boshqa tizimlar, shu jumladan har qanday turdagi internet-pochta) orqali uzatish taqiqlanadi.

1.6 Korporativ elektron pochta matnli xabarlar yoki elektron shakldagi hujjatlar shaklida xizmat ma’lumotlarini almashish uchun ishlatiladi. Konfidensial ma’lumotlarning konfidensialligi va yaxlitligini ta’minlagan holda, xususan, E-xat tizimi orqali uzatilishi shart.

1.7 Internet yoki elektron pochta orqali kirib kelgan har qanday elektron ma’lumotlar virusga qarshi dastur yordamida tekshirilishi kerak.

1.8 Xodimlar uchun internetga va korporativ elektron pochtaga kirishlari bilan bog‘liq ishlarni tashkil qilish Universitetda Lokal tarmoq administratori hamda Departament xodimlari tomonidan amalga oshiriladi.

Korporativ elektron pochtaga kirish huquqiga ega bo‘lgan xodim unikal pochta manzilini oladi. Korporativ elektron pochta manzili xodimga Universitetda Lokal tarmoq administratori hamda Departament xodimlari tomonidan beriladi.

1.9 Lokal tarmoq orqali internetga kirish ish stansiyasida amalga oshiriladi. Boshqa shaxsning ish stansiyasidagi harakatlari uchun javobgarlik ushbu ish amalga oshirilgan ish stansiyasi biriktirilgan xodim zimmasiga yuklatiladi.

1.10 Xodimlar tomonidan Yo‘riqnoma talablarining bajarishi Axborot xavfsizligi administratori hamda Departament boshlig‘i tomonidan nazorat qilinadi, shuningdek, tegishli vazifalar xodimlarning lavozim yo‘riqnomalarida belgilanadi.

1.11 Universitet binolarida tashkil etilgan simsiz internet tarmoqlari orqali har qanday ma’lumotlarni, shuningdek, noma’lum kirish tizimlariga (anonimayzerlar, Wi-Fi tarmoqlari, tashqi VPN serverlar va foydalanuvchini va uning harakatlarini yashiradigan boshqa tizimlar) yuklab olish taqiqlanadi. Shuningdek, kompyuterga yoki mobil qurilmaga masofadan turib kirishni ta’minlaydigan har qanday tizimlardan foydalanishga yo‘l qo‘yilmaydi, garchi bunday kirish ishlab chiqarish va ishlarni tashkil etish ehtiyojlarini ta’minlash bilan bog‘liq bo‘lsa ham.

Shuningdek, kriptovalyutalarni yig‘ib olish, Universitetning ishlab chiqarish faoliyatini ta’minlash bilan bog‘liq bo‘lmagan boshqa har qanday faoliyat uchun Universitetning har qanday qurilmasidan foydalanish qat’iyan man etiladi.

1.12 Xodimlarning internetdagi faoliyati Universitet binolarida “Kerio Control” hamda “FortiGate” tarmoqlararo ekran tizimlari yordamida nazorat qilinadi. Mazkur tarmoqlararo ekran tizimlaridagi jurnallar tahlili quyidagi parametrlarga muvofiq amalga oshiriladi:

- ishlatilgan resurslar ro‘yxati;
- trafik hajmi.

Internetdan foydalanishda kirish, foydalanish vaqti, resurs nomi va xodim haqida boshqa ma’lumotlarni o‘z ichiga olgan elektron yozuvlar Universitetda Lokal tarmoq administratori va Departament xodimlari tomonidan keyingi tahlil qilish uchun saqlanishi shart.

2. Internet foydalanuvchilari uchun asosiy talablar

2.1 Internetdan foydalanganda quyidagilar zarur:

- ushbu Yo‘riqnoma talablariga, shuningdek, axborot xavfsizligini ta’minlashga oid boshqa ichki me’yoriy hujjatlarga rioya qilish;

- internetdan faqat o‘z xizmat vazifalarini bajarish uchun foydalanish;

- Lokal tarmoq administratori yoki Departament xodimlariga ushbu Yo‘riqnoma talablari buzilganligi to‘g‘risida xabar berish;

- o‘zlarining identifikatsiya ma’lumotlarini (parollar va boshqalar) sir saqlash, uchinchi shaxslarga identifikatsiya ma’lumotlarini bermaslik yoki oshkor qilmaslik.

2.2 Universitet xodimlari o‘zlariga berilgan ish stansiyalari orqali internetdan quyidagi maqsadlarda foydalanish huquqiga ega:

- internetdagi axborot resurslariga kirish orqali o‘zlarining ish faoliyatiga oid vazifalarini bajarish uchun zarur bo‘lgan har qanday ochiq ma’lumotni internet tarmog‘idan olish;

- uchinchi tomon tashkilotlari (muassislar, ishtirokchilar, pudratchilar, ijrochilar va boshqalar) bilan o‘zaro aloqalar qilish;

- xodim o‘z vazifalarini va boshqa rasmiy vazifalarini rahbarlar tomonidan belgilangan muddatlarda qat’iy bajarishi sharti bilan, o‘z bilim va malakasini oshirish yuzasidan, shuningdek, O‘zbekistonning ijtimoiy-siyosiy va ijtimoiy-iqtisodiy hayoti bilan tanishish va respublikadagi va dunyodagi o‘z sohasiga oid so‘nggi voqealar to‘g‘risida ma’lumot olish;

- ish faoliyati bilan bog‘liq onlayn xizmatlardan foydalanish, xususan, chiptalarni sotib olish, mehmonxonalarni band qilish, viza olish va h.k.;

- xizmat safarlari, xorijiy vakillar bilan ish yuzasidan yozishmalarni amalga oshirish, tashkil etiladigan boshqa tadbirlarni o‘tkazish bilan bog‘liq tashkiliy masalalarni hal qilish;

- dasturiy ta’minotlarni o‘z vaqtida yangilash va h.k.

2.3 Universitet xodimlariga internetdan foydalanishda quyidagilar taqiqlanadi:

- internetdan shaxsiy yoki ko‘ngilochar maqsadlarda foydalanish;

- internetga ruxsatsiz ulanish imkoniyatini beradigan maxsus qurilma va dasturlardan foydalanish;

- lokal tarmoq elementlarining normal ishlashini buzishga qaratilgan har qanday harakatlarni bajarish;

- internetda ishlashda tashqi proksi-serverlardan foydalanish;

- ish faoliyati bilan bog‘liq ma’lumotlarni yuborish uchun korporativ bo‘lmagan elektron pochtadan foydalanish;

- konfidensial ma’lumotlarni yuborish uchun shaxsiy elektron pochta, ijtimoiy tarmoqlar va boshqa ruxsat etilmagan tezkor xabar almashish tizimlaridan foydalanish;

- foydalanuvchi ma’lumotlari va parollarini uzatish;

- tarmoq yukini oshiradigan va boshqa foydalanuvchilarning normal ishlashiga xalaqit beradigan video va audio oqimlarning uzatiladigan manbalardan foydalanish;

- shubhali manbalarga, shu jumladan quyidagi toifadagi saytlarga tashrif buyurish:

- barcha turdagi onlayn kazinolar;

- o‘yinlar;

- tanishuv saytlari;

- O‘zbekiston Respublikasining amaldagi qonunchiligi bilan taqiqlangan qaroqchilik (pirat) va pornografik kontentni tarqatish saytlari;

- ekstremistik tashkilotlar saytlari;

- mayning saytlari;

- har qanday kriptovalyuta;
- bukmekerlik saytlari;
- internetda noqonuniy operatsiyalarni amalga oshirish va qonun hujjatlariga, shuningdek, ushbu Yo‘riqnoma talablariga zid bo‘lgan boshqa harakatlarni bajarish.

3. Internet orqali ma’lumot olish va tarqatish

3.1 Xodimlar o‘zlarining ish joylaridan internetga kirish imkoniyatiga ega bo‘ladilar (Maxsus bo‘lim xodimlari bundan mustasno). Xodimlar ma’lumotni qabul qilish va tarqatish uchun internetga kirish huquqiga ega.

3.2 Xodimlar internetdan o‘zlarining ish faoliyatiga oid vazifalarini bajarish uchun zarur bo‘lgan har qanday ochiq ma’lumotni qidiruv tizimlari orqali internetdagi axborot resurslariga kirish yoki URL manzilini kiritish orqali olishlari mumkin.

3.3 Xodimlar internetda quyidagilarni amalga oshirishi mumkin:
- Universitet faoliyati to‘g‘risida jamoatchilikka ma’lum bo‘lgan ma’lumotlarni olish;
- Universitetning ommaviy tadbirlari to‘g‘risidagi yangiliklar va axborotlarni tarqatish;
- ish faoliyatida o‘zaro aloqada bo‘lgan uchinchi tomon tashkilotlari uchun zarur bo‘lgan ochiq ma’lumotlarni yetkazib berish;
- bo‘sh ish o‘rinlari to‘g‘risida ma’lumot tarqatish;
- ish faoliyatida o‘zaro aloqada bo‘lish uchun ochiq aloqa ma’lumotlarini va boshqa ma’lumotlarni taqdim etish.

3.4 Yuqoridagi ma’lumotlarni tarqatish huquqi Universitet xodimlariga o‘zlarining xizmat vazifalariga muvofiq ravishda va faqat tegishliligi bo‘yicha o‘z rahbariyatidan bunday tarkibni tarqatish zarurligi to‘g‘risida olingan topshiriqning bajarilishi munosabati bilan beriladi.

3.5 Internetga ulanish huquqiga ega bo‘lgan xodimlarning ro‘yxatini shakllantirishda uning internetda ma’lumot olish va tarqatish bo‘yicha huquq va majburiyatlari ko‘rsatiladi.

3.6 Universitetning internetga ulanadigan xodimlari ro‘yxati uning bevosita rahbari va bo‘linma boshliqlari tomonidan tasdiqlangan rasmiy arizasiga binoan shakllantiriladi. Ko‘rsatilgan arizada internetdan foydalanish zarurati, xodimning internetdan resurslaridan foydalanishdagi huquq va majburiyatlari ko‘rsatilishi kerak.

Arizani Mas’ul rahbar ma’qullaganidan so‘ng, xodim Internetga kirish huquqini oladiganlar ro‘yxatiga kiritiladi va unga kirish imkoniyati yaratiladi.

3.7 Internet tarmog‘i orqali ma’lumot tarqatishda xodimlar quyidagi talablarga rioya qilishlari shart:
- ishonchli, to‘liq va obyektiv ma’lumotlarni nashr etish;
- materiallarni nashr etishda, shu jumladan shaxsiy fikrlarini bildirganda, faqat o‘zlarining ish faoliyatiga oid vazifalariga tayanishlari;
- nashr etilgan materiallar uchun to‘liq javobgarlikni anglash;
- intellektual faoliyat natijalari va individualizatsiya vositalariga nisbatan uchinchi shaxslarning huquqlarini kuzatish va hurmat qilish;
- boshqa internet foydalanuvchilari bilan to‘qnashuvlar va nizolardan saqlanish.

3.8 Universitet xodimlariga quyidagi ma’lumotlarni o‘z ichiga olgan materiallarni nashr etish, yuklab olish va tarqatish taqiqlanadi:

- konfidensial ma’lumotlar, shuningdek, tijorat sirini tashkil etuvchi ma’lumotlar, agar u xizmat vazifalariga kirmasa yoki Lokal tarmoq administratori bilan oldindan kelishib olinmagan bo‘lsa;
- egasining ruxsatisiz, to‘liq yoki qisman mualliflik huquqi yoki boshqa huquqlar bilan himoyalangan ma’lumotlarni tarqatish;
- ruxsatsiz kirish uchun har qanday apparat va dasturiy ta’minotni buzish, yo‘q qilish yoki cheklash uchun mo‘ljallangan zararli dastur, shuningdek, tijorat dasturlari va ularni ishlab chiqarish uchun dasturiy ta’minot uchun seriya raqamlari, parol va pullik internetga ruxsatsiz kirish huquqini beradigan boshqa vositalar;
- tahdid soluvchi, tuhmat, yolg‘on ma’lumot, shuningdek, boshqalarning sha’ni va qadr-qimmatini kamsituvchi ma’lumotlar, etnik nafratni qo‘zg‘atuvchi, zo‘ravonlikni qo‘zg‘atuvchi, noqonuniy xatti-harakatlarni sodir etishga chaqiruvchi materiallar va boshqalar;
- IP-manzil va boshqa xizmat ma’lumotlarini qalbakilashtirish.

3.9 Internetdan yuklab olingan barcha fayllar zararli dasturlarning mavjudligi bo‘yicha majburiy ravishda tekshirilishi shart.

3.10 Universitetda Lokal tarmoq administratori hamda Departament xodimlari xodimlarning Siyosat talablariga zid bo‘lgan ba’zi bir internet-resurslaridan foydalanishni tarmoqlararo ekran va proksi-server orqali cheklash huquqiga ega.

4. Internet-resurslardan foydalanish bo‘yicha nazorat

4.1 Universitet xizmat majburiyatlarini bajarish bilan bog‘liq bo‘lmagan internet resurslarini, shuningdek, mazmuni va yo‘nalishi xalqaro va milliy qonun hujjatlarida taqiqlangan manbalarga kirishni cheklash huquqini o‘zida saqlab qoladi.

4.2 Lokal tarmoq administratori hamda Departament xodimlari Universitet xodimlarining internet resurslaridan foydalanishi to‘g‘risidagi yozuvlarni yuritadi, ushbu Yo‘riqnoma talablariga rioya qilinishini nazorat qiladi va internet resurslaridan xavfsiz foydalanishni ta’minlaydi.

4.3 Axborot xavfsizligi administratori va Departament boshlig‘i Universitetda internetdan maqsadli foydalanishini qisman, to‘liq oldindan kelishilmagan holda, shuningdek, onlayn tekshirishni amalga oshirishga haqlidir.

4.4 Xodimlar tashrif buyurgan internet manbalari to‘g‘risidagi ma’lumotlar keyinchalik tahlil qilish uchun qayd qilinadi va zarur bo‘lganda Rektor topshirig‘iga ko‘ra ularni monitoring qilish uchun tegishli mas’ullarga taqdim etish mumkin.

4.5 Xodimlarning internetdagi faoliyatini kuzatadigan maxsus dasturiy ta’minot ishining natijalariga, shuningdek, internetdan maqsadli foydalanishda qisman va to‘liq tekshiruv natijalariga ko‘ra eng zararli buzuvchilari aniqlanadi.

4.6 Noto‘g‘ri foydalanish holatlari Universitetda Axborot xavfsizligi administratori hamda Departament boshlig‘i tomonidan “Internetdan noto‘g‘ri foydalanish to‘g‘risidagi bayonnoma” ko‘rinishida qayd etiladi.

Aniqlangan internetni suiiste’mol qilish faktiga ko‘ra, buzg‘unchidan tushuntirish xati ko‘rinishidagi yozma ariza olinadi.

Internet tarmog‘idan noto‘g‘ri foydalanish to‘g‘risidagi bayonnoma Axborot xavfsizligi administratori va Departament boshlig‘i hisoboti bilan tasdiqlanadi va Rektorga qaror qabul qilish uchun taqdim etiladi.

4.7 Agar xodim internetdan noto‘g‘ri foydalanishda gumon qilinsa, ichki audit o‘tkaziladi.

5. Korporativ elektron pochtadan foydalanish qoidalari

5.1 Korporativ elektron pochta bilan ishlashda xodimlar quyidagilarni hisobga olishi kerak:

- korporativ elektron pochta – bu yuborilgan xabarni qabul qiluvchiga kafolatli yetkazish vositasi emas;
- korporativ elektron pochta – bu uzatilayotgan ma’lumotlarning konfidensialligini ta’minlaydigan ma’lumotni uzatish vositasi emas. Konfidensial ma’lumotlarni uzatishga faqat xavfsiz ulanishga ega ruxsat etilgan tizimlar yoki E-xat tizimidan foydalanish mumkin.
- har qanday elektron pochta xabarlari, hattoki ma’lum jo‘natuvchi tanish bo‘lgan taqdirda ham tahdid tug‘ilishi mumkin, shu sababli jo‘natuvchini shaxsan o‘zi tanigan jo‘natuvchi bo‘lsa ham ochishda zarur ehtiyot choralarini ko‘rgan bo‘lishi kerak.

5.2 Departament xodimlari foydalanuvchining pochta qutisi va uzatiladigan ma’lumotlar umumiy hajmiga elektron pochta serverini tashkil qilish uchun ishlatiladigan dasturiy ta’minot va telekommunikatsiya va server qurilmalarining hozirgi imkoniyatlaridan kelib chiqib cheklov qo‘yadi. Saqlangan yoki uzatiladigan ma’lumotlar belgilangan cheklovdan oshib ketgan taqdirda, korporativ elektron pochta tizimiga kirish bloklanadi. Korporativ elektron pochta tizimiga kirish bloklangan bo‘lsa, uning pochta qutisi hajmi oshib ketishi va foydalanuvchi pochta qutisini tozalash zarurligi to‘g‘risida xabar paydo bo‘ladi.

5.3 Korporativ elektron pochta foydalanuvchilariga quyidagilar taqiqlanadi:

- korporativ elektron pochtadan har qanday shaxsiy yozishmalar yoki tijorat maqsadlarida foydalanish;
- siyosiy, diniy, insoniylikka qarshi xarakterdagi, shuningdek, odobsiz, tuhmat, haqoratli, tahdid soluvchi yoki noqonuniy materiallarni korporativ elektron pochta yoki boshqa elektron vositalar orqali yuborish, saqlash va foydalanish. Shunga o‘xshash xarakterga ega ma’lumotlar paydo bo‘lganda, xodim darhol o‘zining bevosita rahbarini, Axborot xavfsizligi administratorini hamda Departament boshlig‘ini xabardor qilishi shart.
- reklama (sohaga oid bo‘lmagan) va ko‘ngilochar xarakterdagi materiallarni yuborish;
- ish faoliyatiga aloqasi bo‘lmagan xatlarning ommaviy tarqatilishini amalga oshirish;
- zararli dasturlarni yoki viruslarni yuqtirgan fayllarni yuborish;
- rasmiy yozishmalar uchun bepul internet pochta xizmatlaridan (mail.ru, yandex.ru va boshqalar) foydalanish;
- uchinchi shaxsga o‘z pochta qutilariga axborot tizimlari va resurslariga kirish parolini berish.

5.4 Yuborilgan elektron pochta xabari va boshqa elektron hujjatlarning mazmuni aniq, qisqa va tushunarli bo‘lishi kerak.

5.5 Universitet xodimlar uchun quyidagilar qat’iy taqiqlangan:

- yozishmalar va rasmiy ma’lumot almashish uchun “.UZ” domen hududidan tashqarida joylashgan ruxsatsiz tashqi pochta xizmatlaridan foydalanish;
- konfidensial ma’lumotni himoyalanmagan shaklda korporativ elektron pochta orqali yuborish.

6. Javobgarlik

6.1 Universitetning barcha xodimlari ushbu Yo‘riqnoma talablarini buzganlik uchun shaxsan javobgardirlar.

6.2 Ushbu Yo‘riqnomada belgilangan xodimlarining internet tarmog‘i resurslaridan foydalanish va korporativ elektron pochta bilan ishlash tartibi va talablarining buzilishi Universitet ichki mehnat qoidalari va O‘zbekiston Respublikasining mehnat qonunchiligiga muvofiq intizomiy javobgarlikka tortishga sabab bo‘ladi.

6.3 Axborot xavfsizligi administratorlari hamda Departament boshlig‘i Universitetda mas’ul xodimlar tomonidan ushbu Yo‘riqnoma talablarining bajarilishi ustidan nazoratni ta’minlashga mas’uldir.

Axborot aktivlarini boshqarish
TARTIBI

1. Umumiy qoidalar

1.1 Ushbu Tartib Universitetning axborot tizimlari va resurslari Reestrini (keyingi o‘rinlarda – Reestr) shakllantirish, axborot tizimlari va resurslarini inventarizatsiya qilish, tasniflash va markirovkalash tartibiga qo‘yiladigan talablarni belgilaydi.

1.2 Mazkur Tartib Universitet xodimlari tomonidan foydalaniladigan axborot aktivlariga nisbatan qo‘llaniladi.

1.3 Universitetning axborot xavfsizligini ta’minlash masalalari bo‘yicha mas’ul xodimi (keyingi o‘rinlarda – Axborot xavfsizligi administratori) hamda Raqamli ta’lim texnologiyalari departamenti (keyingi o‘rinlarda – Departament) boshlig‘i ushbu Tartibning ilovasiga muvofiq tegishli Reestrni shakllantirish va yangilab turish uchun javobgardir.

Yangi axborot tizimlari va resurslari (aktivlari) paydo bo‘lishi bilan Reestrga o‘zgartirish va qo‘shimchalar kiritilishi mumkin.

1.4 Universitetda mavjud asosiy axborot tizimlari va resurslari ushbu Siyosatning 8.3-bandiga asosan 1-jadvalda keltirilgan.

1.5 Reestrda saqlanadigan (konfidensial yoki ochiq ma’lumotlar) ma’lumotlarning tasnifiga muvofiq axborot aktivlari klassifikatsiyasi belgilanishi kerak.

2. Axborot aktivlariga egalik qilish va javobgarlik

2.1 Axborot xavfsizligi administratori, Departament boshlig‘i hamda Axborot aktivlarining egasi quyidagilarga javobgar bo‘ladi:

- axborot aktivlarining uzluksiz ishlashi, konfidensialligi va butligini ta’minlash;
- axborot aktivlarining tegishliligi bo‘yicha tasniflanishini ta’minlash;
- xodimlarning axborot aktivlariga kirishini boshqarish va vakolatlarini taqsimlash vazifalarni amalga oshiradi.

2.2 Axborot aktivining egasi axborot aktiviga kirish huquqlarini boshqarish uchun javobgardir.

2.3 Har bir axborot aktivi uchun uning qiymatidan kelib chiqqan holda himoya darajasi o‘rnatiladi. Axborot aktivini himoya qilish darajasi axborot aktivining egasi hamda Departament boshlig‘i bilan kelishilgan holda Axborot xavfsizligi administratori tomonidan belgilanadi.

2.4 Reestrni tuzish va yangilash uchun javobgarlik, shuningdek, axborot aktivlari toifasiga qarab ularning konfidensialligi, yaxlitligi va foydalana olishligini ta’minlash bo‘yicha talablarni belgilash Axborot xavfsizligi administratori hamda Departament boshlig‘iga yuklanadi.

2.5 Axborot aktivlarining axborot xavfsizligini ta’minlash uchun javobgarlik ushbu aktivlarning egalariga, axborot xavfsizligini to‘g‘ri ta’minlash ustidan nazorat esa Axborot xavfsizligi administratori hamda Departament boshlig‘iga yuklanadi.

3. Axborot aktivlariga egalik qilish

3.1 Axborot aktivining egasi – Universitetning tarkibiy qismi bo‘lib, u axborot aktivini shakllantiradi va saqlaydi.

3.2 Barcha asosiy axborot aktivlari egalari (tegishli bo‘linmalari) aniqlanishi va Reestrda ko‘rsatilishi kerak.

3.3 Axborot aktivi egasiga mazkur axborot aktiviga tegishli barcha ma’lumotlar, ma’lumotlarni qayta ishlash jarayonlari va vositalari hamda ilovalari beriladi.

3.4 Axborot aktiviga egalik huquqini axborot aktivi egalari tomonidan boshqa bo‘linmaga topshirishlari mumkin emas. Ushbu vazifa Universitet rahbariyatining qaroriga muvofiq amalga oshiriladi.

4. Axborot aktivlaridan maqbul foydalanish

4.1 Axborot aktivlariga kirish huquqini Universitetning bunday imkoniyatga ega bo‘lgan xodimlari olishadi.

4.2 Axborot aktivlariga kirish xodimlarga ma’lumotlardan foydalanish, shuningdek, axborot aktivlarini shakllantirish uchun taqdim etiladi. Belgilangan kirishlar ushbu Siyosatning 11-ilovasi “Axborot manbalariga kirish matritsasini ishlab chiqish qoidalari”ga muvofiq tashkil etiladi.

4.3 Universitet xodimlari axborot aktivlaridan ish faoliyatiga oid maqsadlari uchun foydalanishga majburdirlar.

4.4 Axborot aktivlari foydalanuvchilari Reestrda ko‘rsatiladi.

4.5 Axborot aktivlariga kirish va ulardan foydalanish qoidalari ularning konfidensialligi, yaxlitligi va foydalana olishliligidan kelib chiqib belgilanadi.

4.6 Konfidensial toifadagi axborot aktivlariga kirish Universitet rahbariyati tomonidan alohida tasdiqlangan konfidensial ma’lumotlar bilan ishlashga ruxsat berilgan shaxslar ro‘yxatiga kiritilgan xodimlar tomonidan olinadi. Belgilangan kirishlar Siyosatning 11-ilovasi “Axborot manbalariga kirish matritsasini ishlab chiqish qoidalari”ga muvofiq shakllantiriladi.

4.7 Konfidensial ma’lumotlar toifasiga kiruvchi axborotlar mavjud bo‘lgan axborot aktivi to‘g‘risidagi ma’lumotlarni uchinchi shaxslarga tarqatish taqiqlanadi.

5. Axborot aktivlarining tasnifi

5.1 Universitetning ma’lumotlari axborot xavfsizligini ta’minlash bo‘yicha ishlarni tashkil etishning zaruriy elementi bo‘lgan, uni himoya qilish talablarini aniqlash uchun tasniflanadi.

5.2 Ma’lumotlarni va axborot hujjatlarini tasniflashda quyidagilar e’tiborga olinadi:

- axborot aktivlarining (ularning ma’lumotlari, vazifalari, ish joylari, serverlar, ish stansiyalar) mavjudligi, yaxlitligi yoki kirish toifalari buzilgan taqdirda ularni xavflilik darajasiga qarab tasniflash asosida ularni muhofaza qilishda differensial yondashuvning me’yoriy-uslubiy asoslari;
- qonunchilik talablari;

- axborot aktivining qiymati va ahamiyati.

5.3 Aktivlarning tasnifi, davriy ravishda qayta ko‘rib chiqilishi, shuningdek, uning dolzarbligini va tegishli darajada himoya qilinishini ta’minlash axborot aktivi egalari, Axborot xavfsizligi administratori hamda Departament boshlig‘i tomonidan ta’minlanadi.

5.4 Himoya darajasini konfidensiallik, yaxlitlik, foydalana olishlik va boshqa axborot talablarini tahlil qilish orqali baholash mumkin.

Universitetda saqlanadigan va qayta ishlanadigan har xil turdagi ma’lumotlarni himoya qilishning turli darajalarini ta’minlash zarurligidan kelib chiqib, shuningdek, boshqa tashkilotlarga yoki xodimlarga zarar yetkazilishining mumkin bo‘lgan usullarini hisobga olgan holda, kirish toifalari, yaxlitligi va mavjudligi himoyalangan axborot resurslari joriy etiladi.

5.5 Ma’lumotlarning belgilangan sinfiga muvofiq, axborot aktiviga tegishli kirish va uni himoya qilish darajasi tashkil etiladi.

6. Axborot aktivlarini tasniflashning asosiy tamoyillari

6.1 Kirish toifalari bo‘yicha axborot tizimlari va resurslari quyidagilarga bo‘linadi:

1) ochiq axborot resurslari (O) – cheksiz ko‘p foydalanuvchilar uchun mo‘ljallangan;

2) cheklangan kirish imkoniyatiga ega bo‘lgan axborot resurslari (K) – konfidensial ma’lumotlarni o‘z ichiga olgan va cheklangan miqdordagi foydalanuvchilar uchun mo‘ljallangan;

6.2 Konfidensial ma’lumotlar O‘zbekiston Respublikasi Vazirlar Mahkamasining 2011-yil 7-noyabrdagi “O‘zbekiston Respublikasi Prezidentining “Milliy axborot resurslarini muhofaza qilishga doir qo‘shimcha chora-tadbirlar to‘g‘risida” 2011-yil 8-iyuldagi PQ-1572-son qarorini amalga oshirish chora-tadbirlari haqida” 296-son qarori 2-ilovasiga muvofiq foydalanishi cheklangan ma’lumotlarni o‘z ichiga oladi.

6.3 Axborot va axborot resurslari quyidagi kirish toifalariga bo‘linadi:

1) to‘siqsiz foydalana olishlik (T) – har doim axborot resursidan foydalana olish mumkin (kutish vaqti bir necha soniya yoki daqiqadan oshmasligi kerak);

2) yuqori foydalana olishlik (Y) – vaqtincha kutishlarsiz axborot resursidan foydalana olish mumkin (kechikish vaqti bir necha soatdan oshmasligi kerak);

3) o‘rtacha foydalana olishlik (O‘) – belgilangan kechikish vaqti bilan axborot resursidan foydalana olish mumkin (kechikish vaqti bir necha kundan oshmasligi kerak);

4) quyi foydalana olishlik (Q) – vaqtinchalik kechikishlar bilan, ammo limit chegaralanmagan axborot resursining mavjudligi (natijasini olishdagi ruxsat etilgan kechikish — bir necha hafta).

6.4 Axborot va axborot resurslari himoyalangan ma’lumotlarning yaxlitligi quyidagi toifalariga bo‘linadi:

1) yuqori (Y) – axborot resurslarini ruxsatsiz o‘zgartirish yoki soxtalashtirish jiddiy zarar yetkazilishiga olib kelishi mumkin, uning yaxlitligi kafolatlangan uslublar (masalan, ERI vositasi) bilan qonunchilik talablariga ko‘ra ta’minlanishi kerak;

2) quyi (Q) – axborot resurslarini ruxsatsiz o‘zgartirish yoki soxtalashtirish kamroq ahamiyatli zarar yetkazilishiga olib kelishi mumkin, uning yaxlitligi kafolatlangan

uslublar, xesh-funksiya kabi vositalar bilan qonunchilik talablariga ko‘ra ta’minlanishi kerak;

3) hech qanday talab yo‘q (-) – da’vo talab etilmaydigan butunligi ta’minlanadigan axborot resurslari.

7. Himoyalangan ma’lumotlarni inventarizatsiya qilish tartibi

7.1 Axborot aktivlarini aniqlash, Reestrni yuritish va axborot aktivlarini tasniflash uchun Axborot xavfsizligi administratori hamda Departament boshlig‘i har yili bir marta Universitetdagi mavjud bo‘lgan axborot resurslarini inventarizatsiya qilish ishlarini tashkillashtiradi.

7.2 Axborot aktivlarini inventarizatsiya qilish jarayonida ushbu Tartibga muvofiq tasniflashning to‘g‘riligi, shuningdek, axborot aktivlari uchun belgilangan xavfsizlik sinfiga muvofiq ularni himoya qilish talablarining bajarilishi ham aniqlanadi.

7.3 Inventarizatsiya natijalari bo‘yicha Reestrga, shuningdek, Universitetning konfidensial ma’lumotlari ro‘yxatiga o‘zgartirish va qo‘shimchalar kiritilishi mumkin.

Shuningdek, inventarizatsiya natijalariga ko‘ra kamchilik aniqlansa, Universitetning axborot-kommunikatsiya texnologiyalarini joriy etish va raqamlashtirish bo‘yicha mas’ul rahbari kamchilik aniqlangan axborot aktivlari egalariga mavjud kamchiliklarni bartaraf etish to‘g‘risida ko‘rsatma beradi.

8. Aktivlarni markirovkalash

8.1 Universitet tomonidan qabul qilingan tasniflash tizimiga muvofiq, Universitetning axborot resurslariga axborotni qayta ishlash jarayonida markirovkalash qo‘llaniladi.

Markirovkalash jarayonlari axborot aktivlariga jismoniy va elektron shaklda qo‘llaniladi.

8.2 Axborot aktivlari ularning egasi tomonidan markirovkalanadi.

8.3 Fizik yorliqlar markalashning keng tarqalgan shakli hisoblanadi. Axborot aktivlari, xuddi elektron hujjatlar singari, jismoniy yorliq bilan belgilanishi mumkin emas, shuning uchun ekranlarda yoki displeylarda paydo bo‘lishi mumkin bo‘lgan bildirish yorliqlari kabi elektron yorliq vositalaridan foydalaniladi.

8.4 Yorliqda yoki markalashning elektron vositalarida axborot aktivining seriya raqami, konfidensiallik belgisi, shuningdek, axborot aktivi egasining qaroriga binoan boshqa ma’lumotlar ko‘rsatiladi.

8.5 Chop etilgan hisobotlar, ekran shakllari, axborot tashuvchilar (lentalar, disklar, kompakt-disklar, kassetalar), elektron xabarlar va uzatilgan fayllar belgilanishi kerak.

8.6 Belgilanishdan noo‘rin foydalanilgan taqdirda, axborotni tasniflash darajasini belgilashning boshqa vositalari qo‘llanilishi mumkin.

8.7 Axborot aktivini tasniflashning har bir darajasi uchun uning egasi axborot aktivini qayta ishlash va undan foydalanish tartibini, shu jumladan xavfsiz ishlash, saqlash, o‘tkazish va yo‘q qilishni belgilaydi.

Ushbu jarayon axborot aktividan foydalanuvchilar tomonidan bajarilishi kerak.

8.8 Axborot aktivini qayta ishlash va undan foydalanish tartibi, shuningdek, boshqa tashkilotlar bilan ma’lumot almashishni ta’minlaydigan shartnomalarga

kiritilishi kerak. Konfidensial axborot bilan xavfsiz ishlash ma’lumot almashish bo‘yicha kelishuvlarning asosiy talabidir.

9. Javobgarlik

9.1 Ma’lumot manbalari toifasiga qarab talab qilinadigan xavfsizlik darajasini belgilanishi (markirovkalash) uchun javobgarlik Axborot xavfsizligi administratori hamda Departament boshlig‘i zimmasiga yuklanadi.

9.2 Ushbu Tartib talablarining buzilishi Universitetning ichki mehnat qoidalari hamda O‘zbekiston Respublikasining mehnat qonunchiligiga muvofiq intizomiy javobgarlikka tortishga sabab bo‘ladi.

Axborot aktivlarini boshqarish tartibiga ilova

Universitetning axborot resurslari REESTRI

T/r	Resurs nomi	Resurs tavsifi	Joylashishi	Formati	Konfidensiallik	Yaxlitlik	Foydalana olishlilik	Yangilash davriyligi	Resurs foydalanuvchilari	Egasi
1.	buxdu.uz	Universitet faoliyatini internetda yoritib borish uchun mo‘ljallangan	Arsenal-D	Raqamli	O	Y	Y	Doimiy	Universitet xodimlari va internet foydalanuvchilari	Raqamli ta’lim texnologiyalar departamenti Universitet matbuot xizmati
2.	Onlayn o‘qitish tizimi (moodle.buxdu.uz)	Ushbu tizim talabalarni onlayn o‘qitish uchun qo‘llaniladi	Universitet bosh binosidagi serverda	Raqamli	O	Y	Y	Doimiy	Universitet xodimlari va internet foydalanuvchilari	Raqamli ta’lim texnologiyalar departamenti O‘quv-uslubiy departament
3.	Oliy ta’lim jarayonlarini boshqarish axborot tizimi (hemis.buxdu.uz)	Oliy ta’lim jarayonlarini boshqarish axborot tizimi	Universitet bosh binosidagi serverda	Raqamli	K	Y	Y	Doimiy	Universitet xodimlari va internet foydalanuvchilari	Raqamli ta’lim texnologiyalar departamenti O‘quv-uslubiy departament
4.	Masofaviy o‘qitish tizimi (masofaviy.buxdu.uz)	Ushbu tizim talabalarni masofaviy o‘qitish uchun qo‘llaniladi	Universitet bosh binosidagi serverda	Raqamli	O	Y	Y	Doimiy	Universitet xodimlari va internet foydalanuvchilari	Raqamli ta’lim texnologiyalar departamenti O‘quv-uslubiy departament

T/r	Resurs nomi	Resurs tavsifi	Joylashishi	Formati	Konfidensiallik	Yaxlitlik	Foydalana olishlilik	Yangilash davriyligi	Resurs foydalanuvchilari	Egasi
5.	Oliy ta’lim jarayonlarini boshqarish axborot tizimi talabalar uchun (student.buxdu.uz)	Oliy ta’lim jarayonlarini boshqarish axborot tizimi	Universitet bosh binosidagi serverda	Raqamli	K	Y	Y	Doimiy	Universitet xodimlari va internet foydalanuvchilari	Raqamli ta’lim texnologiyalar departamenti O‘quv-uslubiy departament
6.	uniwork.buxdu.uz	Raqamli universitet tizimi	Universitet bosh binosidagi serverda	Raqamli	K	Y	Y	Doimiy	Universitet xodimlari va talabalar	Raqamli ta’lim texnologiyalar departamenti
7.	Universitetning “Comparative linguistics, translation and literary studies” jurnali sayti (citrus.buxdu.uz)	Xorijiy tillar fakultetining “Comparative linguistics, translation and literary studies” jurnaliga maqola qabul qilish hamda chop etish tizimi	Arsenal-D	Raqamli	O	Y	Y	Doimiy	Universitet xodimlari va internet foydalanuvchilari	Raqamli ta’lim texnologiyalar departamenti Tahririy-nashriyot bo‘limi
8.	Professor-o‘qituvchilar tomonidan ilmiy jurnallarda chop etilgan maqolalarni kiritish tizimi (journal.buxdu.uz)	Universitet Professor-o‘qituvchilari tomonidan ilmiy jurnallarda chop etilgan maqolalarni joylashtirish tizimi	Arsenal-D	Raqamli	O	Y	Y	Doimiy	Universitet xodimlari va internet foydalanuvchilari	Raqamli ta’lim texnologiyalar departamenti Ilmiy tadqiqot va innovatsion faoliyatni rivojlantirish departamenti

T/r	Resurs nomi	Resurs tavsifi	Joylashishi	Formati	Konfidensiallik	Yaxlitlik	Foydalana olishlilik	Yangilash davriyligi	Resurs foydalanuvchilari	Egasi
9.	“Buxoro davlat universiteti ilmiy axboroti” ilmiy jurnali sayti (srep.buxdu.uz)	Universitet ilmiy maqolalar jurnali	Arsenal-D	Raqamli	O	Y	Y	Doimiy	Universitet xodimlari va internet foydalanuvchilari	Raqamli ta’lim texnologiyalar departamenti Tahririy-nashriyot bo‘limi
10.	Universitetning “Pedagogik mahorat” ilmiy-nazariy va metodik jurnal sayti (pedskills.buxdu.uz)	Universitet ilmiy maqolalar jurnali	Arsenal-D	Raqamli	O	Y	Y	Doimiy	Universitet xodimlari va internet foydalanuvchilari	Raqamli ta’lim texnologiyalar departamenti Tahririy-nashriyot bo‘limi
11.	Universitetning korporativ elektron pochta tizimi (mail.buxdu.uz)	Universitetning ishchi xodimlari, Professor-o‘qituvchilari, doktorant hamda magistrlari uchun korporativ elektron pochta tizimi	Arsenal-D	Raqamli	K	Y	Y	Doimiy	Universitet xodimlari va internet foydalanuvchilari	Raqamli ta’lim texnologiyalar departamenti
12.	Fayl serverlar	Universitet xodimlari o‘rtasida hujjat (fayl) almashish uchun mo‘ljallangan	Universitet bosh binosidagi serverda	Turli xil elektron formatda	K	-	Y	Zarurat tug‘il-ganda	Universitet xodimlari	Raqamli ta’lim texnologiyalar departamenti
13.	Ishchi stansiyalar	Universitet xodimlariga biriktirilgan o‘z xizmat faoliyatini olib	Universitet binosida	Raqamli	K	Y	T	Zarurat tug‘ilgan-da	Universitet xodimlari	Raqamli ta’lim texnologiyalar departamenti

T/r	Resurs nomi	Resurs tavsifi	Joylashishi	Formati	Konfidensiallik	Yaxlitlik	Foydalana olishlilik	Yangilash davriyligi	Resurs foydalanuvchilari	Egasi
		boradigan ishchi stansiyalar								
14.	Server uskunalari	Universitetning axborot resurslari va tizimlarining asosiy kommutatsiya uskunalari va server uskunalari uchun ajratilgan joy	Universitet binosining 2-qavatida	Raqamli	K	Y	T	Zarurat tug‘ilgan-da	Universitet xodimlari	Raqamli ta’lim texnologiyalar departamenti
15.	Ichki telefon tarmog‘i	Apparat-dasturiy kompleks asosida qurilgan IP telefoniya tizimi	Universitet server xonasida	Raqamli	O	Y	O‘	Zarurat tug‘ilganda	Universitet xodimlari	Raqamli ta’lim texnologiyalar departamenti
16.	Kirish chiqishni nazorat qilish tizimi	Universitet binosiga kirish chiqishlarni nazorat qilish tizimi	binoning kirish qismida	Raqamli	K	Y	Y	Zarurat tug‘ilganda	Inson resurslarini boshqarish departamenti	Raqamli ta’lim texnologiyalar departamenti
17.	Videokuzatuv tizimi	Universitet hududidagi mavjud kameralarni ro‘yxatga olish, online kuzatuv jarayonlarini tashkil etish, fakultet rahbarlari, bo‘lim va departament	Arsenal-D, Universitet bosh binosidagi serverda	Raqamli	O	Y	Y	Doimiy	Universitet xodimlari va internet foydalanuvchilari	Raqamli ta’lim texnologiyalar departamenti

T/r	Resurs nomi	Resurs tavsifi	Joylashishi	Formati	Konfidensiallik	Yaxlitlik	Foydalana olishlilik	Yangilash davriyligi	Resurs foydalanuvchilari	Egasi
		boshliqlari uchun alohida sahifa orqali o‘quv jarayonlarini kuzatish hamda universitetda bo‘lib o‘tadigan ijodiy imtihonlarni onlayn ko‘rish tizimi								

Konfidensiallik darajasi: K, O;
Yaxlitlik: Y, Q, – hech qanday talab yo‘q ;
Foydalana olishlilik: T, Y, O‘, Q;
Foydalanuvchilar: Kirish matritsasi asosida resurs bilan ishlash huquqiga ega bo‘lgan xodimlar;
Egasi: Resursga javobgar.

Universitet axborot xavfsizligi
siyosatiga 15-ilova

Axborotni texnik himoya qilishni tashkil etish bo‘yicha YO‘RIQNOMA

1. Umumiy qoidalar

1.1 Ushbu Yo‘riqnomada axborotni texnik himoya qilishning asosiy chora-tadbirlari, usullari va vositalari, Universitetda ma’lumotlarini himoya qilish tizimiga kiritilgan foydalanuvchilar va mansabdor shaxslarning majburiyatlarini belgilaydi.

1.2 Ushbu Yo‘riqnomaning talablari Universitetda foydalanish uchun majburiydir.

1.3 Axborotni ishonchli himoya qilishni tashkil etish va ta’minlash Universitetning axborot xavfsizligini ta’minlash masalalari bo‘yicha mas’ul xodimi (keyingi o‘rinlarda – Axborot xavfsizligi administratori) hamda Raqamli ta’lim texnologiyalari departamenti (keyingi o‘rinlarda – Departament) boshlig‘ining eng muhim vazifalaridan biridir.

1.4 Axborotni ishonchli himoya qilishni ta’minlash Departamentning Tarmoqlarni boshqarish va texnik qo‘llab-quvvatlash sektori bosh mutaxassisi (keyingi o‘rinlarda – Lokal tarmoq administratori) hamda Departament xodimlarining eng muhim vazifalaridan biridir.

2. Asosiy tushunchalar

2.1 Ushbu Yo‘riqnomada quyidagi atamalar va ta’riflar qo‘llaniladi:

2.1.1 **axborotni texnik himoya qilish vositalari** – axborotning hayotiy siklining barcha bosqichlarida (axborotni yaratish, uzatish, qabul qilish, o‘zgartirish, namoyish qilish va saqlash) xavfsizlikni ta’minlaydigan apparat, apparat-dasturiy yoki dasturiy ta’minot.

2.1.2 **axborotni texnik muhofaza qilish** – muhandislik va kriptografik bo‘lmagan usullardan foydalangan holda axborot xavfsizligini ta’minlashga qaratilgan faoliyat.

3. Axborotni texnik himoya qilishni tashkil etish tartibi va majburiyatlari

3.1 Axborotni texnik himoyalashni tashkil etish Axborot xavfsizligi administratori hamda Departament boshlig‘i tomonidan ta’minlanadi.

3.2 Axborotni texnik himoyalashni ta’minlash Universitetda Lokal tarmoq administratori hamda Departament xodimlari tomonidan amalga oshiriladi.

3.2.1 Axborotni texnik himoyalashni tashkil etish bo‘yicha Axborot xavfsizligi administratori hamda Departament boshlig‘ining vazifalariga quyidagilar kiradi:

- axborotni texnik himoyasini ta’minlash va axborotni himoya qilish tizimini tashkil etish bo‘yicha talablarni ishlab chiqish;
- axborot xavfsizligi tizimini rivojlantirish va axborot xavfsizligi texnik vositalarini joriy etish rejalarini tayyorlash va amalga oshirish;

- axborotni texnik himoya qilish vositalariga talablarni ishlab chiqish, ularni sotib olishni, amalga oshirishni va foydalanishga topshirishni tashkil etish;

- axborot xavfsizligi tizimi va unga kiritilgan texnik axborot xavfsizligi vositalarining uzluksiz ishlashini tashkil etish.

3.3 Konfidensial axborotlarni texnik muhofaza qilishni tashkil etish O‘zbekiston Respublikasi Vazirlar Mahkamasining 2015-yil 16-oktyabrdagi “O‘zbekiston Respublikasi axborotlashtirish obyektlarida konfidensial axborot xavfsizligini tashkil etish va ta’minlash tartibi to‘g‘risidagi Nizomni tasdiqlash to‘g‘risida” 295-son qarori talablariga muvofiq ta’minlanishi kerak.

3.4. O‘zbekiston Respublikasi Vazirlar Mahkamasining 2015-yil 16-oktabrdagi “O‘zbekiston Respublikasi axborotlashtirish obyektlarida konfidensial axborot xavfsizligini tashkil etish va ta’minlash tartibi to‘g‘risidagi Nizomni tasdiqlash to‘g‘risida” 295-son qaroriga binoan Axborot xavfsizligi administratori va Departament boshlig‘i quyidagi bosqichlarda axborotni muhofaza qilish tizimini yaratadi (modernizatsiya qiladi):

- loyihalashdan oldingi ekspertiza, himoya tizimini yaratish (modernizatsiya qilish) zarurati asoslarini ishlab chiqish;

- axborot xavfsizligi tizimini loyihalash (loyihalarni ishlab chiqish) va amalga oshirish;

- xavfsizlik vositalarini ekspluatatsiya va qabul sinovlarini o‘tkazgan holda, axborot xavfsizligi tizimini ishga tushirish.

Loyiha oldidan o‘tkazilgan so‘rov natijalariga ko‘ra, axborot xavfsizligi tizimini rivojlantirish bo‘yicha texnik topshiriq ishlab chiqish.

Himoya tizimini loyihalashtirish va amalga oshirish bosqichida texnik loyihani ishlab chiqish, tashkiliy-texnik tadbirlarni ishlab chiqish, axborot xavfsizligini ta’minlash vositalarini sotib olish va ularni o‘rnatish, agar kerak bo‘lsa, axborot xavfsizligini ta’minlash uchun dasturiy ta’minotni ishlab chiqish amalga oshiriladi.

Axborotni muhofaza qilish tizimini ishga tushirish bosqichida sinovdan o‘tkazish, axborotni muhofaza qilish bo‘yicha texnologik jarayonlarni ishlab chiqish, qabul qilish sinovlari o‘tkaziladi.

3.5 Ushbu Yo‘riqnomada ko‘rsatilgan ma’lumotlarni texnik muhofaza qilish choralari va vositalarini amalga oshirish va axborot xavfsizligi tizimini rivojlantirish maqsadida Axborot xavfsizligi administratori Departament boshlig‘i bilan birgalikda axborot xavfsizligini ta’minlash bo‘yicha yillik tadbirlar rejalarini, shu jumladan sotib olish, o‘rnatish, sozlash, axborotni texnik muhofaza qilish vositalarini sinovdan o‘tkazish va ishga tushirish ishlarini amalga oshiradi.

3.6 Axborot xavfsizligi administratori hamda Departament boshlig‘ining dolzarb vazifalariga quyidagilar kiradi:

- axborot xavfsizligi tizimini rivojlantirish va texnik axborot xavfsizligini ta’minlash bo‘yicha rejalarni amalga oshirish;

- axborotni himoya qilishning texnik vositalarini joriy etish va ulardan foydalanishni tashkillashtirish.

3.7 Axborotni himoya qilish bo‘yicha texnik choralar quyidagi asosiy yo‘nalishlarda amalga oshirilishi kerak:

- tarmoq xavfsizligi;

- zararli dasturlardan ma’lumotlarni himoya qilish;
- ruxsatsiz kirishdan himoya qilish;
- texnik kanallar orqali ma’lumot tarqalishidan himoya qilish.

3.8 Universitetning axborot infratuzilmasining barcha tarkibiy qismlari, axborot resurslari texnik jihatdan muhofaza qilinadi.

3.9 Universitetda axborot xavfsizligi tizimini yaratishda axborot xavfsizligining texnik usullarini joriy etish inobatga olinadi.

4. Axborotni texnik himoya qilishda foydalanilgan usullar va vositalar

4.1 Tarmoq xavfsizligi

4.1.1 Universitetning mavjud tarmoqlarida ma’lumotni texnik himoya qilish vositalariga tarmoqlararo ekran va proksi-server vositalari kiradi.

4.1.2 Ushbu vositalar sifatida Universitetda “Kerio Control”, “FortiGate” yordamida amalga oshiriladi.

4.1.3 Universitetda Lokal tarmoq administrator hamda Departament xodimlari tomonidan tarmoqlararo ekrandan foydalanish bo‘yicha quyidagi choralar ko‘riladi:

- lokal tarmoqning internet tarmog‘iga ulanishi chegarasida tarmoqlararo ekran apparat va dasturiy ta’minoti o‘rnatiladi;
- xodimlarning internet tarmog‘iga chiqishi yoki internet tarmog‘idan ma’lumotlarni qabul qilishida tarmoqlararo ekran orqali foydalanishda uzatilayotgan ma’lumotlarning xavfsizligini saqlash choralarini ko‘radi;
- tarmoqlararo ekranga kiritilgan siyosatlarni doimiy yangilab boradi;
- tarmoqni virusli dasturlardan himoyalashni ta’minlaydi.

4.1.4 Tarmoqlararo ekran apparat vositalari sozlamalarida keraksiz tarmoq trafigini filtrlash uchun URL filtri, spam-filtr va zararli dasturlar uchun trafikni boshqarish vositalaridan foydalanish kerak.

4.2 Zararli dasturlardan himoya

4.2.1 Zararli dasturlardan, shu jumladan kompyuter viruslari, troyan va josuslik dasturlari va boshqalardan himoya qilish uchun quyidagi choralar ko‘rilishi kerak:

- zararli dasturlarga qarshi vositalardan (antiviruslar) foydalanish;
- xavfsizlik darajasini oshirish uchun veb-brauzerlarni sozlash, jumladan, ochilgan oynalarni va veb-reklamalarni blokirovka qilish, zararli yoki shubhali kontentni yuklab olishda ogohlantirish, veb-saytlar uchun xavfsiz ko‘rish rejimidan foydalanish va h.k..
- axborotga ishlov berish, saqlash va uzatish vositalarini ishlatilishidan oldin antivirusdan himoya qilish vositasida viruslar mavjudligini tekshirish;
- serverlarda va ish stansiyalarida tashuvchi vositalardan foydalanishni cheklash;
- kiruvchi elektron pochta xabarlarini antivirus himoyasi yordamida skanerlash;
- kontentni filtrlash va proksi-serverlar (tarmoqlararo ekran) yordamida zararli saytlarga kirishni blokirovka qilish;
- foydalanuvchilarning ish stansiyalariga ruxsat etilmagan dasturlarni foydalanuvchilar tomonidan o‘rnatishni taqiqlash va anonimayzerlardan foydalanishni cheklash choralarini qo‘llash.

4.2.2 Virusga qarshi himoya ESET Endpoint hamda boshqa dasturiy ta’minotlardan foydalangan holda ta’minlanadi.

Antivirusdan himoya qilish obyektlari: Universitet binosida foydalanishdagi ish stansiyalari, mobil qurilmalar va serverlar.

4.2.3 Antivirusdan himoya vositalarini boshqarish Universitetda Lokal tarmoq administratori hamda Departament xodimlari tomonidan amalga oshiriladi.

4.2.4 Antivirus himoyasi Siyosatning 9-ilovasidagi “Antivirus himoyasi bo‘yicha yo‘riqnoma”ga muvofiq tashkil qilinishi va ta’minlanishi kerak.

4.3 Ruxsatsiz kirishdan himoyalash

4.3.1 Ruxsatsiz kirishdan himoya qilishning quyidagi texnik usullarini ta’minlashi kerak:

- ruxsatsiz jismoniy harakatlar yoki kirishning oldini oluvchi yoki to‘sib qo‘yadigan muhandislik himoya vositalaridan (eshiklar, devorlar, shiftlar, deraza panjaralari, to‘siqlar va boshqalar) qulflar bilan jihozlangan (mexanik, elektromexanik, elektron), tamg‘alardan foydalanish;
- axborotga ishlov berish, saqlash va uzatishda foydalanadigan vositalari tashqi korpuslarida bir marta ishlatiladigan, muhrlar, yopishqoq lentalar yoki gologramma yorliqlardan foydalanish;
- server xonalarida signalizatsiya va videokuzatuv tizimini o‘rnatish;
- axborotga, tarmoqqa, axborot resurslariga kirishda autentifikatsiya vositalaridan foydalanish.

4.3.2 Tarmoq resurslari (fayl server, printerlar, ish stansiyalari va boshqalar), xizmatlarga (korporativ elektron pochta va h.k.) kirishni boshqarish, chegaralash hamda foydalanuvchilar va ish stansiyalarining hisobini yuritish Active Directory xizmati orqali amalga oshiriladi.

4.3.3 Tarmoq resurslariga kirishni boshqarish Domen serverida amalga oshiriladi, uning konfiguratsiyasi Universitetda Lokal tarmoq administratori hamda Departament xodimlari tomonidan ta’minlanadi.

4.3.4 Universitetda axborotlashtirish obyektlariga kirishni nazorat qilish, chegaralash va boshqarish tizimi Siyosatning 8-ilovasi “Parolli himoya bo‘yicha yo‘riqnoma”da keltirilgan talablar asosida tashkil etilishi kerak.

4.3.5 Axborot resurslariga kirishlarni Siyosatning 11-ilovasi “Axborot manbalariga kirish matritsasini ishlab chiqish qoidalari”da keltirilgan talablar asosida amalga oshirilishi kerak.

4.4 Texnik kanallar orqali ma’lumotlarning sizib chiqishidan himoya qilish

4.4.1 Texnik kanallar orqali ma’lumot sizib chiqishidan himoya qilishning asosiy usullari quyidagilardan iborat:

- axborotni uzatish, qayta ishlash va saqlashda sertifikatlangan texnik vositalar va tizimlardan foydalanish;
- qo‘riqlanadigan obyektni uning chegaralaridan maksimal darajada masofada boshqariladigan hududga joylashtirish;
- qo‘riqlanadigan binolar ro‘yxati va ulardan foydalanish uchun javobgar shaxslar haqidagi ma’lumotlarni to‘liq hujjatlashtirilishi;

- zarurat tug‘ilganda nutq signalini faol himoya qilish vositalaridan foydalanish (shovqin generatorlari);

— himoyalangan xonalarni jihozlash bo‘yicha tavsiya etilgan tadbirlarni amalga oshirish: devorlar, pollar va shiftlar boshqa tashkilotlarning binolari yonida bo‘lmasligi derazalar esa pardalar bilan yopilgan bo‘lishi kerak;

- ma’lumotlarning sizib chiqishi texnik kanallari mavjudligini aniqlash uchun binolarda maxsus tekshirishlar o‘tkazish;

- yong‘in va qo‘riqlash signalizatsiya tizimining bitta qo‘riqlanadigan boshqariladigan zonasida joylashtirish va boshqaruv paneli bilan simli aloqa;

- muhofaza qilinadigan binolarning atrofidagi inshootlarning, ularning shamollatish va muhofaza qilinadigan bino tashqarisidagi undagi suhbatlarni tinglash imkoniyati yo‘qligini ta’minlash;

- muhofaza qilinadigan binolarning atrofidagi inshootlar, muhandislik kommunikatsiyalari tashqarisiga begona (g‘ayritabiiy) narsalarni o‘rnatish imkoniyatini istisno qilish, vibroakustik kanallar orqali ma’lumotni ushlab qolish ehtimolini kamaytirish.

4.4.2 Universitet joylashgan binoda texnik kanallar orqali ma’lumotlarni himoya qilish choralarini amalga oshirishni tashkil etish va nazorat qilish Axborot xavfsizligi administratori hamda Departament boshlig‘i tomonidan amalga oshiriladi.

4.4.3 Universitetning axborot tizimlari joylashgan binolarida texnik kanallar orqali ma’lumotlarni himoya qilish choralarini amalga oshirishni tashkil etish va nazorat qilish Departament boshlig‘i tomonidan amalga oshiriladi.

4.4.4 Konfidensial ma’lumotlarni axborot-kommunikatsiya tizimidan chiqib ketishidan himoya qilish uchun, DLP konfidensial ma’lumotlarning chiqib ketishini oldini olish tizimlaridan foydalanishni tashkil etish Axborot xavfsizligi administratori hamda Departament boshlig‘ining ustuvor vazifalaridan biri hisoblanadi.

4.5 Ish faoliyatini nazorat qilish

4.5.1 Asosiy himoya obyektlarining (server qurilmalari, tarmoq qurilmalari, aloqa kanallari) ishlash holatini kuzatib borish uchun Universitet kecha-kunduz ishlaydigan va himoya obyektlarining ishlashini kuzatish imkonini beradigan tizimni yaratadi, shuningdek, mazkur tizimdan maqsadli foydalanishni tashkil etadi.

4.5.2 Ish faoliyati monitoringi tizimi, shu jumladan monitoring monitorlari Universitet bosh binosida joylashadi.

4.5.3 Ish samaradorligini kuzatish tizimining ishlashi va texnik ta’minoti Departament xodimlari tomonidan ta’minlanadi.

5. Axborotni texnik himoya qilish choralari va vositalarini qo‘llash

5.1 Texnik axborot xavfsizligi vositalarining uzluksiz ishlashi Lokal tarmoq administratori hamda Departament xodimlari tomonidan Siyosat talablariga muvofiq amalga oshiriladi.

5.2 Axborotni muhofaza qilishning texnik va dasturiy vositalarini ishlatish bo‘yicha yo‘riqnomalar Axborot xavfsizligi administratori hamda Departament boshlig‘i tomonidan Universitetda qo‘llaniladigan va foydalaniladigan har bir texnik

himoya vositalariga nisbatan ishlab chiqiladi. Ushbu yo‘riqnomalarda vositalarni ishlab chiqaruvchilarning qo‘llanmalari va foydalanish bo‘yicha hujjatlarida keltirilgan talablar inobatga olinadi.

6. Javobgarlik

6.1 Axborot xavfsizligi administratori hamda Departament boshlig‘i ushbu Yo‘riqnomaga muvofiq axborotni texnik himoya qilish tadbirlarini amalga oshirilishining nazoratiga mas’uldirlar.

6.2 Ushbu Yo‘riqnomada belgilangan talablarning buzilishi Universitetning ichki mehnat qoidalari va O‘zbekiston Respublikasining mehnat qonunchiligiga muvofiq intizomiy javobgarlikka tortilishga olib keladi.

Universitet axborot xavfsizligi
siyosatiga 16-ilova

Axborotni kriptografik himoya qilishni tashkil etish bo‘yicha YO‘RIQNOMA

1. Umumiy qoidalar

1.1 Ushbu Yo‘riqnoma Universitetda axborotni kriptografik muhofaza qilishning asosiy chora-tadbirlarini, usullarini va vositalarini belgilaydi, shuningdek, axborotlarni kriptografik himoya vositalari sifatida ishlatiladigan elektron raqamli imzo (ERI) kalitlari bilan ishlashga vakolatli xodimlarining harakatlarini tartibga soladi.

1.2 Ushbu Yo‘riqnomaning talablari Universitetning barcha xodimlari uchun majburiydir.

1.3 Universitetda uzatilayotgan ma’lumotlarning yaxlitligini ta’minlashda kriptografik himoyalangan E-xat tizimidan foydalaniladi.

1.4 Uzatilayotgan axborotlarning kriptografik himoyasini ta’minlash, ushbu AKHVni ishlab chiquvchi va texnik qo‘llab-quvvatlovchi tashkilot zimmasiga yuklatiladi.

1.5 Universitetning axborot xavfsizligini ta’minlash masalalari bo‘yicha mas’ul xodimi (keyingi o‘rinlarda – Axborot xavfsizligi administratori) hamda Raqamli ta’lim texnologiyalari departamenti (keyingi o‘rinlarda – Departament) boshlig‘i tegishli bo‘linmalar bilan birgalikda E-xat tizimidan foydalangan holda axborotning kriptografik himoyasini tashkil etish bo‘yicha belgilangan talablarning bajarilishini nazorat qiladi.

1.6 Foydalaniladigan axborotlarni himoya qiluvchi kriptografik vositalar O‘zbekiston Respublikasi Prezidentining 2007-yil 3-apreldagi “O‘zbekiston Respublikasida axborotni kriptografik himoyasini tashkil etish chora-tadbirlari to‘g‘risida” PQ-614-son qaroriga muvofiq sertifikatlangan bo‘lishi shart.

2. Asosiy tushunchalar

2.1 Ushbu Yo‘riqnomada quyidagi atamalar va ta’riflar qo‘llaniladi:

2.1.1 **axborotni kriptografik himoya qilish** – kriptografik o‘zgartirish algoritmlari (kriptoalgoritmlar) yordamida amalga oshiriladigan axborotning yaxlitligini, erkinligini va konfidensialligini ta’minlashga qaratilgan chora-tadbirlar majmui;

2.1.2 **axborotni kriptografik himoya qilish vositalari (AKHV)** – axborotning xavfsizligini ta’minlash uchun axborotning kriptografik o‘zgartirilishini amalga oshiradigan apparat, dasturiy yoki apparat-dasturiy vositalar;

2.1.3 **kriptografik algoritm (kriptoalgoritm)** — ma’lumotlarni buzib ko‘rsatish va ruxsatsiz kirishdan himoya qilish maqsadida ma’lumotlarni (axborotni) o‘zgartirishning matematik algoritmi;

2.1.4 **kriptografik tizim** – (shifrlash tizimi, kriptotizim) axborotni kriptografik o‘zgartirish va/yoki boshqarish, shu jumladan, kriptografik kalitlarni tayyorlash

va taqsimlash jarayonini avtomatlashtirilgan boshqarishni ta’minlovchi tashkiliy, texnik va dasturiy vositalar jami;

2.1.5 **ruxsatsiz foydalana olish** – tizimda belgilangan foydalana olishni cheklash qoidalarini buzgan holda subyektning obyektdan yoki axborotdan foydalana olishi;

2.1.6 **shifrlash vositalari** – axborotni almashtirish kriptografik algoritmlarini amalga oshiruvchi va axborotni qayta ishlash, saqlash hamda aloqa kanallari bo‘ylab uzatishda uni ruxsatsiz foydalana olishdan muhofaza qilish uchun mo‘ljallangan apparat, dasturiy yoki apparat-dasturiy vositalar;

2.1.7 **imitomuhofaza vositalari** – axborotni kriptografik almashtirish algoritmlarini amalga oshiruvchi va yolg‘on axborotni majburan qabul qildirishdan muhofaza qilish uchun mo‘ljallangan apparat, dasturiy va apparat-dasturiy vositalar;

2.1.8 **kodlash vositalari** – almashtirishning bir qismini qo‘l operatsiyalari yordamida bajargan holda axborotni kriptografik almashtirish algoritmlarini amalga oshiruvchi vositalar;

2.1.9 **shifrlash** – kriptografik algoritmga va ma’lumotlarning haqiqiy tarkibini ishonchli yashirish uchun kalitga muvofiq ma’lumotlarning (axborotlarning) qayta tiklanadigan o‘zgarishlari to‘plami.

3. Axborotning kriptografik himoyasini tashkil etish tartibi

3.1 Universitetda kriptografik axborotni himoya qilishni tashkil etish Axborot xavfsizligi administratori hamda Departament boshlig‘i tomonidan ta’minlanadi. Shu maqsadda ular quyidagilarni hamkorlikda amalga oshiradi:

- Universitetda kriptografik himoyani ta’minlash va kriptografik axborotni himoya qilish vositalaridan foydalanish bo‘yicha talablar ishlab chiqadi;
- kriptografik tizimni rivojlantirish bo‘yicha rejalar tayyorlaydi;
- AKHVga talablar ishlab chiqadi, ularni sotib olish, joriy etish, ishga tushirish va sertifikatlashtirishni tashkil etadi.

3.2 Ushbu Yo‘riqnomada ko‘rsatilgan ma’lumotlarni kriptografik himoya qilish choralari va vositalari Axborot xavfsizligi administratori hamda Departament boshlig‘i tomonidan belgilanadi va Departamentning Tarmoqlarni boshqarish va texnik qo‘llab-quvvatlash sektori bosh mutaxassisi (keyingi o‘rinlarda – Lokal tarmoq administratori) hamda Departament xodimlari tomonidan amalga oshiriladi.

Ularni amalga oshirish uchun axborot xavfsizligini ta’minlash bo‘yicha yillik tadbirlar rejalari, shu jumladan AKHVlarini joriy etish, ulardan foydalanish bo‘yicha chora-tadbirlar ishlab chiqiladi.

3.3 AKHVni ishlashi Universitet xodimlari tomonidan ushbu AKHV ishlab chiquvchilaridan foydalanish bo‘yicha ko‘rsatmalarga muvofiq amalga oshiriladi.

3.4 AKHVni ishlatish bo‘yicha Yo‘riqnoma Axborot xavfsizligi administratori hamda Departament boshlig‘i tomonidan xodimlarga yetkaziladi.

4. Kriptografik axborotni himoya qilish usullari va vositalari

4.1 Universitetda ma’lumotlarning AKHV orqali himoyalangan uzatilishini ta’minlash maqsadida AKHVdan E-xat tizimidan foydalaniladi.

4.2 E-xat tizimidan foydalanuvchi xodimlar ro‘yxati Universitetning axborot-kommunikatsiya texnologiyalarini joriy etish va raqamlashtirish bo‘yicha mas’ul rahbari tomonidan belgilanadi.

4.3 E-xat tizimining foydalanuvchilariga tizimdagi raqamli imzolar asosida foydalanuvchilarning autentifikatsiyasini, kirish va uzatilayotgan ma’lumotlarni shifrlash, shuningdek, uzatish jarayonida uning yaxlitligini ta’minlash uchun raqamli imzoni shakllantirishni ta’minlaydigan ERI kalitlar beriladi.

4.4 Soliq va bank xizmatlaridan foydalanish va tegishli hisobotlarni taqdim etish va olish uchun soliq va bank muassasalari tomonidan taqdim etilgan ERIlardan foydalaniladi.

Mazkur kalitlardan foydalanish (qabul qilish, yangilash, xavfsiz saqlash, bekor qilish va boshqa harakatlar) Buxgalteriya bosh buxgalteri zimmasiga yuklatilgan.

4.5 Ish faoliyatida foydalaniladigan ERI kalitlari, shuningdek, ERI ochiq kalitlari sertifikatlari Universitet xodimlari bo‘lgan E-xat tizimi foydalanuvchilariga himoyalangan USB tashuvchida Axborot xavfsizligi administratori hamda Departament boshlig‘i tomonidan beriladi.

Yaratilgan ERI kalitlar Universitet xodimlari bo‘lgan Edo.ijro.uz va E-xat tizimlari foydalanuvchilariga “UNICON.UZ” DUK bilan tuzilgan shartnoma asosida beriladi.

4.6 E-xat tizimida “UNICON.UZ” DUKning kriptografik himoyalashga asoslangan dasturiy ta’minotidan foydalaniladi. Ushbu kalitlar O‘zMSt 285:2024 va O‘zMSt 286:2024 davlat standartiga muvofiq uzatiladigan ma’lumotni kriptografik shifrlashni ta’minlaydi. AKHV himoyalangan USB tashuvchiga o‘rnatiladi, bu ERI shakllanishi va tekshirilishini, shuningdek, tizim foydalanuvchilari ish stansiyasiga ulanganda shifrlashni ta’minlaydi.

4.7 Axborot xavfsizligi administratori hamda Departament boshlig‘i tomonidan AKHVdan Universitet veb-resurslariga ulanishlarda HTTPS va SSL/TLS protokollaridan foydalangan holda doimiy ravishda himoyalangan ulanishlar tashkil etildi.

4.8 Axborot xavfsizligi administratori tomonidan AKHVdan Universitet rasmiy veb-saytigan ulanishda https va SSL/TLS protokollaridan foydalangan holda himoyalangan ulanishlarida tashkil etilgan.

Rasmiy veb-saytni autentifikatsiya qilish uchun ishonchli markaz tomonidan Universitetga berilgan TLS sertifikati va bunda SHA-256 va Curve-25519 kriptografik algoritmlaridan foydalanilgan.

Rasmiy veb-saytga ulanish AES-256 kriptografik shifrlash algoritmidan foydalangan holda TLS 1.2 protokoli yordamida himoyalangan.

4.9 SSL sertifikatlarining o‘z vaqtida yangilanishi ustidan nazorat Universitet rahbariyati tomonidan amalga oshiriladi. Shu maqsadda Axborot xavfsizligi administratori ushbu Yo‘riqnomaning 2-ilovasiga muvofiq shaklda SSL sertifikatlarini yangilash jurnalini yuritadi.

5. Axborotni kriptografik himoya vositalarini qo‘llash

5.1 Universitetda Lokal tarmoq administratori hamda Departament xodimlari tomonidan E-xat tizimining mijoz dasturlari xodimlarining ish stansiyalariga o‘rnatiladi va sozlanadi.

Shuningdek, Axborot xavfsizligi administratori hamda Departament boshlig‘i Universitetda E-xat tizimida ishlash uchun xodimlarning ERI kalitlardan foydalanishi ustidan nazoratni ta’minlaydi.

5.2 Universitetda qo‘llaniladigan AKHVlar belgilangan tartibda O‘zbekiston Respublikasida sertifikatlangan bo‘lishi kerak.

6. AKHVdan foydalanishda xodimlarning majburiyatlari

6.1 E-xat tizimida ERI kalitlar bilan ishlaydigan foydalanuvchilar quyidagilarga majbur:

- ERI kalitlarning xavfsizligini ta’minlash va ulardan foydalanilmasa, himoyalangan joylarda (seyflarda) saqlash;
- foydalanuvchi yo‘qligida yoki Edo.ijro.uz va E-xat tizimlarida ishlamayotganda ERI kalitlarni ish joyida qarovsiz qoldirmaslik;
- Universitetda Lokal tarmoq administratori hamda Departament xodimlarini ERI kalitning yo‘qolishi yoki o‘g‘irlanishi, ERI kalitning buzilishi, ERI kalit tashuvchisining shikastlanishi, tizimlarga kirishdagi muammolar to‘g‘risida xabardor qilish;
- ishdan bo‘shash yoki AKHV va ERI bilan bog‘liq vazifalarni bajarishdan ozod qilish paytida ERI kalit saqlash vositasini topshirish;
- berilgan ERI kalitlarni saqlash vositasidan boshqa maqsadlarda ishlatmaslik.

6.2 Ishdan chiqqan ERI kalitlar yoki ularning saqlash vositalari Axborot xavfsizligi administratoriga hamda Departament boshlig‘iga belgilangan tartibda almashtirish uchun qaytariladi.

6.3 Axborot xavfsizligi administratori hamda Departament boshlig‘i Universitet xodimlariga Edo.ijro.uz va E-xat tizimlarida ishlash uchun berilgan ERI kalitlarning hisobga olinishini ta’minlashi shart.

7. Javobgarlik

7.1 Lokal tarmoq administratori hamda Departament xodimlari ushbu Yo‘riqnomaga muvofiq axborotni kriptografik himoya qilish choralarini amalga oshirish uchun javobgardir.

7.2 ERI kalitlar bilan ishlaydigan Universitetning barcha xodimlari ushbu Yo‘riqnomani buzganliklari uchun shaxsan javobgar bo‘ladilar.

7.3 Axborot xavfsizligi administratori hamda Departament boshlig‘i ushbu Yo‘riqnoma talablarining Lokal tarmoq administratori hamda Departament xodimlari, shuningdek, Universitetning boshqa barcha xodimlari tomonidan bajarilishini nazorat qilishni ta’minlash uchun javobgardir.

7.4 Ushbu Yo‘riqnomada belgilangan talablarning buzilishi Universitetning ichki mehnat qoidalari va O‘zbekiston Respublikasining mehnat qonunchiligiga muvofiq intizomiy javobgarlikka tortilishga olib keladi.

Universitet axborot xavfsizligi
siyosatiga 17-ilova

Himoyalangan ma’lumotlarga ishlov berish TARTIBI

1. Umumiy qoidalar

1.1 Ushbu Tartib O‘zbekiston Respublikasi Vazirlar Mahkamasining 2015-yil 16-oktyabrdagi “O‘zbekiston Respublikasi axborotlashtirish obyektlarida konfidensial axborot xavfsizligini tashkil etish va ta’minlash tartibi to‘g‘risidagi Nizomni tasdiqlash to‘g‘risida” 295-son qarori va O‘zbekiston Respublikasi Bosh vazirining o‘rinbosari – Davlat sirlarini saqlash bo‘yicha idoralararo komissiya raisi tomonidan 2006-yil 5-dekabrda tasdiqlangan — tarqatilishi cheklangan ma’lumotlarga ega hujjatlar, fayllar va nashrlarni ro‘yxatga olish, ishlov berish va saqlash tartibi to‘g‘risidagi yo‘riqnomaga asosan ishlab chiqilgan.

2. Himoyalanadigan ma’lumotlar ro‘yxati

2.1 Quyidagilar himoya qilinadi va tarqatilmaydi:

- Universitetning konfidensial ma’lumotlari ro‘yxatiga kiritilgan, hujjatlashtirilgan axborotlar;
- axborot resurslarida saqlanadigan konfidensiallik darajasiga ega bo‘lgan axborot resurslari Siyosatning 14-ilovasida ko‘rsatilgan “Axborot aktivlarini boshqarish tartibi”ga muvofiq tegishli ma’lumotlar;
- tarqatilishi cheklangan konfidensial bo‘lmagan ma’lumotlarga ega bo‘lgan hujjatlar, fayllar va nashrlar.

2.2 Konfidensial ma’lumotlar ro‘yxati O‘zbekiston Respublikasi Vazirlar Mahkamasining 2011-yil 7-noyabrdagi “O‘zbekiston Respublikasi Prezidentining 2011-yil 8-iyuldagi PQ-1572-son Farmonini amalga oshirish chora-tadbirlari to‘g‘risida” 296-son qaroriga 2-ilovada belgilangan ma’lumotlarni shu jumladan, tijorat sirini tashkil etuvchi ma’lumotlar va shaxsga doir ma’lumotlarni o‘z ichiga oladi.

2.3 Universitetning konfidensial ma’lumotlari ro‘yxati O‘zbekiston Respublikasi Vazirlar Mahkamasining 2015-yil 16-oktyabrdagi “O‘zbekiston Respublikasida axborotlashtirish obyektlarida konfidensial ma’lumotlarni tashkil etish va xavfsizligini ta’minlash to‘g‘risidagi nizomni tasdiqlash to‘g‘risida” 295-son qarorida belgilangan tartibda tuzilishi kerak.

2.4 Universitetda konfidensial ma’lumotlar ro‘yxati maxsus ishchi guruh tomonidan shakllantiriladi. Ishchi guruh tomonidan konfidensial ma’lumotlar ro‘yxatini qayta ko‘rib chiqish uch yilda kamida bir marta amalga oshiriladi.

2.5 Konfidensial ma’lumotlarga murojaat qilishda ishchi guruh qonunchilik talablari va iqtisodiy maqsadga muvofiqligini hisobga olishi, shuningdek, ma’lumotlardan foydalanishdagi cheklovlar Universitet faoliyatiga sezilarli darajada xalaqit berishi mumkinligini hisobga olish kerak.

2.6 Universitetda konfidensial ma’lumotlarni tashkil etuvchi ma’lumotlar ro‘yxati, shuningdek, ushbu ro‘yxatga kiritilgan o‘zgartirishlar va qo‘shimchalar Rektor buyrug‘i bilan kuchga kiradi va ularga tegishli konfidensial ma’lumotlarni qayta ishlashga qabul qilingan Universitet xodimlariga Universitetning axborot xavfsizligini ta’minlash masalalari bo‘yicha mas’ul xodimi (keyingi o‘rinlarda – Axborot xavfsizligi administratori) hamda Raqamli ta’lim texnologiyalari departamenti (keyingi o‘rinlarda – Departament) boshlig‘i tomonidan yetkaziladi.

Universitetdagi konfidensial ma’lumotlar ro‘yxatini shakllantirishda Vazirlikning konfidensial ma’lumotlar ro‘yxatidan kelib chiqilishi inobatga olinadi.

2.7 Tarqatilishi cheklangan konfidensial bo‘lmagan ma’lumotni o‘z ichiga olgan hujjatlar, fayllar va nashrlar O‘zbekiston Respublikasi Bosh vazirining o‘rinbosari – Davlat sirlarini saqlash bo‘yicha idoralararo komissiya raisi tomonidan 2006-yil 5-dekabrda tasdiqlangan — tarqatilishi cheklangan ma’lumotlarga ega bo‘lgan hujjatlar, fayllar va nashrlarni hisobga olish, ishlov berish va saqlash tartibi to‘g‘risidagi yo‘riqnomaga muvofiq belgilanadi.

Tarqatilishi cheklangan ma’lumotlarga O‘zbekiston matbuot va axborot agentligi tomonidan e’lon qilinishi taqiqlangan ma’lumotlarning ro‘yxati, Universitet, vazirliklar va boshqa idoralarning ochiq matbuotda, radio va televizion ko‘rsatuvlarda e’lon qilinishi taqiqlangan ma’lumotlar ro‘yxati, shuningdek, oshkor qilinmagan ma’lumotlar, ochiq e’lon qilinishi O‘zbekiston Respublikasiga zarar yetkazishi mumkin bo‘lgan boshqa ma’lumotlar kiradi.

3. Himoyalanadigan ma’lumot bilan ishlashga qo‘yiladigan talablar

3.1 Universitetda konfidensial ma’lumotlar ro‘yxatini shakllantirish, yuritish va o‘z xodimlariga yetkazish ustidan nazorat Universitetning axborot-kommunikatsiya texnologiyalarini joriy etish va raqamlashtirish bo‘yicha mas’ul rahbari (keyingi o‘rinlarda – Mas’ul rahbar) tomonidan amalga oshiriladi.

3.2 Universitetning konfidensial ma’lumotlarini, shu jumladan axborot resurslarida himoya qilish bo‘yicha ishlarni tashkil etish va amalga oshirish, O‘zbekiston Respublikasi Vazirlar Mahkamasining 2015-yil 16-oktyabrdagi “O‘zbekiston Respublikasida axborotlashtirish obyektlarida konfidensial ma’lumotlarni tashkil etish va xavfsizligini ta’minlash to‘g‘risidagi nizomni tasdiqlash to‘g‘risida” 295-son qarori talablariga muvofiq amalga oshiriladi.

3.3 Universitetda konfidensial ma’lumotlar ro‘yxatiga kiritilgan konfidensial ma’lumotlarni tarqatmaslik ustidan nazoratni Axborot xavfsizligi administratori Departament boshlig‘i bilan hamkorlikda amalga oshiradi.

3.4 Universitetning axborot tizimlari va resurslarining konfidensiallik darajasi Siyosatning 14-ilovasida keltirilgan “Axborot aktivlarini boshqarish tartibi”ga muvofiq belgilanadi.

3.5 Universitetda konfidensial xarakterdagi ishlar olib boriladigan muhofaza qilinadigan binolarning ro‘yxati hujjatlashtirilishi va himoyalangan binolar to‘g‘risidagi ma’lumotlar axborotlashtirish obyekti pasportiga kiritilishi Axborot xavfsizligi administratori hamda Departament boshlig‘ining ustuvor vazifalaridan biri bo‘lishi lozim.

3.6 Konfidensial ma’lumotlar qayta ishlanadigan axborotlashtirish obyektlari O‘zbekiston Respublikasi Prezidentining 2011-yil 8-iyuldagi “Milliy axborot resurslarini himoya qilish bo‘yicha qo‘shimcha chora-tadbirlar to‘g‘risida” PQ-1572-son qaroriga muvofiq attestatsiyalanadi.

3.7 Matnli va grafik konfidensial ma’lumotlarni ko‘rishni istisno qilish maqsadida binolar tegishli vositalar bilan jihozlanishi kerak.

3.8 Konfidensial xarakterdagi muzokaralarni olib borishda va konfidensial ma’lumotlarni qayta ishlash uchun texnik vositalardan foydalanishda axborot xavfsizligiga tahdid manbalarini zararsizlantirish choralari ko‘riladi.

3.9 Axborot tizimining ishlashi davomida konfidensial ma’lumotlarning himoyasini ta’minlash uchun quyidagi asosiy talablarga rioya qilish kerak:

- axborot tizimida ishlaydigan shaxslarning (foydalanuvchi, xizmat ko‘rsatuvchi xodimlar) himoyalangan ma’lumotlariga kirish kirish uchun avtorizatsiya tizimida belgilangan tartibda amalga oshirilishi kerak;
- muhofaza qilinadigan axborotni qayta ishlash obyektlari joylashgan binoda faqat qayta ishlangan ma’lumotlarga ruxsat berilgan shaxslar bo‘lishi mumkin;
- boshqa profilaktika va ta’mirlash ishlarini olib borish uchun muhofaza qilinadigan Universitet binolariga boshqa shaxslarni qabul qilish faqat Mas’ul rahbarning ruxsati bilan amalga oshirilishi lozim.

3.10 Konfidensial ma’lumotlarga ega bo‘lgan axborot tizimida axborotni qayta ishlashning texnologik jarayonida ishlatiladigan barcha axborot tashuvchilar axborot tizimiga egalik qiladigan birlikda hisobga olinishi kerak.

Vaqtincha foydalanilmaydigan axborot tashuvchi vositalarini ruxsatsiz shaxslar kira oladigan joylarda saqlashga yo‘l qo‘yilmaydi.

3.11 Konfidensial ma’lumotlarni faqat boshqariladigan hudud ichida joylashgan ajratilgan lokal tarmoqlarda ishlash mumkin. Axborotlashtirish obyektlari masofaviy bo‘lganda, O‘zbekiston Respublikasida sertifikatlangan kriptografik ma’lumotlarni himoya qilish vositalaridan foydalanish kerak.

3.12 Axborot resurslarida mavjud bo‘lgan konfidensiallik darajasidagi ma’lumotlarni himoya qilish va tarqatmaslik uchun javobgarlik ularning egalari, Axborot xavfsizligi administratori hamda Departament boshlig‘iga yuklatiladi. Universitetning axborot resurslarida mavjud bo‘lgan konfidensial ma’lumotlarni himoya qilish va tarqatmaslik ustidan nazorat Axborot xavfsizligi administratori hamda Departament boshlig‘i tomonidan amalga oshiriladi.

3.13 Ushbu Tartibning 2.7-bandida ko‘rsatilgan tarqatilishi cheklangan konfidensial bo‘lmagan ma’lumotlarni o‘z ichiga olgan hujjatlar, fayllar va nashrlarda “XDFU” belgisi, hujjat va nashrlarda qo‘shimcha ravishda nusxalari soni qo‘yiladi.

3.14 “XDFU” belgisini qo‘yish zarurligini aniqlash ushbu Tartibning 2.7-bandiga ko‘ra shakllantirilgan ro‘yxatlar asosida amalga oshiriladi: hujjat bo‘yicha — ijrochi va hujjatni imzolagan shaxs, nashrda esa — muallif va nashrni nashrga tasdiqlovchi rahbar.

3.15 Tarqatilishi cheklangan ma’lumotlarni o‘z ichiga olgan hujjatlar, fayllar va nashrlar boshqa jurnallardan alohida jurnallarda ro‘yxatga olinishi kerak, unda nusxalar soni, hujjat varaqlari soni va hujjatga qo‘shimchalar ko‘rsatilishi kerak.

3.16 Qog‘ozda tarqatilishi cheklangan ma’lumotlar bo‘lgan hujjatlarni ularning ijrochilariga va ijrochilar o‘rtasida o‘tkazish ro‘yxatga olish va nazorat shakllarida imzolangan holda amalga oshiriladi.

3.17 Tarqatilishi cheklangan ma’lumotlarni o‘z ichiga olgan hujjatlar:

- belgilangan tartibda qonun hujjatlari talablariga muvofiq ta’minlangan, aloqa kanallari, kuryerlik aloqalari yoki kuryerlik uzatish xizmatlari orqali yuboriladi. Cheklangan tarqatish, kuryerlik xizmati yoki kuryer transferi to‘g‘risidagi rasmiy ma’lumotlarni o‘z ichiga olgan hujjatlar yuborilgan taqdirda, qalin qog‘ozdan qilingan konvertlar (paketlar) ishlatiladi. Bunday hujjatlarni yuborishda boshqaruv obyektlarining mas’ul ish yuritish bo‘limlari va tarkibiy bo‘linmalarning xodimlari ularni qog‘ozga oldindan o‘rab, keyin konvertlarga soladilar. Konvertning yuqori qismiga muhrning izi qo‘yiladi;
- seyflarda, qulflanadigan shkaflarda, javonlarda yoki stol tortmasida saqlanadi, bunda uchinchi shaxslarning hujjatlarga kirish huquqi bundan mustasno.

3.18 Takrorlangan hujjatlarni ro‘yxatga olish birma-bir amalga oshiriladi.

Tarqatilishi cheklangan hujjatlarning elektron nusxalari boshqa axborot tashuvchi vositalarga faqat Mas’ul rahbarning yozma ruxsati bilan o‘tkazilishi mumkin. Bunday holda, hujjatning elektron matnida “Xizmat doirasida foydalanish uchun” cheklovchi muhri va nusxasi raqami qo‘yiladi.

3.19 Tarqatilishi cheklangan ma’lumotlar bo‘lgan hujjatlar, fayllar va nashrlarni hisobga olish, takrorlash, saqlash, foydalanish, saqlash va yo‘q qilish uchun tanlash Universitet xodimlari tomonidan 2006-yil 5-dekabrda O‘zbekiston Respublikasi Bosh vazirining o‘rinbosari – Davlat sirlarini saqlash bo‘yicha idoralararo komissiya raisi tomonidan tasdiqlangan, tarqatilishi cheklangan ma’lumotlarga ega bo‘lgan hujjatlar, fayllar va nashrlarni ro‘yxatga olish, ishlov berish va saqlash tartibi to‘g‘risidagi yo‘riqnomaga muvofiq amalga oshiriladi.

3.20 “XDFU” belgisi bo‘lgan hujjatlar, fayllar va nashrlar bilan ishlovchi xodimlar ushbu Tartib va 2006-yil 5-dekabrda O‘zbekiston Respublikasi Bosh vazirining o‘rinbosari – Davlat sirlarini saqlash bo‘yicha idoralararo komissiya raisi tomonidan tasdiqlangan — tarqatilishi cheklangan ma’lumotlarga ega bo‘lgan hujjatlar, fayllar va nashrlarni ro‘yxatga olish, ishlov berish va saqlash tartibi to‘g‘risidagi yo‘riqnoma bilan tanishishlari kerak.

3.21 Universitetning tarkibiy bo‘linmalari rahbarlari va tegishli mansabdor shaxslar hujjatlar, fayllar va nashrlarning “XDFU” belgisi bo‘lgan ma’lumotlarning to‘g‘ri saqlanishini, nusxalanishi va ishlatilishini, hujjatlar, fayllar va nashrlarni yozib olish, ishlov berish va saqlash tartibi to‘g‘risidagi yo‘riqnomaning talablariga, shuningdek, 2006-yil 5-dekabrdagi O‘zbekiston Respublikasi Bosh vazirining o‘rinbosari – Davlat sirlarini saqlash bo‘yicha idoralararo komissiya raisi tomonidan tasdiqlangan — tarqatilishi cheklangan ma’lumotlarga ega bo‘lgan hujjatlar, fayllar va nashrlarni ro‘yxatga olish, ishlov berish va saqlash tartibi to‘g‘risidagi yo‘riqnoma talablariga, rioya etilishi uchun javobgar.

4. Javobgarlik

4.1 Ushbu Tartib talablarining bajarilishi uchun javobgarlik Universitetning tarkibiy bo‘linmalar rahbarlari va tegishli mansabdor shaxslar zimmasiga yuklanadi.

4.2 Universitetning axborot resurslarida mavjud bo‘lgan konfidensial ma’lumotlarni himoya qilish va tarqatmaslik yuzasidan tegishli choralarni ko‘rish bo‘yicha javobgarlik ularning egalari, Lokal tarmoq administratori hamda Departament xodimlari zimmasiga yuklanadi.

4.3 Universitetda Axborot xavfsizligi administratori hamda Departament boshlig‘i ushbu Tartibning xodimlar tomonidan bajarilishini nazorat qilishni ta’minlash uchun javobgardir.

4.4 Ushbu Tartibda belgilangan talablarning buzilishi Universitetning ichki mehnat qoidalari va O‘zbekiston Respublikasining mehnat qonunchiligiga muvofiq intizomiy javobgarlikka tortilishga olib keladi.

Universitet axborot xavfsizligi
siyosatiga 18-ilova

Favqulodda vaziyatlarda ish faoliyatini tiklashni va uzluksiz ishlashni ta’minlash REJASI

1. Umumiy qoidalar

1.1 Ushbu Reja Universitetda axborotni qayta ishlash, uzatish, saqlashga mo‘ljallangan axborot resurslarini va axborotni himoya qilish texnik vositalarning uzluksiz ishlashini va ish qobiliyatini tiklashni ta’minlashga mo‘ljallangan.

1.2 Universitet axborot resurslarining uzluksiz ishlashini ta’minlash bo‘yicha chora-tadbirlarga quyidagilar kiradi:

- rejalashtirilgan profilaktika va ta’mirlash ishlari;
- zaxira apparat vositasi;
- dasturlar va ma’lumotlarning zaxira nusxasini yaratish;
- uzluksiz aloqani va elektr ta’minotini ta’minlash;
- server va telekommunikatsiya qurilmalarining normal ishlashi uchun sharoit yaratish.

1.3 Universitetning axborot tizimlari va resurslari faoliyatini tiklash bo‘yicha chora-tadbirlarga quyidagilar kiradi:

- aloqa kanallari va zaxira qurilmalarini faollashtirish;
- dasturlarni va ma’lumotlarni zaxira nusxalaridan tiklash;
- qurilmani ta’mirlash yoki almashtirish;
- dasturiy ta’minotni qayta o‘rnatish.

2. Uzluksiz ishlashni ta’minlash choralari

2.1 Rejalashtirilgan profilaktik ishlar tarmoq serverlari, axborot tizimlari serverlari, tarmoq kommutatsiya uskunalari, ma’lumotni himoya qilish asosiy vositalarning to‘g‘ri ishlashini baholash uchun amalga oshiriladi.

2.2 Rejalashtirilgan profilaktik ishlarni Universitetning Raqamli ta’lim texnologiyalari departamenti Tarmoqlarni boshqarish va texnik qo‘llab-quvvatlash sektori bosh mutaxassisi (keyingi o‘rinlarda – Lokal tarmoq administratori) hamda Raqamli ta’lim texnologiyalari departamenti (keyingi o‘rinlarda – Departament) xodimlari olib boradilar. Ularning vazifalariga 2.1-bandda ko‘rsatilgan texnik vositalarni saqlash kiradi.

2.3 Rejalashtirilgan profilaktik ishlar oyiga bir marta quyidagi texnik vositalarga nisbatan o‘tkazilishi kerak:

- lokal tarmoqning telekommunikatsiya qurilmalari;
- axborot resurslarining, shu jumladan ularga o‘rnatilgan operatsion tizimlarning MBBT va amaliy dasturlarning server qurilmalari;
- ma’lumotlarni saqlash tizimi;
- axborotni himoyalash tizimi.

2.4 Rejalashtirilgan profilaktik ishlar texnik jihozlarga texnik xizmat koʻrsatish qoidalariga muvofiq amalga oshiriladi.

2.5 Profilaktik ishlarga quyidagilar kiradi:

- sozlamalarning yaxlitligini tekshirish;
- tizim fayllarini tahlil qilish;
- MBBT nazorati;
- yuzaga kelgan xatolarni va ishchi holatini tahlil qilish;
- texnik vositalarning asosiy elementlarining ishlashini tekshirish;
- diagnostika vositalari yordamida diagnostika qilish.

2.6 Taʼmirlash ishlari Lokal tarmoq administratori hamda Departament xodimlari tomonidan texnik jihozlarning ishlamay qolgan elementlarining ishlashini tiklash yoki nosozliklar yuz berganda amalga oshiriladi.

2.7 Profilaktik va taʼmirlash ishlarini olib borishda ish stansiyalari va serverlarini ochish va muhrlash, profilaktika ishlarini bajarish, dasturlarni oʻrnatish va oʻzgartirish toʻgʻrisidagi maʼlumotlar ushbu Rejaning 2-ilovasiga muvofiq “Ish stansiyalari va serverlarni ochish va muhrlash, profilaktika ishlarini bajarish, dasturlarni oʻrnatish va oʻzgartirishlarni qayd etish jurnali”da qayd etiladi.

2.8 Universitetda Lokal tarmoq administratori hamda Departament xodimlari oʻzlari nazorat qiladigan apparatning ishlashini taʼminlash uchun javobgardirlar.

2.9 Universitet axborot resursining serverlari Lokal tarmoq administratori hamda Departament xodimlari tomonidan zaxiralanadi.

2.10 Axborot resurslarining dasturiy taʼminotini va maʼlumotlarini zaxiralash Siyosatning 7-ilovasi “Tizim va amaliy dasturlarni yangilash, shuningdek, maʼlumotlarning zaxira nusxalarini shakllantirish va tiklash boʻyicha Nizom”ga muvofiq amalga oshiriladi.

3. Avariya holatidagi tiklash choralari

3.1 Axborot resurslarining ishlashini tiklash avariya holatini tiklash rejasiga muvofiq amalga oshirilishi kerak.

Universitetning har bir axborot resursi uchun avariyani tiklash boʻyicha batafsil reja tuzilishi kerak (1-ilova).

Axborot xavfsizligi administratori hamda Departament boshligʻi tomonidan chora-tadbirlar ishlab chiqiladi va tasdiqlash uchun Universitetning axborot-kommunikatsiya texnologiyalarini joriy etish va raqamlashtirish boʻyicha masʼul rahbari (keyingi oʻrinlarda – Masʼul rahbar)ga kiritiladi. Chora-tadbirlar unda belgilangan masʼullar tomonidan amalga oshiriladi.

3.2 Avariya holatlari va favqulodda vaziyatlar yuz berganda Axborot xavfsizligi administratori hamda Departament boshligʻi Masʼul rahbarga darhol xabar berishlari shart.

3.3 Axborot xavfsizligi administratori avariya holatida yoki favqulodda vaziyatda mazkur Rejaning 3-ilovasiga muvofiq “Favqulodda (avariyaviy) vaziyatlarni hisobga olish jurnali”da qayd etishi kerak.

4. Favqulodda vaziyatlar yuzasidan choralar

4.1 Tabiiy va texnogen hodisalar natijasida yuzaga kelgan favqulodda vaziyatlarda Universitet axborot tizimlarining doimiy ishlashini ta’minlash uchun datamarkazining zaxira resurslaridan foydalanish, shuningdek, zaxira nusxalarni boshqa-boshqa binolarda (joylarda) xavfsizlik choralarini ko‘rgan holda joylashtirish hamda saqlash Axborot xavfsizligi administratori va Departament boshlig‘ining ustuvor vazifalaridan biridir.

Favqulodda vaziyatlarda ish faoliyatini
tiklashni va uzluksiz ishlashni ta’minlash
Rejasiga 1-ilova

Ishchi holatini tiklash avariyaviy
REJASI

Avariya yoki nosozlik nomi	Harakatlar bosqichlari	Bajarilish vaqti*	Mas’ullar
Elektr ta’minoti hamda aloqa tarmog‘ining uzilishi			
Elektr ta’minotining uzilishi (to‘liq yoki qisman)	1) Mas’ul rahbarga xabar berish; 2) UPS zaxira elektr ta’minotining yoqilishini va ishlashini tekshirish; 3) Asosiy serverlar va tarmoq qurilmalarining ishlashini tekshirish; 4) Uzoq vaqt davomida elektr uzilib qolganda akkumulyator batareyalarini yoki dizel generatorini ulash (dizel generatorining avtomatik ishlashi ta’minlanadi); 5) Sabablarni va kerakli tiklash vaqtini aniqlashtirish uchun tuman elektr tarmoqlari korxonasiga qo‘ng‘iroq qilish; 6) Asosiy elektr ta’minotini tiklash, zaxira quvvat manbalarini zaryadlash.	5-10 daqiqa 1-5 daqiqa 20 daqiqa 20 daqiqa Asosiy elektr ta’minoti tiklangandan keyingi 12 soat	Axborot xavfsizligi administratori, Departament boshlig‘i
Aloqa uzilishi	1) Mas’ul rahbarga xabar berish; 2) Aloqa kanallarini tekshirish (Uzonline) va tarmoq qurilmalari — marshrutizatorlar, kalitlar va proksi-serverlarning ishlashi, tarmoq kabelining holatini tekshirish (ishlamay qolish sabablarini aniqlash); 3) Zaxira tarmoq qurilmalari, zaxira aloqa kanalidan foydalangan holda aloqani tiklash yoki tarmoq kabelini almashtirish; 4) Tashqi aloqa yo‘qolgan taqdirda telekommunikatsiya operatori bilan aloqa qilish; 5) Ishlamay qolgan tarmoq qurilmalarini ta’mirlash yoki yangisini sotib olish, to‘liq aloqani tiklash.	5-10 daqiqa 10-20 daqiqa 10-20 daqiqa 5-10 daqiqa 2 sutka	Axborot xavfsizligi administratori, Lokal tarmoq administratori, Departament boshlig‘i va xodimlari
Axborot resurslari va serverlarning ishdan chiqishi			

Avariya yoki nosozlik nomi	Harakatlar bosqichlari	Bajarilish vaqti*	Mas’ullar
Ilova serveri va ma’lumotlar bazasi ishlamay qolishi (serverning jismoniy komponentining ishdan chiqishi — protsessor, OZU, materinka, tarmoq kartasi va boshqalar).	1) Mas’ul rahbarga xabar berish; 2) Zaxira serverining ishlashi va axborot xavfsizligini nazorat qilish; 3) Zaxira virtual serverini ishga tushirish; 4) Ishlamay qolgan serverning ishlamay qolish sabablarini aniqlash; 5) Ishlamay qolgan serverni ta’mirlash yoki ishlamay qolgan komponentni almashtirish; 6) Ishlamay qolgan serverni qayta tiklash; 7) Asosiy serverdagi ma’lumotlarni qayta tiklash (agar bitta saqlash tizimidan foydalanilmasa) va serverni ishga tushirish.	5-10 daqiqa 5-10 daqiqa 10-30 daqiqa 10-30 daqiqa 1 soatdan 2 sutkagacha 1 soatdan 2 sutkagacha	Axborot xavfsizligi administratori, Lokal tarmoq administratori, Departament boshlig‘i va xodimlari
Serverning birida tizim yoki dasturiy ta’minotning ishlamay qolishi	1) Mas’ul rahbarga xabar berish; 2) Zaxira serverining ishlashi va axborot xavfsizligini nazorat qilish; 3) Zaxira virtual serverini ishga tushirish; 4) Ishlamay qolgan serverning ishlamay qolish sabablarini aniqlash; 5) Obraz yordamida tizim dasturini tiklash yoki ishlamay qolgan serverda dastur dasturini qayta tiklash; 6) Ishlamay qolgan serverni qayta tiklash; 7) Asosiy serverdagi ma’lumotlarni qayta tiklash (agar bitta saqlash tizimidan foydalanilmasa) va serverni ishga tushirish.	5-10 daqiqa 5-10 daqiqa 10-30 daqiqa 10-30 daqiqa 1 soatdan 2 sutkagacha 1 soatdan 1 sutkagacha	Axborot xavfsizligi administratori, Lokal tarmoq administratori, Departament boshlig‘i va xodimlari
Veb-resurslar ishlashidagi uzilishlar			
Elektr ta’minotini o‘chirish (to‘liq yoki qisman) (asosiy va zaxira), Aloqa buzilishi, Serverning ishdan chiqishi, Tizim dasturining noto‘g‘ri ishlashi	1) Mas’ul rahbarga xabar berish; 2) Sabablarini bilib, xizmat ko‘rsatuvchi provayderning mas’ul shaxs bilan bog‘lanish; 3) Rasmiy veb-saytning ishlashini, ma’lumotlarning to‘liqligini va tiklanishini tekshirish.	5-10 daqiqa 5-10 daqiqa Qayta tiklangandan so‘ng	Axborot xavfsizligi administratori, Lokal tarmoq administratori, Departament boshlig‘i va xodimlari
Dasturiy ta’minot (veb-dastur) ishdan chiqishi	1) Mas’ul rahbarga xabar berish; 2) Veb-serverga masofadan ulanish, xizmat ko‘rsatuvchi provayderdagi mas’ul shaxs bilan muloqot qilish va ishlamaslik sabablarini aniqlash;	5-10 daqiqa 10-20 daqiqa	Axborot xavfsizligi administratori,

Avariya yoki nosozlik nomi	Harakatlar bosqichlari	Bajarilish vaqti*	Mas’ullar
	3) Dasturni va serverdagi ma’lumotlarni qayta o‘rnatish orqali ishlarni tiklash.	1 soatdan 3 soatgacha	Lokal tarmoq administratori, Departament boshlig‘i va xodimlari
Axborot xavfsizligi insidentlari	1) Mas’ul rahbarga xabar berish; 2) Sabablarini aniqlash uchun xizmat ko‘rsatuvchi provayderning mas’ul shaxs bilan bog‘lanish; 3) Sabablarini aniqlash va zarur hollarda Hamkorlik reglamenti asosida harakatlarni amalga oshirish; 4) Insident oqibatlarini bartaraf etish va insident takrorlanmasligi yuzasidan tegishli ishlarni amalga oshirish.	5-10 daqiqa 5-10 daqiqa 15-30 daqiqa Qayta tiklangandan so‘ng	Axborot xavfsizligi administratori, Departament boshlig‘i
Tabiiy va texnogen hodisalar oqibatida yuzaga kelgan avariyalar	Tabiiy va texnogen hodisalar oqibatida yuzaga kelganda Universitetning 2024-yil 15-fevraldagi 93-son buyruq asosida harakat qilinadi.	Hodisa yuzaga kelgan vaqtdan boshlab	Universitetning barcha xodimlari

Izoh:

1) “Bajarilish vaqti” ustunida avariya sodir bo‘lgan va aniqlangan vaqtdan boshlab vaqt ko‘rsatiladi;

2) Yangi ishlab chiqilgan axborot tizimlari uchun qo‘shimcha Ishchi holatini tiklash avariyaviy rejasi ishlab chiqiladi va ushbu Favqulodda vaziyatlarda ish faoliyatini tiklashni va uzluksiz ishlashni ta’minlash rejasiga kiritiladi.

Mas’ul rahbar *— Universitetning axborot-kommunikatsiya texnologiyalarini joriy etish va raqamlashtirish bo‘yicha mas’ul rahbari;*
Axborot xavfsizligi administratori *— Universitetning axborot xavfsizligini ta’minlash masalalari bo‘yicha mas’ul xodimi;*
Lokal tarmoq administratori *— Universitetning Tarmoqlarni boshqarish va texnik qo‘llab-quvvatlash sektori bosh mutaxassisi;*
Departament *— Universitetning Raqamli ta’lim texnologiyalari departamenti*

Favqulodda vaziyatlarda ish faoliyatini
tiklashni va uzluksiz ishlashni ta’minlash
Rejasiga 2-ilova

Ish stansiyalari va serverlarni ochish va muhrlash, profilaktika ishlarini bajarish, dasturlarni o‘rnatish va o‘zgartirishlarni qayd etish
JURNALI

T/r	Sana	Hodisa	Javobgar imzosi
1.			
2.			
3.			
4.			
5.			

Favqulodda vaziyatlarda ish faoliyatini tiklashni va uzluksiz ishlashni ta’minlash Rejasiga 3-ilova

Favqulodda (avariyaviy) vaziyatlarni hisobga olish JURNALI

T/r	Favqulodda (avariyaviy) vaziyat yuzaga kelgan sana va vaqt	Favqulodda (avariyaviy) vaziyat turi	Favqulodda (avariyaviy) vaziyat yuzaga kelgan joy	Jalb qilingan kuchlar va vositalar	Tugatish sanasi va vaqti
1.					
2.					
3.					
4.					
5.					

Universitet axborot xavfsizligi
siyosatiga 19-ilova

Hodisalar va favqulodda vaziyatlarni boshqarish, shuningdek, uchinchi tomon tashkilotlari bilan o‘zaro aloqalar bo‘yicha REGLAMENT

1. Umumiy qoidalar

1.1 Ushbu Reglament Universitetda axborot xavfsizligi bilan bog‘liq hodisalarni, shu jumladan favqulodda vaziyatlarni qayta ishlash tartibini, shuningdek, ushbu hodisalar yuz bergan taqdirda uchinchi tomon tashkilotlari bilan o‘zaro aloqalar tartibini belgilaydi.

2. Hodisalar va favqulodda vaziyatlarni ko‘rib chiqish tartibi

2.1 Siyosatning 12-bo‘limida keltirilgan baxtsiz hodisa, favqulodda vaziyat yuzaga kelgan taqdirda, xodimlar Universitetning axborot xavfsizligini ta’minlash masalalari bo‘yicha mas’ul xodimi (keyingi o‘rinlarda – Axborot xavfsizligi administratori)ga hamda Raqamli ta’lim texnologiyalari departamenti (keyingi o‘rinlarda – Departament) boshlig‘iga hodisalar yuzasidan tezkorlikda xabar berishlari kerak.

2.2 Axborot xavfsizligi hodisasi, avariya yoki favqulodda vaziyat aniqlagandan so‘ng, xodimlar tegishliligi bo‘yicha Axborot xavfsizligi administratori hamda Departament boshlig‘iga hodisa yuzaga kelish vaqti, tahdidlarning sabablari va manbalari, to‘g‘risida to‘liq ma’lumot berishlari lozim.

2.3 Favqulodda vaziyatlar sodir bo‘lganda Axborot xavfsizligi administratori va Departament boshlig‘i quyidagilarni bajarishlari lozim:

- hodisaning kelib chiqishi sabablarini bilish (hodisa sodir bo‘lgan vaqti, tahdid xarakteri, oqibatlari va h.k.)
- hodisalar to‘g‘risida Universitetning axborot-kommunikatsiya texnologiyalarini joriy etish va raqamlashtirish bo‘yicha mas’ul rahbari (keyingi o‘rinlarda – Mas’ul rahbar)ga ma’lumot berish;
- hodisalar holati yuzasidan ma’lumotlarni ushbu Siyosatning 20-ilovaga muvofiq “Axborot xavfsizligi hodisalarini qayd etish jurnali”ga qayt etish.

Axborot xavfsizligi administratori Siyosatning 18-ilovasi “Favqulodda vaziyatlarda ish faoliyatini tiklashni va uzluksiz ishlashni ta’minlash rejasi”ga muvofiq favqulodda holat yuzaga kelganda qayd etish jurnaliga yozish kerak.

2.4 Axborot xavfsizligining muhim va salbiy oqibatlariga olib keladigan axborot xavfsizligi hodisalari yuz berganda, Mas’ul rahbarga tezkorlikda xabar berilishi shart.

2.5 Axborot xavfsizligining har qanday holati yuzasidan quyidagilar amalga oshirilishi kerak:

- xatarlarni lokalizatsiya qilish;
- hodisa oqibatlarini bartaraf etish.

2.6 Tahdidlarni va ularning oqibatlarini bartaraf etish Lokal tarmoq administratori hamda Departament xodimlari tomonidan amalga oshiriladi, shuningdek, zarurat

tug‘ilsa tegishli rahbariyat ruxsati bilan yordamchi mutaxassislari jalb qilinishi mumkin.

2.7 Axborot xavfsizligi administratori hamda Departament boshlig‘i tomonidan Universitetda hodisalar likvidatsiya qilinadi.

2.8 Universitetda Axborot xavfsizligi administratori Departament boshlig‘i boshlig‘i bilan birgalikda hodisa asoratlarini yo‘qotish bo‘yicha monitoring olib boriladi va bu bo‘yicha tayyorlangan ma’lumotlar Mas’ul rahbarga taqdim etiladi.

2.9 Tahdidlar oldi olingandan so‘ng Lokal tarmoq administratori hamda Departament xodimlari hodisalar asorati yuzasidan ish olib boriladi.

2.10 Axborot xavfsizligi hodisalar asoratlarini oldini olish yuzasidan quyidagilarni bajarish lozim:

- hodisa yuzaga kelishi yuzasidan barcha ma’lumotlarni aniqlash va baholash;
- axborot xavfsizligi hodisasi sodir bo‘lgan aniq ma’lumotlarni saqlash va zaxiralash;
- ma’lumotlarni qayta tiklash uchun zaxira tizimidan foydalanish;
- zaxira vositasini ishga tushirish, ishlamay qolgan elementni ta’mirlash yoki to‘liq yangisiga almashtirish orqali elementning ishlashini tiklash.

Axborot xavfsizligi bilan bog‘liq hodisalarni bartaraf etish bo‘yicha ishlar Siyosatning 18-ilovasida keltirilgan “Favqulodda vaziyatlarda ish faoliyatini tiklashni va uzluksiz ishlashni ta’minlash rejasi”ga muvofiq amalga oshirilishi kerak.

2.11 Axborot xavfsizligi hodisasi asoratlari bartaraf etilganligi yuzasidan olingan ma’lumot tahlilini amalga oshirish.

Tahlil qilishda quyidagilarni hisobga olish lozim:

- hodisalarni barcha oqibatlarini bartaraf etish;
- tiklangan muhofaza qilinadigan ma’lumotlarning to‘liqligi va to‘g‘riligi va foydalana olishligini tekshirish;
- axborot xavfsizligiga tahdidlari takrorlanishini oldini olish.

2.12 Axborot xavfsizligi hodisalarini likvidatsiya qilgandan so‘ng hodisalarni qayta tekshirish kerak.

Qayta tekshirish uchun Universitetning mas’ul bo‘linma xodimlaridan iborat ishchi guruh tuzadi.

Axborot xavfsizligi hodisalarining oxirgi xulosasi:

- hodisaning asl kelib chiqish sababini aniqlash;
- axborot xavfsizligi bilan bog‘liq hodisa yuz berishiga sababchi bo‘lgan buzuvchilar yoki javobgar shaxslarni aniqlash;
— ushbu hodisa takrorlanmaslik uchun tavsiyalar ishlab chiqish.

2.13 Aniqlangan axborot xavfsizligi hodisasida aybdor bo‘lganlar mehnat qonunchiligiga, shuningdek, Respublikaning amaldagi ma’muriy va jinoiy qonunchiligiga muvofiq javobgarlikka tortiladilar.

2.14 Axborot xavfsizligi hodisalari qayta ro‘y bermasligi uchun quyidagilar tavsiya qilinadi:

- kelgusida hodisalar takroran sodir bo‘lmasligi uchun qo‘shimcha choralar ishlab chiqish;
- axborot xavfsizligining me’yoriy-huquqiy, dasturiy-texnik va tashkiliy chora-tadbirlarga o‘zgartirish kiritish;

Yuqoridagi takliflar Universitet rahbariyati tomonidan tasdiqlangach ish faoliyatiga tatbiq etiladi.

3. Axborot xavfsizligi bilan bog‘liq hodisalar yuz berganda, uchinchi tomon tashkilotlari bilan o‘zaro hamkorlik qilish tartibi

3.1 Axborot xavfsizligi bilan bog‘liq hodisa yoki favqulodda vaziyat sodir bo‘lganda, shuningdek, Siyosatning 12-bandida ko‘rsatilgan hodisalar yuz bergan taqdirda, Universitet Hamkorlik reglamentiga muvofiq “Kiberxavfsizlik markazi” DUK bilan o‘zaro hamkorlik qilishi lozim.

3.2 “Kiberxavfsizlik markazi” DUK bilan o‘zaro hamkorlik doirasida Axborot xavfsizligi administratori tomonidan quyidagilar amalga oshirishi lozim:

- hodisa aniqlanishi bilan 2 (ikki) soat ichida “Kiberxavfsizlik markazi” DUKga xabar berish;
- “Kiberxavfsizlik markazi” DUKga voqea to‘g‘risida xabar berilgandan so‘ng, ma’lumotlarining yaxlitligi va ishonchliligini saqlash choralari ko‘riladi;
- hodisani oldini olish bo‘yicha ko‘rilgan choralar to‘g‘risida “Kiberxavfsizlik markazi” DUKga xabar berish;
- “Kiberxavfsizlik markazi” DUKga yordam ko‘rsatish va voqeani tekshirishda ishtirok etish.

3.3 “Kiberxavfsizlik markazi” DUKdan xabarnoma olgandan so‘ng, bir kun ichida Axborot xavfsizligi administratori Departament boshlig‘i bilan birgalikda axborot xavfsizligi hodisasining oqibatlarini tezkor oldini olish, shuningdek, axborot xavfsizligi hodisasi to‘g‘risidagi ma’lumotlar xavfsizligini ta’minlash uchun tegishli choralarni ko‘radi.

3.4 Sodir bo‘lgan hodisalarning bartaraf etilganligi to‘g‘risida 3 (uch) ish kunida Axborot xavfsizligi administratori hamda Departament boshlig‘i “Kiberxavfsizlik markazi” DUKga rasmiy tarzda ma’lumot taqdim etishlari kerak.

3.5 Universitet Axborot xavfsizligi administratori hamda Departament boshlig‘i Universitetda hodisalarni tekshirish ishlarini tashkillashtiradi, o‘tkazadi va muvofiqlashtiradi.

3.6 Axborot xavfsizligi bilan bog‘liq hodisalarni tekshirishda “Kiberxavfsizlik markazi” DUK mutaxassislari jalb qilinishi mumkin, og‘ir oqibatlarga olib keladigan hodisalarni tekshirishda buzg‘unchilarni javobgarlikka tortish uchun o‘rnatilgan tartibda huquqni muhofaza qilish idoralari mutaxassislari jalb qilinadi.

3.7 Voqea yuzasidan maxsus tekshiruv o‘tkazish va ularga manfaatdor shaxslar va huquqni muhofaza qilish idoralarini jalb qilish to‘g‘risida qaror Universitet rahbariyati tomonidan qabul qilinadi.

3.8 Agar Mas’ul rahbar boshchiligida Universitetda aniqlangan axborot xavfsizligi hodisasini mustaqil tekshirish olib borilsa, u holda uning ish natijalari bo‘yicha hodisalarni aniqlash usullari va sharoitlarini unga tegishli bo‘lgan axborot resurslariga nisbatan tahlil natijalari to‘g‘risida hisobot “Kiberxavfsizlik markazi” DUKga taqdim etiladi, shuningdek, axborot xavfsizligi hodisasi oqibatlarini bartaraf etish va axborot resurslari ishiga ruxsatsiz aralashish faktlarini oldini olish bo‘yicha chora-tadbirlar rejasi hisobot bilan birga taqdim etiladi.

3.9 Taqdim etgan tekshiruv natijalari bo‘yicha “Kiberxavfsizlik markazi” DUK axborot xavfsizligi bilan bog‘liq hodisalarning takrorlanishiga yo‘l qo‘ymaslik maqsadida, taklif va tavsiyalarni ishlab chiqadi va rasmiy shaklda Universitetga taqdim etadi. Axborot xavfsizligi administratori hamda Departament boshlig‘i o‘z o‘rnida taklif va tavsiyalarni amalga oshirish rejasini tayyorlaydi va uning bajarilishini nazoratga oladi.

Universitet axborot xavfsizligi
siyosatiga 20-ilova

Axborot xavfsizligi hodisalarini qayd etish jurnali shakli

T/r	Hodisa sodir bo‘lgan vaqti va sanasi	Hodisa sodir bo‘lgan himoya obyekti nomi	Xavfni amalga oshirish turi va usuli	Hodisa oqibatlarining mohiyati	Qabul qilingan choralar	Javobgar shaxs imzosi
1.						
2.						
3.						
4.						
5.						

Universitet axborot xavfsizligi
siyosatiga 21-ilova

Axborot xavfsizligi siyosati bilan tanishish jurnali shakli

T/r	F.I.Sh.	Bo‘linma (departament/bo‘lim/ markaz/fakultet)	Lavozim	Sana	Imzo
1.					
2.					
3.					
4.					
5.					

Videokuzatuv tizimidagi ma’lumotlarni taqdim etish to‘g‘risida NIZOM

1. Umumiy qoidalar

1. Ushbu Nizom Universitetga tegishli bo‘lgan videokuzatuv kameralariga yozib olingan videoarxivni keyinchalik aniq bir masalaga oydinlik kiritish maqsadida qayta ko‘rib chiqish hamda o‘rnatilgan ichki tartib asosida jismoniy va yuridik shaxslarga taqdim etish tartibini belgilaydi.

2. Atamalar va ta’riflar

Ushbu Nizomda quyidagi asosiy tushunchalardan foydalaniladi:

Talabgor – O‘ziga tegishli bo‘lgan muammoli masalaga oydinlik kiritish maqsadida Universitet videokuzatuv tizimiga qayd etilgan videoarxivni ko‘rmoqchi bo‘lgan jismoniy yoki yuridik shaxs

Videokuzatuv operatori – Universitet videokuzatuv tizimi kuzatib borish huquqi berilgan Universitetning Raqamli ta’lim texnologiyalari departamenti xodimi

Videokamera – Optoelektronik o‘zgartirish va televizion signalni uzatish yordamida uzatiladigan sahnani televizion tahlil qilish uchun mo‘ljallangan qurilma.

Videoarxiv – kuzatuv kamerasiga qayd etilgan va saqlashga olib qo‘yilgan fayl (videomaterial).

Videotahlil – Real vaqt rejimidagi videokameralardan yoki videoarxiv yozuvlaridan olingan tasvirlar ketma-ketligini tahlil qilish jarayoni.

3. Nizomning maqsadi

3.1 Universitet videokuzatuv tizimi Universitet hududida jamoat tartibiga rioya qilishga bo‘lgan kompleks yondashuvni ta’minlashi, fuqarolar ommaviy bo‘ladigan obyektlar va hududlarni turli tahdidlarga qarshi himoya bilan ta’minlashi, korrupsion, kriminal, terrorchilik, jinoiy va boshqa xarakterdagi tahdidlar ehtimolini kamaytirishi maqsadida joriy etilgan.

3.2 Ushbu Nizom talablari Universitet xodimlari, professor o‘qituvchilar, talabalar, shu bilan birga Universitet hududiga kirish huquqi bo‘lgan uchinchi tomon tashkilot xodimlari uchun qo‘llaniladi.

4. Ma’lumotlarni taqdim etish ishlarni tashkil etish

4.1 Universitetning xodimlari, professor o‘qituvchilar, talabalar, shu bilan birga Universitet hududiga kirish huquqi bo‘lgan uchinchi tomon tashkilot xodimlari Universitet videokuzatuv tizimiga qayd etilgan qanday turdagi videomateriallar

Universitetning mulki ekanligini tan oladi, unga kirish va tahlil qilish Universitet manfaatlariga javob berishi shart.

Ushbu ma’lumotlarga kirish va tahlil qilish Universitet rektori ruxsati bilan Raqamli ta’lim texnologiyalari departamenti tomonidan amalga oshiriladi.

4.2 Videoarxivni taqdim etish quyidagi shaxslar ishtirok etadi:

- Talabgor;
- Videokuzatuv operatori;
- Axborot xavfsizligi bo‘limi boshlig‘i.

4.3 Videoarxivni taqdim etish quyidagi bosqichlarni o‘z ichiga oladi:

- ushbu Nizomning 1-ilovasiga muvofiq shaklda ariza berish;
- arizani ko‘rib chiqish va qaror qabul qilish;
- videoarxiv materiali ustida videotahlilni o‘tkazish;
- videotahlil natijalari bo‘yicha qaror qabul qilish;
- videoarxivni ro‘yxatdan o‘tkazish va taqdim etish.

4.4 videoarxivni tahlil qilish tartibi

4.5 Talabgor arizasini quyida keltirilgan hujjatlar va ma’lumotlarni ilova qilgan holda Videokuzatuv operatoriga taqdim etadi.

4.7 Videokuzatuv operatori arizani ko‘rib chiqadi va videotahlilni o‘tkazadi. Natijasi bo‘yicha 3 ish kuni mobaynida arizani qabul qilish to‘g‘risida qaror qabul qiladi yoki asoslantirilgan rad javobini yuboradi. Ushbu jarayonning sxemasi ushbu Nizomning 2-ilovasi “Qayd etilgan videoyozuvlarni (videoarxivni) taqdim etish sxemasi”da keltirilgan.

4.8 Arizani qabul qilishni rad etish uchun quyidagilar asos bo‘ladi:

- arizaning belgilangan talablarga nomuvofiqligi;
- arizada keltirilgan ma’lumotlar bo‘yicha videokuzatuv mavjud emasligi;
- hujjatlar va ma’lumotlarning to‘liq taqdim etilmaganligi;
- arizaga ilova qilingan hujjatlar va ma’lumotlarning soxtaligi (qalbakiligi) yoki noto‘g‘riligining aniqlanganligi;
- Videoarxiv bir shaxsni yoki jamoatchilikni huquqini poymol qilish yoki qasddan tarqatish uchun yoki birovni kamsitish maqsadida olinayotgan bo‘lsa;
- arizaning ushbu Nizom bilan belgilangan boshqa talablarga nomuvofiqligi.

4.9 Huquqni muhofaza qiluvchi organlarga hamda boshqa yuridik shaxslarga videoarxivni taqdim etishda Universitet tomonidan komissiya tuziladi.

4.10 Komissiyaning tarkibi, a’zolarining huquq, majburiyatlari va javobgarligi Universitet rahbarining qarori bilan belgilanadi.

4.11 Komissiya ishining yakuni Talabgor yuridik shaxs arizasiga ko‘ra videoarxivni har tomonlama tahlil qilish va berish yoki bermaslik to‘g‘risida qaror qabul qilish hisoblanadi.

Videoarxivni taqdim etishga qaror qabul qilinganda komissiya a’zolari va Talabgor ushbu Nizom 3-ilovasida keltirilgan “Qayd etilgan videoyozuvlarni (videoarxivni) taqdim etish dalolatnomasi”ni imzolaydilar.

5. Javobgarlik

Raqamli ta’lim texnologiyalari departamenti boshlig‘i ushbu ushbu Nizom talablarining bajarilishi ustidan nazoratni ta’minlashga mas’uldir.

Ushbu Nizomda belgilangan talablarining buzilishi O‘zbekiston Respublikasining qonunchiligiga muvofiq javobgarlikka tortishga sabab bo‘ladi.

Universitet videokuzatuv tizimidagi
ma’lumotlarni taqdim etish to‘g‘risida
Nizomga 1-ilova

Buxoro davlat universiteti Raqamli ta’lim
texnologiyalari departamenti boshlig‘i
_____ga
_____
tomonidan

A R I Z A

Ushbuni yozib ma’lum qilamanki, men _____,
_____
(bo‘lgan holat va vaziyat haqida qisqacha tafsilot)
_____
_____
_____
_____
_____
_____
_____

Yuqoridagi holatga aniqlik kiritish, vaziyatni oydinlashtirish maqsadida menga mutasaddi xodimlar ishtirokida 2025-yilning “__” _____ sanasi soat ___-___ dan “__” _____ sanasi soat ___-___ gacha bo‘lgan vaqt oralig‘ida _____
_____da o‘rnatilgan kuzatuv kamerasi videoyozuvlarini ko‘rib chiqishda amaliy yordam berishingizni so‘rayman.
Murojaat uchun telefon raqamim: _____

Talabgor _____ _____ _____
F.I.Sh. Imzo Sana

Buxoro davlat universiteti Raqamli ta’lim texnologiyalari departamenti MA’LUMOTNOMA

Ushbu murojaat bo‘yicha kuzatuv kameralari videoyozuvlari o‘rganib chiqildi. Holat bo‘yicha quyidagilar aniqlandi:
_____
_____
_____
_____
_____
_____

Videokuzatuv operatori _____ _____ _____
F.I.Sh. Imzo Sana

Universitet videokuzatuv tizimidagi
ma’lumotlarni taqdim etish to‘g‘risida
Nizomga 2-ilova

Qayd etilgan videoyozuvlarni (videoarxivni) taqdim etish SXEMASI

Bosqichlar	Subyektlar	Tadbirlar	Bajarish muddatlari
I. Murojaatlarni shakllantirish va yuborish			
1-bosqich	Talabgor	1. Belgilangan namunadagi arizani to‘ldirish. 2. Zarur hollarda boshqa hujjatlarni taqdim etish.	1. Xohishiga ko‘ra 2. Zarur hollarda
2-bosqich	Videokuzatuv operatori	1. Arizani ko‘rib chiqish 2. Inson hayoti, salomatligi shuningdek Universitet faoliyati bilan bog‘liq alohida kechiktirib bo‘lmaydigan hollarda arizani darhol ko‘rib chiqish	1. bir ish kuni mobaynida 2. Real vaqt rejimida
II. Arizani qayta ishlash tartibi			
3-bosqich	Videokuzatuv operatori	1. Talabgorning arizasini ko‘rib chiqish imkoniyati mavjudligini (arizada ko‘rsatilgan hududda videokuzatuv kamerasi arxivi mavjudligi, videoarxiv muddat oralig‘i to‘g‘ri ko‘rsatilganligi, videoarxiv mavjudligi, taqdim etishga mo‘ljallanganligi va boshqa jihatdan) o‘rganadi, videotahlilni amalga oshiradi. 2. Videoarxivni tayyorlash va taqdim etish uchun tayyorlaydi yoki Talabgor arizasini asosli rad etish to‘g‘risida Talabgor arizasidagi keltirilgan namunadagi ma’lumotnomani to‘ldiradi va arizani bekor qiladi.	1. uch ish kuni mobaynida 2. ikki ish kuni mobaynida
4-bosqich	Tomonlar	Videoarxivni taqdim etish Dalolatnomani imzolash.	Tomonlarni kelishuvi asosida bir ish kunida

Universitet videokuzatuv tizimidagi
ma’lumotlarni taqdim etish to‘g‘risida
Nizomga 3-ilova

Qayd etilgan videoyozuvlarni (videoarxivni) taqdim etish DALOLATNOMASI

Talabgorning JSHSHIR	
F.I.Sh.	
Manzili	
Telefon raqami, elektron manzili	

Biz quyida imzo chekuvchilar:
Talabgor ishtirokida qayd etilgan videoyozuvni (videoarxivni) Talabgorga quyida keltirilgan holatda taqdim etilganligini tasdiqlaymiz:

Video nomi	
Video formati	
Hosil qilingan vaqti	
Hajmi	
Davomiyligi	
XESH funksiya	

Videokuzatuv operatori_____ _____ _____
imzo F.I.SH Sana

AKT departamenti vakili _____ _____ _____
imzo F.I.SH Sana

Talabgor_____ _____
imzo F.I.SH Sana

Universitet videokuzatuv tizimidagi ma’lumotlarni taqdim etish to‘g‘risidagi NIZOM bilan tanishtirildim. Ushbu videoarxiv bilan bog‘liq yuzaga keladigan barcha holatlarga javobgarligim tushuntirildi.

Talabgor_____ _____ _____
imzo F.I.SH Sana

Universitet axborot xavfsizligi
siyosatiga 23-ilova

Axborot xavfsizligi riskini baholash natijalari

1. Universitetning axborot xavfsizligi xavfini aniqlash quyidagi bosqichlardan iborat:

1) risklarni aniqlash;

2) risk tahlili;

3) riskni baholash.

2. Axborot xavfsizligi risklarini aniqlash bosqichlari:

1) Universitetning axborot aktivlarini aniqlash va ularni baholash – Universitet uchun axborot aktivining qiymatini yoki ahamiyatini aniqlash;

2) axborot aktivlariga nisbatan axborot xavfsizligiga tahdidlarni aniqlash;

3) axborot aktivlarini axborot xavfsizligiga tahdidlardan himoya qilish tizimidagi zaifliklarni aniqlash — axborot aktivining xavfsizlik darajasini yoki axborot xavfsizligi tahdidini amalga oshirish imkoniyatini baholash uchun zaifliklarni aniqlash.

3. Axborot xavfsizligi risklarini aniqlash uchun Universitetga tegishli barcha axborot aktivlari ro‘yxati aniqlanadi.

4. Axborot aktivining qiymati Universitet faoliyatini buzish, moliyaviy yo‘qotishlar va Universitet obro‘siga putur yetkazish bilan bog‘liq mumkin bo‘lgan oqibatlarga (kutilayotgan zararga) qarab belgilanadi.

Axborot aktivining qiymati yoki ahamiyatini baholashda unga kiritilgan axborotning xavfsizlik toifasi (sinfi) ham hisobga olinadi.

5. Axborot aktivlarini identifikatsiya qilish va ularning qiymatini (ahamiyatini) aniqlash 1-jadvalga muvofiq keltirilgan.

Universitet o‘zining axborot aktivlariga nisbatan tahdidlarni aniqlash va axborot xavfsizligi risklarini miqdoriy baholashni amalga oshiradi, ularning qiymati Universitet o‘z vazifalarini bajarishi va faoliyatini amalga oshirish uchun ularning ahamiyati darajasidan kelib chiqqan holda belgilanadi va quyidagicha aniqlanadi:

past — 1-4

o‘rta — 5-7

yuqori — 8-10.

6. Har bir axborot aktiviga nisbatan axborot xavfsizligi tahdidlarini aniqlash bosqichida axborot aktiviga ham axborot, jarayonlar, apparat va dasturiy ta’minot, ham Universitetning o‘ziga zarar yetkazishi mumkin bo‘lgan potensial tahdidlar ro‘yxati aniqlanadi.

Universitetning axborot aktivlarining axborot xavfsizligiga tahdidlar ro‘yxati, ularning paydo bo‘lish ehtimoli qiymatini ko‘rsatuvchi tahdid darajasi ($_{Ptah}$) 2-jadvalda keltirilgan.

7. Zaifliklarni aniqlash bosqichida zaifliklarning mavjudligi va ulardan axborot aktiviga axborot xavfsizligi tahdidlariga ta’sir ko‘rsatish uchun foydalanish

imkoniyatlari baholanadi.

Zaifliklar deganda tahdidni muvaffaqiyatli amalga oshirishga yordam beradigan yoki uni amalga oshirish uchun foydalaniladigan axborot aktivlarining axborot xavfsizligi tizimidagi xavfsizlikning zaif tomonlari tushuniladi.

8. Axborot xavfsizligiga tahdidlarni amalga oshirish uchun foydalanilishi mumkin bo‘lgan zaifliklar 3-jadvalda keltirilgan.

Zaifliklar Universitetda axborot xavfsizligini ta’minlash bo‘yicha tashkiliy-texnik chora-tadbirlarning amalga oshirilishi (muvofiqligi) darajasi bilan bog‘liq.

Har bir tashkiliy-texnik tadbirning bajarilishi quyidagicha baholanadi:

- 0 — chora bajarilmagan (himoya vositalari yo‘q, boshqarish tartib-taomillari aniqlanmagan yoki bajarilmagan, dasturiy ta’minotda zaiflik mavjud va h.k.);

- 0 dan 1 gacha — chora qisman amalga oshirilgan (himoya vositasi mavjud, ammo uning ma’lumotlar bazasi yangilanmagan yoki keraklicha sozlanmagan, boshqarish tartib-taomillari aniqlangan, ammo zarur davriylikda bajarilmagan, dasturiy ta’minot yangilangan, lekin zaiflik mavjudligi yuzasidan tekshirish o‘tkazilmagan va h.k.)

- 1 — chora hech qanday kamchiliklarsiz amalga oshirilgan.

Axborot aktivlariga nisbatan zaifliklarni baholash 4-jadvalda keltirilgan.

9. Har bir axborot aktivi uchun *Kzaif* zaifligini amalga oshirish (bartaraf qilish) koeffitsienti aniqlanadi. Ushbu koeffitsient zaifliklarni bartaraf etishga qaratilgan va 4-jadvalda ko‘rsatilgan chora-tadbirlarni amalga oshirish darajasini belgilaydi. Ushbu chora-tadbirlar Universitetning Axborot xavfsizligi siyosatida belgilangan tashkiliy va texnik tadbirlarni o‘z ichiga oladi.

10. Axborot xavfsizligiga tahdid xavfi quyidagi formula bo‘yicha baholanadi:

$$\mathrm{R} = \mathrm{Ptah} * \mathrm{C} * (\,1\, - \frac{\sum_n^i \mathrm{K}zaif}{\mathrm{n}})$$

Bu yerda:

R — agar ma’lum bir tahdid amalga oshirilgan bo‘lsa, axborot aktiviga (xavf darajasi) nisbatan salbiy oqibat riskining raqamli qiymati;

Ptah — axborot aktiviga nisbatan axborot xavfsizligiga tahdidning paydo bo‘lish (ro‘y bo‘lish) ehtimoli;

C – axborot aktivining qiymati (ahamiyati);

Kzaif – ma’lum bir tahdidga nisbatan zaifliklarni bajarish koeffitsienti;

n – ma’lum bir axborot xavfsizligi tahdidiga nisbatan zaifliklarning umumiy soni.

11. Tahdidlar amalga oshirilganda axborot aktivlariga nisbatan axborot xavfsizligi risklarini tahlil qilishning miqdoriy usul natijasi 5-jadvalda, Axborot aktivlariga nisbatan salbiy oqibat yuzaga kelish riski tahlili 6-jadvalda, Axborot xavfsizligi qoldiq riskini hisoblash natijalari 7-jadvalda keltirilgan.

1-jadval. Axborot aktivlarini identifikatsiya qilish va ularning qiymatini (ahamiyatini) aniqlash

№	Axborot aktivining nomi	Himoyalanganlik toifasi (klassi)	Axborot aktivining qiymati (ahamiyati)
1.	buxdu.uz	Ochiq axborot	6 (axborotning ahamiyati – 8)
2.	moodle.buxdu.uz	Ochiq axborot	6 (axborotning ahamiyati – 8)
3.	hemis.buxdu.uz	Ochiq axborot	6 (axborotning ahamiyati – 8)
4.	masofaviy.buxdu.uz	Ochiq axborot	3 (axborotning ahamiyati – 5)
5.	student.buxdu.uz	Ochiq axborot	7 (axborotning ahamiyati – 7)
6.	uniwork.buxdu.uz	Ochiq axborot	3 (axborotning ahamiyati – 5)
7.	citrus.buxdu.uz	Ochiq axborot	3 (axborotning ahamiyati – 5)
8.	journal.buxdu.uz	Ochiq axborot	3 (axborotning ahamiyati – 5)
9.	srep.buxdu.uz	Ochiq axborot	3 (axborotning ahamiyati – 5)
10.	pedskills.buxdu.uz	Ochiq axborot	3 (axborotning ahamiyati – 5)
11.	Korporativ elektron pochta	Ochiq axborot	3 (axborotning ahamiyati – 5)
12.	Universitet fayl serveri	Ochiq axborot	7 (axborotning ahamiyati – 7
13.	IP telefoniya	Ochiq axborot	7 (axborotning ahamiyati – 7)
14.	Ishchi stansiyalar	Ochiq va konfidensial axborot	3 (axborotning ahamiyati – 5)
15.	Server uskunalari	Ochiq va konfidensial axborot	8 (axborotning ahamiyati – 8)
16.	Kirish chiqishni nazorat qilish tizimi	Konfidensial axborot	3 (axborotning ahamiyati – 5)
17.	Videokuzatuv tizimi	Konfidensial axborot	3 (axborotning ahamiyati – 5)

2-jadval: Axborot tizimlari va resurslarining zaifliklari

Toifasi	Raqami	Zaifliklar
Apparat vositalari	VH01	Yetarlicha xizmat ko‘rsatilmaslik/ma’lumotlar tashuvchilarning nuqsonli installyatsiyasi
	VH02	Vositalarning davriy almashtirishlar sxemasining mavjud emasligi
	VH03	Namlikka, changga, ifloslanishga ta’sirchanlik
	VH04	Elektromagnit nurlanishga sezgirlik
	VH05	Konfiguratsiyaga o‘zgartirish kiritilishini nazorat qilish samaradorligining yo‘qligi
	VH06	Kuchlanishning nobarqarorligiga ta’sirchanlik
	VH07	Temperatura o‘zgarishlariga ta’sirchanlik
	VH08	Muhofazalanmagan saqlash
	VH09	Yo‘q qilish qoidalarining buzilishi
	VH10	Nazorat qilinmagan holda nusxa olish
	VS01	Dasturiy ta’minotning bo‘lmasligi yoki yetarlicha testlanmaganligi
	VS02	Dasturiy ta’minotdagi ma’lum bo‘lgan kamchiliklar
	VS03	Ishchi stansiyasini “tizimdan chiqish”siz qoldirish
	VS04	Axborot yetarli darajada o‘chirilmasdan ma’lumotlar tashuvchilarini berish yoki ulardan takroran foydalanish
	VS05	Audit dalillarining yo‘qligi
	VS06	Foydalanish huquqlarining noto‘g‘ri taqsimlanishi
	VS07	Keng tarqalgan dasturiy ta’minot

Toifasi	Raqami	Zaifliklar
	VS08	Vaqtga nisbatan amaliy dasturlarning noto‘g‘ri ma’lumotlarga qo‘llanilishi
Dasturiy ta’minot	VS09	Murakkab foydalanuvchi interfeysi
	VS10	Hujjatlarning yo‘qligi
	VS11	O‘rnatish parametrlarining noto‘g‘riligi
	VS12	Noto‘g‘ri ma’lumotlar
	VS13	Foydalanuvchi identifikatsiyasi va autentifikatsiyasi uchun mexanizmlarning mavjud emasligi
	VS14	Muhofaza qilinmagan parollar jadvallari
	VS15	Parollarning yomon menejmenti
	VS16	Keraksiz serverlardan foydalanish imkoniyati
	VS17	Oxirigacha ishlab chiqilmagan yoki dasturiy ta’minot
	VS18	Ishlab chiquvchilar uchun noaniq yoki to‘liq bo‘lmagan spetsifikatsiyalar
	VS19	O‘zgartishlar kiritilishini samarali nazorat qilishning yo‘qligi
	VS20	Dasturiy ta’minotni nazoratsiz yuklash va foydalanish
	VS21	Rezerv nusxalarning mavjud emasligi
	VS22	Hisobotlarni rahbariyatga taqdim etmaslik
Tarmoq	VN01	Xabar yuborilganligi yoki olinganligi isbotining yo‘qligi
	VN02	Muhofazalanmagan aloqa liniyalari
	VN03	Kabellarning yomon montaj qilinganligi
	VN04	Yagona ishlamay qolish nuqtasi
	VN05	Jo‘natuvchi va oluvchini identifikatsiya va autentifikatsiya qilishning yo‘qligi
	VN06	Xavfsiz bo‘lmagan tarmoq arxitekturasi
	VN07	Parollarni ochiq ko‘rinishda berish
	VN08	Tarmoqning noadekvat boshqarilishi (tizimning marshrutlashtirish xatolariga qarshi tura olish qobiliyati)
	VN09	Umumiy foydalanishdagi tarmoqqa muhofazalanmagan ulanishlar
	VN10	Muhofazalanmagan sezgir trafik
Xodimlar	VP01	Xodimlarning yo‘qligi
	VP02	Ishga qabul qilishning adekvat bo‘lmagan protseduralari
	VP03	Xavfsizlikni yetarlicha o‘qitmaslik
	VP04	Dasturiy ta’minotdan va uskunadan noto‘g‘ri foydalanish
	VP05	Xavfsizlik sohasidan xabardor emasligi
	VP06	Monitoring mexanizmlarining yo‘qligi
	VP07	Shtatdan tashqari xodimlar yoki texnik xodimlarning nazoratsiz ishlashi
	VP08	Xabarlar almashinish va ma’lumotlar uzatish vositalaridan to‘g‘ri foydalanish siyosatining yo‘qligi
Tashkilotning ishlash joyi	VC01	Bino va xonalarga kirishni fizik boshqarish vositalaridan adekvat bo‘lmagan va e’tiborsiz holda foydalanish
	VC02	Suv toshish ehtimoli bo‘lgan hududda joylashish
	VC03	Nostabil energiya bilan ta’minlash
	VC04	Binolar, eshiklar va derazalar fizik muhofazasining yo‘qligi
Tashkilot	VO01	Foydalanuvchilarni ro‘yxatga olish va chiqarish rasmiy protsedurasining yo‘qligi
	VO02	Kirish huquqini qayta ko‘rib chiqish rasmiy jarayonining yo‘qligi
	VO03	Buyurtmachilar va/yoki uchinchi shaxslar bilan shartnomalarda (xavfsizlik sohasida) shartlarning yetarli emasligi yoki yo‘qligi

Toifasi	Raqami	Zaifliklar
	VO04	Axborotni qayta ishlash vositalari monitoringi protseduralarining yo‘qligi
	VO05	Muntazam auditlarning (nazoratning) yo‘qligi
	VO06	Risklarni aniqlash va identifikatsiya qilish protseduralarining yo‘qligi
	VO07	Ma’mur va foydalanuvchining qayd etish jurnallarida nosozliklar to‘g‘risidagi xabarlar yozuvlarining yo‘qligi
	VO08	Kerakli darajada bo‘lmagan xizmat ko‘rsatish servisi
	VO09	Xizmat ko‘rsatish darajasi to‘g‘risida bitimning yo‘qligi yoki yetishmasligi
	VO10	O‘zgartirishlar kiritishni nazorat qilish protsedurasining yo‘qligi
	VO11	AXBT hujjatlarini nazorat qilish rasmiy protsedurasining yo‘qligi
	VO12	AXBT yozuvlarini nazorat qilish rasmiy protseduralarining yo‘qligi
	VO13	Umumiy foydalanishdagi axborotga nisbatan rasmiy mualliflashtirish jarayonining yo‘qligi
	VO14	Axborot xavfsizligi sohasida vazifalarni zarur tarzda taqsimlanmaganligi
	VO15	Uzluksiz ish rejalarining yo‘qligi
	VO16	Elektron pochtadan foydalanish siyosatining yo‘qligi
	VO17	Dasturiy ta’minotni foydalaniladigan tizimlarga kiritish protseduralarining yo‘qligi
	VO18	Konfidensial ma’lumotlarni qayta ishlash protseduralarining yo‘qligi
	VO19	Axborot xavfsizligi sohasidagi lavozim yo‘riqnomalarida javobgarlikning yo‘qligi
	VO20	Xodimlar bilan shartnomalarda (axborot xavfsizligi sohasida) shartlarning yo‘qligi yoki yetarlicha emasligi
	VO21	Axborot xavfsizligi insidenti yuz berganda muayyan intizomiy jarayonning yo‘qligi
	VO22	Mobil kompyuter texnikasidan foydalanish bo‘yicha rasmiy siyosatning yo‘qligi
	VO23	Rezerv aktivlarni nazorat qilishning yo‘qligi
	VO24	“Toza stol va toza ekran” siyosatining yo‘qligi yoki mos kelmasligi
	VO25	Axborotni qayta ishlash vositalarida mualliflashtirish mexanizmining yo‘qligi
	VO26	Xavfsizlikning buzilish monitoringi mexanizmlarining yo‘qligi
	VO27	Xavfsizlik zaifliklari to‘g‘risida hisobot protseduralarining yo‘qligi
	VO28	Intellektual mulk huquqlariga amal qilish protseduralarining yo‘qligi

Jadval №3. Universitetning axborot xavfsizligiga asosiy tahdidlarning ro‘yxati va tavsifi

Tahdidlar quyidagi mezonlarga ko‘ra tasniflanishi mumkin:
- vujudga kelish manbasiga ko‘ra: B-ichki, C-tashqi;
- vujudga kelishi sababli: A-tasodifiy, G-qasddan;
- vujudga kelish xususiyatiga ko‘ra: E – tabiiy yoki obyektiv, F – subyektiv.

Turkumi	T/r	Tahdid nomi	Manbaining ko‘rinishi, tabiati va sababi*	Ta’sir qilish obyektlari va oqibatlari	Mavjud zaifliklar	Tahdidni baholash
Jismoniy tahdidlar	TP01	Yong‘in	A, D, E, F, B, C	Barcha himoya obyektlari. Muvaffaqiyatsizlik yoki yo‘qotish	VH06, VH08, VN02, VN03, VC01, VC04	0,2
	TP02	Suv toshishi	A, D, E, F, B, C		VH03, VH04, VH07, VH08, VN02, VN03, VC01, VC04	0,2
	TP03	Ifloslanish, zararli radiatsiya	A, D, E, F, B, C		VH06, VH08, VC01, VC04	0,3
	TP04	Katta baxtsiz hodisa	A, D, E, F, B, C		VH03, VH06, VH08, VC04, VH08, VN02, VN03, VC01,	0,3
	TP05	Portlash, halokat	A, D, E, F, B, C		VH08, VC02, VC04 VH03, VH04, VN02, VC01	0,2
	TP06	Chang, korroziya, muzlash	A, D, E, F, B, C		VH03, VH06, VH07, VH08, VN02, VN03, VC01	0,1
Tabiiy tahdidlar	TN01	Iqlim hodisasi	A, E, C	Barcha himoya obyektlari. Muvaffaqiyatsizlik yoki yo‘qotish	VH04, VH08, VC01 VC04	0,4
	TN02	Seysmik hodisa	A, E, C		VH08, VC01	0,4
	TN03	Vulqon hodisasi	A, E, C		VH08, VC01, VC04	0
	TN04	Meteorologik hodisa	A, E, C		VH08, VC01, VC04	0,3
	TN05	Suv toshqini	A, E, C		VH08, VC02, VC04	0,4
	TN06	Pandemiya/epidemiya hodisasi	A, E, C		VH08, VC01	0,4

Turkumi	T/r	Tahdid nomi	Manbaining ko‘rinishi, tabiati va sababi*	Ta’sir qilish obyektlari va oqibatlari	Mavjud zaifliklar	Tahdidni baholash
Infratuzilmaning ishlamay qolishi	TI01	Ta’minot tizimining ishdan chiqishi	A, D, F, C	Uskuna va dasturiy ta’minot, ishchi stansiyalari va serverlari, mahalliy tarmoq, korporativ elektron pochta, axborot tizimlari va resurslari. Muvaffaqiyatsizlik, ishning to‘xtatilishi	VO03, VO08, VO09	0,6
	TI02	Sovutish yoki shamollatish tizimining ishlamay qolishi	A, D, F, B, C		VH01, VH03, VH07, VO08, VO09, VO15	0,7
	TI03	Energiya ta’minotining buzilishi	A, D, E, F, C		VH01, VH06, VC03, VO03, VO09-1, VO15-1	0,7
	TI04	Telekommunikatsiya tarmog‘ining ishdan chiqishi	A, D, E, F, C		VN04, VN05, VN09, VP06, VP08, VO03, VO09, VO15	0,8
	TI05	Telekommunikatsiya uskunalari ishlamay qolishi	A, D, F, B		VH01, VH02, VH05, VH08, VS11, VN05, VN09, VP06, VP07, VP08, VO08, VO15	0,8
	TI06	Elektromagnit nurlanish	A, D, E, F, C		VH04	0,4
	TI07	Termal nurlanish	A, D, E, F, B, C		VH07	0,4
	TI08	Elektromagnit impulslar	A, D, E, F, C		VH04	0,4
Texnik muvaffaqiyatsiz-liklar	TT01	Qurilma yoki tizimning ishdan chiqishi	A, F, B	Uskuna va dasturiy ta’minot, ishchi stansiyalari va serverlari, mahalliy tarmoq, korporativ elektron pochta,	VH01, VH02, VH05, VS01, VS02, VS10, VS11, VS19, VS20, VN05, VP02, VP04, VP06, VO04, VO05, VO07, VO08, VO09, VO10, VO15, VO17, VO25	0,7
	TT02	Axborot tizimining to‘yinganligi	A, D, F, B		VH09, VS16, VS19, VS20, VO10	0,5

Turkumi	T/r	Tahdid nomi	Manbaining ko‘rinishi, tabiati va sababi*	Ta’sir qilish obyektlari va oqibatlari	Mavjud zaifliklar	Tahdidni baholash
	TT03	Axborot tizimini ta’mirlash qobiliyatini buzilishi	A, D, F, B	axborot tizimlari va resurslari. Muvaffaqiyatsizlik, ishning uzilishi, uskuna yoki ma’lumotlarning yo‘qolishi	VH01, VH09, VS11, VS17, VP04, VC02, VO08, VO09, VO10, VO15, VO25	0,4
Xodimlar harakati	TH01	Terrorizm, hujumlar, sabotaj	D, F, B, C	Barcha himoya obyektlari. Muvaffaqiyatsizlik yoki yo‘qotish	VS03, VS12, VS13, VS15, VS20, VN01, VN06, VN08, VP05, VP08, VO16 VN02, VO04, VO05, VO27	0,2
	TH02	Ijtimoiy muhandislik	D, F, B, C	Tarmoqlar va axborot tizimlarining apparat va dasturiy ta’minoti. Konfidensiallik, yaxlitlik va mavjudlikni buzish	VS03, VS12, VS13, VS15, VS20, VN01, VN06, VN08, VP05, VP08, VO16	0,2
	TH03	Qurilmaning nurlanishini ushlab turish	D, F, B, C	Axborot, konfidensiallikni buzish	VN02, VO04, VO05, VO27	0,4
	TH04	Masofaviy monitoring	D, F, B, C		VS03, VP05, VP07, VC04, VO24	0,2
	TH05	Tinglash	D, F, B, C		VP05, VP06, VP07, VC01, VC04	0,6

Turkumi	T/r	Tahdid nomi	Manbaining ko‘rinishi, tabiati va sababi*	Ta’sir qilish obyektlari va oqibatlari	Mavjud zaifliklar	Tahdidni baholash
	TH06	Tashuvchi va saqlovchi vositalarni yoki hujjatlarni o‘g‘irlash	D, F, B, C	Axborot tashuvchi va saqlovchi vositalar va hujjatlar. Yaxlitlik va konfidensiallikni buzish	VH08, VH09, VS04, VS21, VP05, VP06, VP07, VC01, VC04, VO11, VO18, VO19, VO20, VO21, VO26	0,6
	TH07	Uskunani o‘g‘irlash	D F, B, C	Uskunalar. Yo‘qotish, faoliyatni olib borishning buzilishi	VH08, VH09, VP05, VP06, VP07, VC01, VC04, VO20, VO21, VO26	0,4
	TH08	Raqamli identifikatorni yoki identifikatsiya ma’lumotlarini o‘g‘irlash	D, F, B, C	Ishchi stansiyalari, serverlar, tarmoqlar va axborot tizimlari. Ruxsatsiz kirish	VH08, VH10, VS04, VS14, VS15, VN08, VP05, VP06, VP07, VC01, VC04, VO19, VO20, VO26	0,5
	TH09	Tashlab yuborilgan yoki takror ishlatilayotgan ma’lumot tashuvchi qurilmalardan ma’lumot olish	D, F, B, C	Axborot, konfidensiallikni buzish	VH09, VS04, VP05, VP06, VO24	0,4
	TH10	Axborotni oshkor qilish	A, D, F, B, C		VS06, VP05, VP06, VO11, VO12, VO18, VO20, VO21	0,6
	TH11	Ishonchsiz manbalardan ma’lumotlarni kiritish	A, D, F, B, C	Axborot, ishonchlilikning buzilishi	VS12, VP05, VP06, VO13, VO20, VO21	0,5

Turkumi	T/r	Tahdid nomi	Manbaining ko‘rinishi, tabiati va sababi*	Ta’sir qilish obyektlari va oqibatlari	Mavjud zaifliklar	Tahdidni baholash
	TH12	Uskunani buzish	D, F, B, C	Uskuna va ma’lumot. Funktsionallik, yaxlitlik, konfidensiallik va mavjudlikni buzish	VH05, VP04, VP06-0, VP07, VC01, VC04, VO02, VO10, VO26, VO27	0,4
	TH13	Dasturiy ta’minotni buzish	A, D, F, B, C	Dasturiy ta’minot vositalari va ma’lumotlar. Funktsionallik, yaxlitlik, konfidensiallik va mavjudlikni buzish	VS01, VS02, VS07, VS08, VS19, VS20, VN10, VP04, VP06, VP07, VC01, VC04, VO02, VO10, VO17, VO26, VO27	0,4
	TH14	Veb-aloqa orqali Drive-by ekspluatatsiyasidan foydalanish	D, F, B, C	Axborot resurslari va tizimlari. Ruxsatsiz kirish	VS02, VS12, VS16, VS19, VS20, VN01, VN06, VN10, VP05, VP08, VO16	0,6
	TH15	Takroriy hujum, o‘rtadagi odam hujumi	D, F, B, C	Ma’lumot. Ruxsatsiz kirish	VS02, VS07, VS13, VS20, VN02, VN06, VN07, VP05, VO16	0,5
	TH16	Shaxsiy ma’lumotlarni ruxsatsiz qayta ishlash	A, D, F, B, C		VH05, VH08, VH10, VS02, VS03, VS06, VS13, VS15, VN01, VN02, VN07, VN10, VP06, VP07, VP08, VC04, VO02, VO04, VO18, VO24, VO26, VO27	0,6
	TH17	Obyektlarga ruxsatsiz kirish	D, F, B, C	Barcha himoya obyektlari. Ruxsatsiz kirish	VP07, VC01, VC04	0,4
	TH18	Qurilmalardan ruxsatsiz foydalanish	D, F, B, C	Qurilma.	VH08, VP07, VC01, VC04, VO02, VO10, VO26	0,4

Turkumi	T/r	Tahdid nomi	Manbaining ko‘rinishi, tabiati va sababi*	Ta’sir qilish obyektlari va oqibatlari	Mavjud zaifliklar	Tahdidni baholash
	TH19	Qurilmalardan noto‘g‘ri foydalanish	A, D, F, B, C	Nosozlik, ish faoliyatining to‘xtashi	VP04	0,6
	TH20	Qurilmalar yoki ma’lumot tashuvchilarni shikastlash	A, D, F, B, C	Qurilma. Axborotlarni tashuvchi va saqlovchi vositalar Nosozlik, ish faoliyatining to‘xtashi	VP04, VS01, VS11, VS17, VS18	0,4
	TH21	Soxta dasturiy ta’minotni nusxalash	D, F, B, C	Dasturiy ta’minot, Funktsionallik va mualliflikning buzilishi	VH08, VH10, VS13, VS19, VP06, VP07, VO04, VO17	0,5
	TH22	Qalbaki yoki nusxalangan dasturiy ta’minotdan foydalanish	A, D, F, B, C		VS071, VS19, VS20, VP05, VP06, VO17	0,4
	TH23	Ma’lumotlarga shikast yetkazish	D, F, B, C	Ma’lumotlar yaxlitligini buzish	VS10, VS11, VS18, VS21, VP04, VP06, VP07, VO01, VO02, VO04, VO18, VO25	0,5
	TH24	Noqonuniy ma’lumotlarni qayta ishlash	D, F, B, C	Ma’lumotlar, ma’lumotlardan noqonuniy foydalanish, mualliflik huquqining buzilishi	VH08, VH10, VS12, VS13, VO01, VO02, VO04, VO11, VO12, VO13	0,4

Turkumi	T/r	Tahdid nomi	Manbaining ko‘rinishi, tabiati va sababi*	Ta’sir qilish obyektlari va oqibatlari	Mavjud zaifliklar	Tahdidni baholash
	TH25	Zararli dasturlarni yuborish yoki tarqatish	A, D, E, F, B, C	Ishchi stansiyalari, tarmoq, axborot tizimlari va resurslari. Nosozlik, nosozlik, yo‘qotish, ruxsatsiz kirish	VH10, VS02, VS19, VN06, VN07, VN10, VP05, VO16, VO26	0,6
	TH26	Joylashuvni aniqlash	D, F, B, C	Axborot, konfidensiallikni buzish	VP08, VO22	0,2
Xizmatlar yoki funksiyalarni buzish	TC01	Foydalanishda xatoliklar	A, F, B, C	Uskuna va dasturiy ta’minot, tarmoq, axborot tizimlari va resurslari, axborot. Nosozlik, nosozlik, yo‘qotish, ruxsatsiz kirish	VH05, VS01, VS04, VS09, VS10, VS11, VS17, VS19, VS20, VP03, VP05, VP06, VO04, VO10, VO17, VO25	0,5
	TC02	Huquqlar yoki ruxsatlarni suiiste’mol qilish	A, D, F, B, C		VS06, VS14, VP07, VO02, VO05, VO10, VO14, VO19	0,6
	TC03	Huquqlar yoki ruxsatlarni soxtalashtirish	D, F, B, C		VS06, VS13, VS14, VS15, VN06, VP05, VP06, VO01, VO02	0,5
	TC04	Harakatlarni rad etish	D, F, B, C		VS05, VS22, VP06, VO05, VO12, VO14, VO19	0,7
Tashkiliy tahdidlar	TO01	Xodimlarning etishmasligi	A, E, F, B	Uskuna va dasturiy ta’minot, tarmoq, axborot tizimlari va resurslari, axborot. Ish faoliyatining buzilishi	VP01, VP02, VO14,	0,5
	TO02	Resurslarning etishmasligi	A, E, F, B		VO15, VO23, VO25	0,6
	TO03	Xizmat ko‘rsatuvchining to‘lovga layoqatsizligi	A, E, F, C		VO03, VO08, VO09	0,4
	TO04	Qonunchilik yoki normativ-huquqiy hujjatlarning buzilishi	A, D, F, B, C		VP03, VP05, VO03, VO18, VO19, VO20, VO28	0,6

Turkumi	T/r	Tahdid nomi	Manbaining ko‘rinishi, tabiati va sababi*	Ta’sir qilish obyektlari va oqibatlari	Mavjud zaifliklar	Tahdidni baholash
Saqlash tizimlari va infratuzilmasiga tahdidlar	TD01	Ruxsat etilmagan foydalanish	D, F, B, C	Saqlash tizimi va infratuzilmasi, saqlash joylaridagi ma’lumotlar, Axborot tashuvchi yoki saqlovchi vositalar Axborotning yaxlitligi, mavjudligi va konfidensialligini buzish	VH05, VH08, VH10, VS02, VS03, VS06, VS13, VS15, VN01, VN02, VN07, VN10, VP06, VP07, VP08, VC04, VO02, VO04, VO18, VO24, VO26, VO27	0,6
	TD02	Ruxsatsiz kirish	D, F, B, C		VP07, VC01, VC04	0,4
	TD03	Qonunlar va me’yoriy hujjatlarga rioya qilmaslik uchun yuridik javobgarlik	A, D, F, B, C		VP03, VP05, VO03, VO18, VO19, VO20, VO28	0,6
	TD04	Saqlash tizimlariga DoS va DDoS hujumlar	D, F, C		VN02, VN03, VN10	0.9
	TD05	Ma’lumotlarga zarar etkazish, o‘zgartirish va yo‘q qilish	A, D, F, B, C		VH08, VH09, VS04, VS21, VP05, VP06, VP07, VC01, VC04, VO11, VO18, VO19, VO20, VO21, VO26	0,6
	TD06	Ma’lumotlar sizib chiqishi	D, F, B		VS06, VP05, VP06, VO11, VO12, VO18, VO20, VO21	0,6
	TD07	Axborot tashuvchi yoki saqlovchi vositani o‘g‘irlash yoki tasodifiy yo‘qotish	A, D, F, B, C		VP04, VS01, VS11, VS17, VS18	0,4
	TD08	Zararli dastur hujumi yoki inyeksiyasi	D, F, B, C		VH10, VS02, VS19, VN06, VN07, VN10, VP05, VO16, VO26	0,6
	TD09	Noto‘g‘ri ishlov berish yoki foydalanish tugagandan keyin utilizatsiya qilish	A, D, F, B		VH09, VS04, VP05, VP06, VO24	0,4

4-jadval: Axborot aktivlariga nisbatan zaifliklarning baholanishi (bahosi 0 dan 1 gacha).

Tashkiliy-texnik chora-tadbirlar-ning nomi		Bajariladigan chora- tadbirlarning nomi	hemis.buxdu.uz	masofaviy.buxdu.uz	uniwork.buxdu.uz	moodle.buxdu.uz	citrus.buxdu.uz	srep.buxdu.uz	pedskills.buxdu.uz	student.buxdu.uz	buxdu.uz	Korporativ elektron pochta	Journal.buxdu.uz	Universitet fayl serveri	IP telefoniya	Ishchi stansiyalar	Server uskunalari	Kirish chiqishni nazorat qilish tizimi	Videokuzatuv tizimi
VH. Apparat vositalari	VH01	1. Mas'ul shaxslarni tayinlash 2. O‘rnatish vositalari hisobi 3.Texnologik infratuzilmaning ortiqcha miqdori kamaytirilganligi. 4.Xizmat ko‘rsatish rejasi mavjudligi. 5.Davriy ravishda xizmat ko‘rsatish ishlari olib borilishi. 6.Sandbox(maxsus laboratoriya) orqali tekshirib olinishi	0,7	0,7	0,7	0,5	0,5	0,6	0,4	0,6	0,5	0,5	0,5	0,6	0,4	0,6	-	0,6	0,6
	VH02	1. Mas’ul shaxslarni tayinlash 2.Vositalarning davriy almashtirish sxemasi mavjudligi	0,2	0,2	0,2	0,2	0,2	0,2	0,2	0,2	0,2	0,2	0,2	0,2	0,2	0,3	-	0,3	0,3
	VH03	1. Uskunalarni changdan himoya qilish 2. Ventilyatsiya 3. Sanitariya me’yorlariga rioya qilish	0,9	0,9	0,9	0,9	0,9	0,9	0,9	0,9	0,9	0,9	0,9	0,9	0,9	0,5	-	0,5	0,5
	VH04	1.Elektromagnit nurlanishdan himoya qilish 2.Elektromagnit nurlanishga sezgir bo‘lmagan uskunalardan foydalanish	0,9	0,9	0,9	0,9	0,9	0,9	0,9	0,9	0,9	0,9	0,9	0,9	0,9	0,7	-	0,7	0,7
	VH05	1.Konfiguratsiya o‘zgarishlarini masofadan kuzatish. 2. Konfiguratsiya o‘zgarishlarining davriy monitoringi 3.Konfiguratsiya o‘zgartirilishi qayd etilib borilishi.	0,7	0,7	0,7	0,4	0,4	0,7	0,7	0,7	0,4	0,4	0,4	0,7	0,7	0,5	-	0,5	0,5
	VH06	1.Momaqaldiroq va chaqmoqdan himoyalash tizimi mavjudligi. 2.Yerga ulanish vositalarining mavjudligi. 3.Kuchlanish stabilizatori mavjudligi. 4.Alternativ kuchlanishga ulanish mavjudligi. 5.Doimiy kuchlanish (UPS) mavjudligi.	0,8	0,8	0,8	0,9	0,9	0,8	0,8	0,8	0,9	0,9	0,9	0,8	0,8	0,5	-	0,5	0,5

Tashkiliy-texnik chora-tadbirlar-ning nomi		Bajariladigan chora- tadbirlarning nomi	hemis.buxdu.uz	masofaviy.buxdu.uz	uniwork.buxdu.uz	moodle.buxdu.uz	citrus.buxdu.uz	srep.buxdu.uz	pedskills.buxdu.uz	student.buxdu.uz	buxdu.uz	Korporativ elektron pochta	Journal.buxdu.uz	Universitet fayl serveri	IP telefoniya	Ishchi stansiyalar	Server uskunalari	Kirish chiqishni nazorat qilish tizimi	Videokuzatuv tizimi
	VH07	1.Iqlim uskunalari (konditsioner) mavjudligi. 2.Temperatura gradusini belgilovchi datchiklar mavjudligi.	0,9	0,9	0,9	0,9	0,9	0,9	0,9	0,9	0,9	0,9	0,9	0,9	0,9	0,5	-	0,5	0,5
	VH08	1. Nazorat zonasi chegarasidan masofada joylashtirish 2.Server xonasida saqlash 3. Binolarni qulflash 4.Xavfsizlik signalizatsiya datchiklari 5. Muhrlash	0,9	0,9	0,9	0,9	0,9	0,9	0,9	0,9	0,9	0,9	0,9	0,9	0,9	0,7	-	0,7	0,7
	VH09	1. Hisobdan chiqarish tartibining mavjudligi va rioya etilishi 2.Mas’ul shaxslarni tayinlash 3.Axborot vositalaridagi qoldiq ma’lumotlarni yo‘q qilish 4. Hisobdan chiqarilishi kerak bo‘lgan uskunalarni to‘g‘ri saqlash	0,7	0,7	0,7	0,9	0,9	0,7	0,7	0,7	0,9	0,9	0,9	0,7	0,7	0,5	-	0,5	0,5
	VH10	1.Konsollar, ma’lumotlarni uzatish moslamalari, printerlar to‘g‘ri sozlanganligi. 2.Nazorat qilingan holda nusxa olish tartibi mavjudligi.	0,6	0,6	0,6	0,6	0,6	0,6	0,6	0,6	0,6	0,6	0,6	0,6	0,6	0,6	-	0,6	0,6
VS. Dasturiy	VS01	1.Litsenziyalangan dasturiy ta’minotdan foydalanish siyosati 2. Ishga tushirishdan oldin dasturiy ta’minotni sinovdan o‘tkazish (sinov operatsiyasi) 3.Dasturiy ta’minotga o‘zgartirishlar kiritish tartibi	0,8	0,8	0,8	0,5	0,5	0,6	0,5	0,6	0,5	0,5	0,5	0,6	0,5	0,6	-	0,6	0,6

Tashkiliy-texnik chora-tadbirlar-ning nomi		Bajariladigan chora- tadbirlarning nomi	hemis.buxdu.uz	masofaviy.buxdu.uz	uniwork.buxdu.uz	moodle.buxdu.uz	citrus.buxdu.uz	srep.buxdu.uz	pedskills.buxdu.uz	student.buxdu.uz	buxdu.uz	Korporativ elektron pochta	Journal.buxdu.uz	Universitet fayl serveri	IP telefoniya	Ishchi stansiyalar	Server uskunalari	Kirish chiqishni nazorat qilish tizimi	Videokuzatuv tizimi
	VS 02	1. Litsenziyalangan dasturiy ta’minotdan foydalanish siyosati 2.Dasturiy ta’minotni tekshirish va zaifliklarni bartaraf etish 3. Zaifliklar uchun ishlab chiqilgan dasturiy ta’minotning dastlabki kodini tahlil qilish	0,6	0,6	0,6	0,5	0,5	0,4	0,4	0,4	0,5	0,5	0,5	0,4	0,4	0,4	-	0,4	0,4
	VS 03	1.Barcha foydalanuvchilar uchun uchinchi omadsiz harakatdan keyin bloklanishi. 2.Foydalanuvchilar aktiv bo‘lmaganda jarayon bloklanishi. 3.Imtiyozli foydalanuvchilarni boshqarish tizimi orqali amalga oshirilishi. 4.Ishchi stansiyalarni nazoratli boshqaruvi mavjudligi.	0,8	0,8	0,8	0,7	0,7	0,8	0,8	0,8	0,7	0,7	0,7	0,8	0,8	0,7	-	0,7	0,7
	VS04	1.Axborot tashuvchi vositalarni olib kirish/chiqish tartibi va ularni yo‘q qilish tartibi mavjudligi. 2.Yo‘q qilingan vositalari o‘z vaqtida tiklab bo‘lmaydigan holatda keltirilib utilizatsiya qilinishi. 3.Axborot tashuvchi vositalarni yo‘q qilish qoidalari mavjudligi.	0,7	0,7	0,7	0,7	0,7	0,7	0,7	0,7	0,7	0,7	0,7	0,7	0,7	0,7	-	0,7	0,7
	VS05	1.Tashqi va ichki auditni o‘tkazish tartibi 2. Audit jurnallarini to‘plash va to‘g‘ri saqlash	0,6	0,6	0,6	0,5	0,5	0,6	0,5	0,6	0,5	0,5	0,5	0,6	0,5	0,4	0,8	0,4	0,4
	VS06	1.Kirish nazorati 2. Kirish matritsasining mavjudligi va amalga oshirilishi 3.Parol himoyasi 4. Imtiyozli foydalanuvchilarni tekshirish va nazorat qilish	0,8	0,8	0,8	0,6	0,6	0,8	0,6	0,8	0,6	0,6	0,6	0,8	0,6	0,7	0,9	0,7	0,7

Tashkiliy-texnik chora-tadbirlar-ning nomi		Bajariladigan chora- tadbirlarning nomi	hemis.buxdu.uz	masofaviy.buxdu.uz	uniwork.buxdu.uz	moodle.buxdu.uz	citrus.buxdu.uz	srep.buxdu.uz	pedskills.buxdu.uz	student.buxdu.uz	buxdu.uz	Korporativ elektron pochta	Journal.buxdu.uz	Universitet fayl serveri	IP telefoniya	Ishchi stansiyalar	Server uskunalari	Kirish chiqishni nazorat qilish tizimi	Videokuzatuv tizimi
	VS07	1.Ruxsatetilgan dasturiy ta'minotlar ro'yxati mavjudligi. 2.Active Directory domen nazorati administrator huquqi bilan mavjudligi.	0,8	0,8	0,8	0,5	0,5	0,5	0,6	0,5	0,5	0,5	0,5	0,5	0,6	0,5	-	0,5	0,5
	VS08	1.Tizim administratori harakatlarining nazorat qilinishi. 2.Amaliy dasturlarni qo'llab-quvvatlash bo'yicha operatsiyalarni nazorat qilinishi.	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,5	-	0,5	0,5
	VS09	Dasturiy ta'minotlarda foydalanuvchiga tushunarli interfeys yaratilgan.	*0,7*	*0,7*	*0,7*	*0,8*	*0,8*	*0,8*	*0,8*	*0,8*	*0,8*	*0,8*	*0,8*	*0,8*	*0,8*	0,9	-	0,9	0,9
	VS10	1.Dasturiy ta'minotdan foydalanish tartibi bo'yicha yo'riqnomaning mavjudligi. 2.Dasturiy ta'minotni tekshirish va sozlamalariga o'zgartirishlar kiritish bo'yicha to'liq hujjatlari mavjudligi. 3.Dasturiy ta'minotning loyiha- texnik hujjatlarining mavjudligi.	0,8	0,8	0,8	0,7	0,7	0,6	0,6	0,6	0,7	0,7	0,7	0,6	0,6	0,5	-	0,5	0,5
	VS11	1.Dasturiy ta'minot belgilangan talablar asosida o'rnatilganligi. 2.Dasturiy ta'minotni o'rnatish qoidalarining mavjudligi.	0,6	0,6	0,6	0,5	0,5	0,5	0,6	0,5	0,5	0,5	0,5	0,5	0,6	0,5	-	0,5	0,5
	VS12	1.Dasturiy ta'minotda noto'g'ri ma'lumotlardan foydalanilmasligi 2.Dasturiy ta'minotdagi ma'lumotlarni tekshirish tartibining mavjudligi	0,5	0,5	0,5	0,6	0,6	0,8	0,8	0,8	0,6	0,6	0,6	0,8	0,8	0,5	-	0,5	0,5

Tashkiliy-texnik chora-tadbirlar-ning nomi		Bajariladigan chora- tadbirlarning nomi	hemis.buxdu.uz	masofaviy.buxdu.uz	uniwork.buxdu.uz	moodle.buxdu.uz	citrus.buxdu.uz	srep.buxdu.uz	pedskills.buxdu.uz	student.buxdu.uz	buxdu.uz	Korporativ elektron pochta	Journal.buxdu.uz	Universitet fayl serveri	IP telefoniya	Ishchi stansiyalar	Server uskunalari	Kirish chiqishni nazorat qilish tizimi	Videokuzatuv tizimi
	VS13	1.Kirish nazorati 2. Kirish matritsasining mavjudligi va amalga oshirilishi 3.Parol himoyasi 4.Ko‘p faktorli autentifikatsiyadan foydalaning	0,8	0,8	0,8	0,6	0,6	0,8	0,6	0,8	0,6	0,6	0,6	0,8	0,6	0,7	0,9	0,7	0,7
	VS14	1.Parol himoyasi 2.Parolning murakkabligi	0,9	0,9	0,9	0,6	0,6	0,6	0,6	0,6	0,6	0,6	0,6	0,6	0,6	0,8	0,7	0,8	0,8
	VS15	1.Parol himoyasi 2.Paroldan foydalanish va saqlashni nazorat qilish	0,7	0,7	0,7	0,7	0,7	0,7	0,7	0,7	0,7	0,7	0,7	0,7	0,7	0,7	0,6	0,7	0,7
	VS16	1.Vaqtlangan dasturiy ta’minotdan foydalanish 2. Keraksiz xizmatlarni o‘chirib qo‘yish	0,8	0,8	0,8	0,7	0,7	0,5	0,5	0,5	0,7	0,7	0,7	0,5	0,5	0,7	-	0,7	0,7
	VS17	1.Yangi dasturiy ta’minotni maxsus dasturiy ta’minotlar orqali tekshirish tartibinining mavjudligi. 2.Dasturiy ta’minotlarni yangilash tizimi mavjudligi. 3.Guruhli xavfsizlik siyosati orqali nazorat o‘rnatilganligi	0,2	0,2	0,2	0,2	0,2	0,2	0,2	0,2	0,2	0,2	0,2	0,2	0,2	0,2	-	0,2	0,2
	VS18	1.Noodatiy vaziyatlarda harakatlarni ta’minlash qoidalari va tartib-taomillarini tartibga solinganligi. 2.Texnik nosozliklar bilan bog‘liq insidentlarni monitoring qilinishi va aniqlanishi.	0,4	0,4	0,4	0,3	0,3	0,2	0,2	0,2	0,3	0,3	0,3	0,2	0,2	0,2	-	0,2	0,2

Tashkiliy-texnik chora-tadbirlar-ning nomi		Bajariladigan chora- tadbirlarning nomi	hemis.buxdu.uz	masofaviy.buxdu.uz	uniwork.buxdu.uz	moodle.buxdu.uz	citrus.buxdu.uz	srep.buxdu.uz	pedskills.buxdu.uz	student.buxdu.uz	buxdu.uz	Korporativ elektron pochta	Journal.buxdu.uz	Universitet fayl serveri	IP telefoniya	Ishchi stansiyalar	Server uskunalari	Kirish chiqishni nazorat qilish tizimi	Videokuzatuv tizimi
	VS19	1.Ichki foydalanuvchilarning harakatlarini qayd etib borilishi. 2.Imtiyozli huquqlarga ega foydalanuvchilarning kirish huquqini boshqarilishi. 3.Masofadan kirishni cheklanishi va nazorat qilinishi.	0,6	0,6	0,6	0,3	0,3	0,5	0,5	0,5	0,3	0,3	0,3	0,5	0,5	0,5	-	0,5	0,5
	VS 20	1.Antivirus dasturiy ta’minotidan foydalanish yo‘riqnomasi mavjudligi 2.Internet tarmog‘idan va korporativ pochtadan foydalanish yo‘riqnomasi mavjudligi 3.Dasturiy vositalarning o‘matilishim doimiy nazorat (monitoring) qilinishi	0,7	0,7	0,7	0,7	0,7	0,7	0,7	0,7	0,7	0,7	0,7	0,7	0,7	0,5	-	0,5	0,5
	VS21	1.Zaxira protseduralari mavjudligi. 2.Saqlash paytida ma’lumotlarni tuzilgan; 3.Klasster serverlarida saqlash mavjudligi. 4.Dasturiy ta’minot va ma’lumotlarning zaxira nusxasi yaratilganligi.	0,9	0,9	0,9	0,8	0,8	0,8	0,8	0,8	0,8	0,8	0,8	0,8	0,8	0,5	-	0,5	0,5
	VS22	Hodisalar haqida rahbariyatga hisobot taqdim etish	0,8	0,8	0,8	0,7	0,7	0,7	0,7	0,7	0,7	0,7	0,7	0,7	0,7	0,2	1	0,2	0,2
VN.	VN01	xabarlardan foydalanish qoidalari	1	1	1	1	1	0,7	0,7	0,7	1	1	1	0,7	0,7	1	-	1	1

Tashkiliy-texnik chora-tadbirlar-ning nomi		Bajariladigan chora- tadbirlarning nomi	hemis.buxdu.uz	masofaviy.buxdu.uz	uniwork.buxdu.uz	moodle.buxdu.uz	citrus.buxdu.uz	srep.buxdu.uz	pedskills.buxdu.uz	student.buxdu.uz	buxdu.uz	Korporativ elektron pochta	Journal.buxdu.uz	Universitet fayl serveri	IP telefoniya	Ishchi stansiyalar	Server uskunalari	Kirish chiqishni nazorat qilish tizimi	Videokuzatuv tizimi
	VN02	1.SSL/TLS, VPN dan foydalanish 2.Yong‘inga chidamli izolyatsiyalangan va axborot xavfsizligi talablariga mis kabellardan foydalanilishi. 2. Kabel yotqizish joylari jismoniy himoya qilinganligi. 3.Elektr simlari uzilishlar va shikastlanishlardan himoya qilinganligi.	0,8	0,8	0,8	0,9	0,9	0,8	0,8	0,8	0,9	0,9	0,9	0,8	0,8	0,8	-	0,8	0,8
	VN03	1.Kabellar hujjatlashtirilgan va markazlashtirilganligi. 2. Mumkin bo‘lgan zararni minimallashtirishni hisobga olgan holda kabel yotqizilganligi (zaxira aloqa liniyasi qisman). 3.Kabel jurnallari yuritilishi. 4.Infratuzilma aloqa liniyalari topologyalari ishlab chiqilganligi va doimiy nazorat qilinishi.	0,7	0,7	0,7	0,7	0,7	0,7	0,7	0,7	0,7	0,7	0,7	0,7	0,7	0,7	-	0,7	0,7
	VN04	1.Xavfsizlik nuqtai nazaridan oylik tarmoq tekshiruvlari o‘tkazilishi. 2.Zaxira tarmoq mavjudligi. 3.Telekommunikatsiya tarmoqlariga xizmat ko‘rsatish kanallari mavjudligi. 4.Tarmoqdagi uzilishlar yoki nosozliklarni tahlil qilish va bartaraf etish boyicha mutaxassislar guruhi mavjudligi.	0,3	0,3	0,3	0,3	0,3	0,3	0,3	0,3	0,3	0,3	0,3	0,3	0,3	0,3	-	0,3	0,3

Tashkiliy-texnik chora-tadbirlar-ning nomi		Bajariladigan chora- tadbirlarning nomi	hemis.buxdu.uz	masofaviy.buxdu.uz	uniwork.buxdu.uz	moodle.buxdu.uz	citrus.buxdu.uz	srep.buxdu.uz	pedskills.buxdu.uz	student.buxdu.uz	buxdu.uz	Korporativ elektron pochta	Journal.buxdu.uz	Universitet fayl serveri	IP telefoniya	Ishchi stansiyalar	Server uskunalari	Kirish chiqishni nazorat qilish tizimi	Videokuzatuv tizimi
	VN05	1.Tashqi axborot tizimi bilan bog‘lanishda VPN kanalidan foydalanilishi. 2.Axborotlarni qayta ishlash tizimlari alohida VPN kanallarda ishlashi. 3.Kirish imkoniyatini foydalanuvchilar bo‘ylab taqsimlanishi — kirish matritsasini ishlab chiqilganligi. 4.Kirishga muvaffaqiyatsiz urinishlar sonining cheklanganligi. 5.Faol bo‘lmaganda foydalanuvchining kirish seansini bloklanishi.	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,5	-	0,5	0,5

Tashkiliy-texnik chora-tadbirlar-ning nomi		Bajariladigan chora- tadbirlarning nomi	hemis.buxdu.uz	masofaviy.buxdu.uz	uniwork.buxdu.uz	moodle.buxdu.uz	citrus.buxdu.uz	srep.buxdu.uz	pedskills.buxdu.uz	student.buxdu.uz	buxdu.uz	Korporativ elektron pochta	Journal.buxdu.uz	Universitet fayl serveri	IP telefoniya	Ishchi stansiyalar	Server uskunalari	Kirish chiqishni nazorat qilish tizimi	Videokuzatuv tizimi
	VN06	1.Perimetrni himoya qilinganligi (tarmoqlararo ekranlarni kodlanilishi) — ilova yoki resurslardan o‘zaro aloqasi nazarda tutilmagan portlar, protokollar yoki ilovalar orqali foydalanish imkoniyatini cheklanganligi. 2.Infratuzilma bilan bog‘liq tarmoq rejalari mavjud. 3.Tashqi masofaviy kirishdan foydalanilmasligi. 4.Ichki masofaviy kirishda SSH protokolidan foydalanilishi. 5.Ruxsatsiz jismoniy ulanishlar mavjud emasligi. 6.Ruxsatsiz ulanishlarni doimiy tekshirish nazorati yo‘lga qo‘yilganligi. 7.Telekommunikatsiya tarmoq qurilmaga ulanishda cheklovlar sozlanganligi (MAClar bo‘yicha). 8.Telekommunikatsiya infratuzilmalarida aylanmalarni oldini olish protokollari sozlanganligi.	0,6	0,6	0,6	0,6	0,6	0,6	0,6	0,6	0,6	0,6	0,6	0,6	0,6	0,6	-	0,6	0,6
	VN07	1.Domenlardan foydalanish 2.VLAN-dan foydalanish 3.Wi-Fi farqlash 4. Tashqi tarmoqlarga kirishni boshqarish	0,7	0,7	0,7	0,7	0,7	0,7	0,7	0,7	0,7	0,7	0,7	0,7	0,7	0,7	-	0,7	0,7
	VN08	Parolni himoya qilish, parollarni o‘zgartirish va ularni uzatish	0,8	0,8	0,8	0,6	0,6	0,7	0,7	0,7	0,6	0,6	0,6	0,7	0,7	0,7	-	0,7	0,7
	VN09	1.Muqobil marshrutlardan foydalanmaslik 2.Tarmoq uskunalarini bron qilish 3.Aloqa liniyalarini bron qilish	0,6	0,6	0,6	0,6	0,6	0,6	0,6	0,6	0,6	0,6	0,6	0,6	0,6	0,6	-	0,6	0,6

Tashkiliy-texnik chora-tadbirlar-ning nomi		Bajariladigan chora- tadbirlarning nomi	hemis.buxdu.uz	masofaviy.buxdu.uz	uniwork.buxdu.uz	moodle.buxdu.uz	citrus.buxdu.uz	srep.buxdu.uz	pedskills.buxdu.uz	student.buxdu.uz	buxdu.uz	Korporativ elektron pochta	Journal.buxdu.uz	Universitet fayl serveri	IP telefoniya	Ishchi stansiyalar	Server uskunalari	Kirish chiqishni nazorat qilish tizimi	Videokuzatuv tizimi
	VN10	1. SSL/TLS, VPN qo‘llanilishi	0,9	0,9	0,9	0,8	0,8	0,9	0,9	0,9	0,8	0,8	0,8	0,9	0,9	0,9	-	0,9	0,9
VP. Xodimlar	VP01	1.Mas’ul shaxslarni tayinlash 2.Mas’uliyatni taqsimlash 3.Tegishli kompetensiyaning mavjudligi 4. Mutaxassislarning almashinishi	0,5	0,5	0,5	0,6	0,6	0,7	0,7	0,7	0,6	0,6	0,6	0,7	0,7	0,8	-	0,8	0,8
	VP02	1.Komillik darajasini belgilash 2. Ishga qabul qilishda malakani tekshirish	0,6	0,6	0,6	0,7	0,7	0,5	0,5	0,5	0,7	0,7	0,7	0,5	0,5	0,6	-	0,6	0,6
	VP03	Malaka oshirish	0,4	0,4	0,4	0,4	0,4	0,4	0,4	0,4	0,4	0,4	0,4	0,4	0,4	0,4	-	0,4	0,4
	VP04	1.Axborot resurslariga kirish tartibga solinganligi. 2.Turli foydalanuvchilar guruhlarining imtiyozlari tartibga solinganligi. 3.Ketayotganda kompyuterlar o‘chirilishi.	0,8	0,8	0,8	0,8	0,8	0,8	0,8	0,8	0,8	0,8	0,8	0,8	0,8	0,8	-	0,8	0,8
	VP05	1. Xodimlar uchun axborot xavfsizligi bo‘yicha trening 2. Axborot xavfsizligi siyosatini ma’lum qilish 3. Axborot xavfsizligi talablarini xodimlarga yetkazish 4. Xodimlar tomonidan talablarga rioya etilishini nazorat qilish	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,5	-	0,5	0,5

Tashkiliy-texnik chora-tadbirlar-ning nomi		Bajariladigan chora- tadbirlarning nomi	hemis.buxdu.uz	masofaviy.buxdu.uz	uniwork.buxdu.uz	moodle.buxdu.uz	citrus.buxdu.uz	srep.buxdu.uz	pedskills.buxdu.uz	student.buxdu.uz	buxdu.uz	Korporativ elektron pochta	Journal.buxdu.uz	Universitet fayl serveri	IP telefoniya	Ishchi stansiyalar	Server uskunalari	Kirish chiqishni nazorat qilish tizimi	Videokuzatuv tizimi
	VP06	Videokuzatuv vositalarining mavjudligi. DLP tizimi mavjudligi. 3.Ichki foydalanuvchilarning barchasida DLP agenti o‘rnatilganligi. 4.DLP tizimida messenjerlardan ma’lumotlarni sizib chiqishi nazorat qilinishi.	0,8	0,8	0,8	0,8	0,8	0,8	0,8	0,8	0,8	0,8	0,8	0,8	0,8	0,6	0,9	0,6	0,6
	VP07	1.Muhim ma’lumotlar va hujjatlar ishonchli saqlanganligi. 2.Ishchilarni tashkil etishda texnik va ma’muriy talablar rasmiylashtirilishi. 3.Majburiyatnomalarni rasmiylashtirilishi. 4.Axborot xavfsizligi siyosati bilan tanishtirilishi. 5.Axborotlashtirish xonalariga kirish tartibining o‘matilganligi.	0,7	0,7	0,7	0,7	0,7	0,7	0,7	0,7	0,7	0,7	0,7	0,7	0,7	0,7	0,7	0,7	0,7
	VP08	1.Ro‘yxatdan o‘tgan kiruvchi va chiquvchi ma’lumotlarining xavfsizligini ta’minlanishi. 2.DLP tizimi mavjudligi. 3.Ichki foydalanuvchilarning barchasida DLP agenti o‘rnatilganligi. 4.akhv tizimida messenjerlardan ma’lumotlarni sizib chiqishi nazorat qilinishi.	0,8	0,8	0,8	0,8	0,8	0,8	0,8	0,8	0,8	0,8	0,8	0,8	0,8	0,6	0,7	0,6	0,6
VC.	VC01	1. Kirish joyidagi xavfsizlik. 2. Perimetr himoyasi. 3.Videokuzatuv vositalarining mavjudligi. 4.Kirishni nazorat qilish va boshqarish tizimining mavjudligi.	0,8	0,8	0,8	0,8	0,8	0,8	0,8	0,8	0,8	0,8	0,8	0,8	0,8	0,8	0,8	0,8	0,8

Tashkiliy-texnik chora-tadbirlar-ning nomi		Bajariladigan chora- tadbirlarning nomi	hemis.buxdu.uz	masofaviy.buxdu.uz	uniwork.buxdu.uz	moodle.buxdu.uz	citrus.buxdu.uz	srep.buxdu.uz	pedskills.buxdu.uz	student.buxdu.uz	buxdu.uz	Korporativ elektron pochta	Journal.buxdu.uz	Universitet fayl serveri	IP telefoniya	Ishchi stansiyalar	Server uskunalari	Kirish chiqishni nazorat qilish tizimi	Videokuzatuv tizimi
	VC02	1.Drenaj ishlarini avtomatlashtirilganligi 2.Yerto‘lalarda, tez-tez toshqinlarga moyil joylarga nasoslar o‘rnatilganligi. 3.Falshpol o‘rnatilganligi. 4.Uskunalarni suv kirishi mumkin bo‘lgan hududdan tashqarida joylashtirilganligi.	0,9	0,9	0,9	0,9	0,9	0,9	0,9	0,9	0,9	0,9	0,9	0,9	0,9	0,9	0,9	0,9	0,9
	VC03	1. Zaxira quvvat liniyasi 2.Dizel generatori	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,5
	VC04	1.Binolarni va uning atrofini tashqi omillardan himoya qilishni tashkil etilganligi: suv toshqini, avtomobil harakati va boshqalar. 2.Binolarga begonalarning kirib kelishidan himoya qilish choralari mavjudligi. 3.Ochiq foydalanilmaydigan eshiklar yo‘qligi. 4.Nazorat qilinmaydigan hududlarga to‘siqlar (panjaralar) o‘matilganligi. 5.Hududga kirish chiqish joyi maxsus texnik qo‘riqlash vositalari bilan jihozlanganligi. 6.Perimetr inson omili bilan himoya qilinganligi.	0,9	0,9	0,9	0,9	0,9	0,9	0,9	0,9	0,9	0,9	0,9	0,9	0,9	0,9	0,9	0,9	0,9

Tashkiliy-texnik chora-tadbirlar-ning nomi		Bajariladigan chora- tadbirlarning nomi	hemis.buxdu.uz	masofaviy.buxdu.uz	uniwork.buxdu.uz	moodle.buxdu.uz	citrus.buxdu.uz	srep.buxdu.uz	pedskills.buxdu.uz	student.buxdu.uz	buxdu.uz	Korporativ elektron pochta	Journal.buxdu.uz	Universitet fayl serveri	IP telefoniya	Ishchi stansiyalar	Server uskunalari	Kirish chiqishni nazorat qilish tizimi	Videokuzatuv tizimi
VO. Tashkiliy tadbirlar	VO01	1.Kirish imkoniyatini foydalanuvchilar bo‘ylab taqsimlash — kirish matritsasini ishlab chiqilganligi. 2.Ichki va tashqi foydalanuvchilar uchun identifikatsiya/autentifikatsiya qilish qoidalari va tartib-taomillarini tartibga solinganligi. 3.Foydalanuvchilar va uskunalarni tarmoqqa ulash qoidalari va tartib-taomillarini tartibga solinganligi	0,7	0,7	0,7	0,5	0,5	0.6	0.7	0.6	0,5	0,5	0,5	0.6	0.7	0,6	0,8	0,6	0,6
	VO02	1.Ilovalar va ma’lumotlarga kirish qoidalarini tartibga solinganligi 2.Kirishga muvaffaqiyatsiz urinishlar sonini cheklanganligi. 3.Faol bo‘lmaganda foydalanuvchining kirish seansini bloklanishi.	0,8	0,8	0,8	0,7	0,7	0,7	0,7	0,7	0,7	0,7	0,7	0,7	0,7	0,7	0,5	0,7	0,7
	VO03	1. Konfidensial ma’lumotlarni uchinchi shaxslarga oshkor qilmaslik to‘g‘risidagi shartnoma 2.Buyurtmachilar yoki uchinchi shaxslarning nazoratli xizmat ko‘rsatishi. 2.Masofaviy ulanishlarni cheklanganligi. 3.Sinov dasturiy ta’minotlarni amaldagi tizimga o‘rnatilmasligi.	0,8	0,8	0,8	0,8	0,8	0,8	0,8	0,8	0,8	0,8	0,8	0,8	0,8	0,8	0,8	0,8	0,8
	VO04	1. Monitoring tizimlaridan foydalanish 2.Mablag‘lar jurnallarini davriy tekshirish	0,3	0,3	0,3	0,3	0,3	0,3	0,3	0,3	0,3	0,3	0,3	0,3	0,3	0,2	-	0,2	0,2

Tashkiliy-texnik chora-tadbirlar-ning nomi		Bajariladigan chora- tadbirlarning nomi	hemis.buxdu.uz	masofaviy.buxdu.uz	uniwork.buxdu.uz	moodle.buxdu.uz	citrus.buxdu.uz	srep.buxdu.uz	pedskills.buxdu.uz	student.buxdu.uz	buxdu.uz	Korporativ elektron pochta	Journal.buxdu.uz	Universitet fayl serveri	IP telefoniya	Ishchi stansiyalar	Server uskunalari	Kirish chiqishni nazorat qilish tizimi	Videokuzatuv tizimi
	VO05	1.Audit o‘tkazish rejalarining mavjudligi. 2.Tashqi audit o‘tkazishda autsorsing tashkilotlarini jalb qilinishi. 3.Audit natijalarining tahlil qilinishi. 4.Audit o‘tkazish uchun maxsus bo‘linma (mutaxassis) mavjudligi.	0,4	0,4	0,4	0,4	0,4	0,4	0,4	0,4	0,4	0,4	0,4	0,4	0,4	0,4	0,6	0,4	0,4
	VO06	1.Risk va tahdidlarni baholash tartibining belgilanganligi. 2.Risklar bahosi natijalarining tahlil qilinishi. 3.Risk bahosi bo‘yicha choralarning belgilanishi.	0,8	0,8	0,8	0,8	0,8	0,8	0,8	0,8	0,8	0,8	0,8	0,8	0,8	0,8	0,8	0,8	0,8
	VO07	1.Nosozliklarni qayd etish jurnalining mavjudligi va yuritilib borilishi. 2.Texnik nosozliklar bilan bog‘liq insidentlarga javob qaytarish qoidalari va tartib-taomillarini tartibga solinganligi.	0,6	0,6	0,6	0,7	0,7	0,7	0,7	0,7	0,7	0,7	0,7	0,7	0,7	0,4	-	0,4	0,4
	VO08	1.Belgilangan talablar asosida davriy xizmat ko‘rsatish tizimi yo‘lga qo‘yilganligi. 2 Serverlarning operatsion tizimlari yangilanib borilishi. 3. Operatsion tizimlarni yangilashda nazorat mavjudligi.	0,6	0,6	0,6	0,6	0,6	0,6	0,6	0,6	0,6	0,6	0,6	0,6	0,6	0,4	-	0,4	0,4
	VO09	1.Infratuzilmaga xizmat ko‘rsatish bilan bog‘liq alohida rejalarining mavjudligi. 2.Xizmat ko‘rsatish darajasini nazorat qilish tizimining o‘matilganligi va nazorat qilinishi.	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,4	-	0,4	0,4

Tashkiliy-texnik chora-tadbirlar-ning nomi		Bajariladigan chora- tadbirlarning nomi	hemis.buxdu.uz	masofaviy.buxdu.uz	uniwork.buxdu.uz	moodle.buxdu.uz	citrus.buxdu.uz	srep.buxdu.uz	pedskills.buxdu.uz	student.buxdu.uz	buxdu.uz	Korporativ elektron pochta	Journal.buxdu.uz	Universitet fayl serveri	IP telefoniya	Ishchi stansiyalar	Server uskunalari	Kirish chiqishni nazorat qilish tizimi	Videokuzatuv tizimi
	VO10	1.O‘zgartirishlar kiritish tartibining mavjudligi. 2.Kiritilgan o‘zgartirishlar tegishli jurnallarda qayd etilishi. 3.O‘zgartirishlar bo‘yicha Log fayllarni tahlil qilinishi.	0,8	0,8	0,8	0,7	0,7	0,4	0,7	0,4	0,7	0,7	0,7	0,4	0,7	0,5	-	0,5	0,5
	VO11	AXBT hujjatlarini ishlab chiqish va ro‘yxatdan o‘tkazish	0,6	0,6	0,6	0,6	0,6	0,6	0,6	0,6	0,6	0,6	0,6	0,6	0,6	0,6	0,6	0,6	0,6
	VO12	AXBT yozuvlarini nazorat qilish tartibining mavjudligi	0,1	0,1	0,1	0,1	0,1	0,1	0,1	0,1	0,1	0,1	0,1	0,1	0,1	0,1	0,1	0,1	0,1
	VO13	Ommaga ochiq axborotni avtorizatsiya qilish tartibining mavjudligi	0,2	0,2	0,2	0,2	0,2	0,2	0,2	0,2	0,2	0,2	0,2	0,2	0,2	0,2	0,2	0,2	0,2
	VO14	1.Javobgarlikni taqsimlash 2.Ish tavsiflari	0,8	0,8	0,8	0,8	0,8	0,8	0,8	0,8	0,8	0,8	0,8	0,8	0,8	0,8	0,8	0,8	0,8
	VO15	1.Uzluksiz ish jarayonini ta’minlash rejalarining mavjudligi. 2.Rejaga asosan belgilangan ishlarning o‘z vaqtida bajarilishi. 3.Monitoring tizimining mavjudligi.	0,7	0,7	0,7	0,7	0,7	0,5	0,7	0,5	0,7	0,7	0,7	0,5	0,7	0,6	0,5	0,6	0,6
	VO16	1. Elektron pochta siyosatiga ega bo‘lish 2.Elektron pochta siyosatiga rioya etilishini nazorat qilish	-	-	-	-	-	-	0,5	-	-	-	-	-	0,5	-	-	-	-
	VO17	1. Operatsion tizimlarga dasturiy ta’minotni o‘rnatish tartibining mavjudligi	0,2	0,2	0,2	0,2	0,2	0,2	0,2	0,2	0,2	0,2	0,2	0,2	0,2	0,2	-	0,2	0,2

Tashkiliy-texnik chora-tadbirlar-ning nomi		Bajariladigan chora- tadbirlarning nomi	hemis.buxdu.uz	masofaviy.buxdu.uz	uniwork.buxdu.uz	moodle.buxdu.uz	citrus.buxdu.uz	srep.buxdu.uz	pedskills.buxdu.uz	student.buxdu.uz	buxdu.uz	Korporativ elektron pochta	Journal.buxdu.uz	Universitet fayl serveri	IP telefoniya	Ishchi stansiyalar	Server uskunalari	Kirish chiqishni nazorat qilish tizimi	Videokuzatuv tizimi
	VO18	1.Konfidensial ma’lumotlar bilan ishlash tartibi 2. Talablarga rioya etilishini nazorat qilish 3.Qonunbuzarlarga qarshi choralar va ularni qo‘llash	0,7	0,7	0,7	0,7	0,7	0,7	0,7	0,7	0,7	0,7	0,7	0,7	0,7	0,7	0,7	0,7	0,7
	VO19	Lavozim yo‘riqnomalarida javobgarlikning belgilanganligi	0,8	0,8	0,8	0,8	0,8	0,8	0,8	0,8	0,8	0,8	0,8	0,8	0,8	0,8	0,8	0,8	0,8
	VO20	Xodimlar bilan tuzilgan mehnat shartnomalarida javobgarlikning mavjudligi	0,6	0,6	0,6	0,6	0,6	0,6	0,6	0,6	0,6	0,6	0,6	0,6	0,6	0,6	0,6	0,6	0,6
	VO21	Intizomiy choralar	0,3	0,3	0,3	0,3	0,3	0,3	0,3	0,3	0,3	0,3	0,3	0,3	0,3	0,3	0,3	0,3	0,3
	VO22	1. Mobil qurilmalardan foydalanish siyosatiga ega bo‘lish 2. Mobil qurilmadan foydalanish siyosatiga rioya etilishini nazorat qilish	0,7	0,7	0,7	0,7	0,7	0,7	0,7	0,7	0,7	0,7	0,7	0,7	0,7	0,7	0,7	0,7	0,7
	VO23	1.Axborot tizimlarining asosiy server qurilmalari zaxira server qurilmasiga ma’lumotlar bazasini doimiy ravishda replikatsiya qilishi. 2.Reja asosida axborot tizimlarining ma’lumotlar bazasini tashqi xotiraga replikatsiya qilinishi. Ma’lumotlarni zaxiralash va tiklash yo‘lga qo‘yilganligi. 3.Zaxira olish uchun alohida saqlash vositalari ajratilganligi. Konfiguratsiya ma’lumotlarini muntazam ravishda nusxalash yo‘lga qo‘yilganligi.	0,6	0,6	0,6	0,6	0,6	0,6	0,6	0,6	0,6	0,6	0,6	0,6	0,6	0,6	0,6	0,6	0,6

Tashkiliy-texnik chora-tadbirlar-ning nomi		Bajariladigan chora- tadbirlarning nomi	hemis.buxdu.uz	masofaviy.buxdu.uz	uniwork.buxdu.uz	moodle.buxdu.uz	citrus.buxdu.uz	srep.buxdu.uz	pedskills.buxdu.uz	student.buxdu.uz	buxdu.uz	Korporativ elektron pochta	Journal.buxdu.uz	Universitet fayl serveri	IP telefoniya	Ishchi stansiyalar	Server uskunalari	Kirish chiqishni nazorat qilish tizimi	Videokuzatuv tizimi
	VO24	"Toza stol" va "toza ekran" siyosatiga ega bo‘lish va ularga rioya qilish	0,1	0,1	0,1	0,1	0,1	0,1	0,1	0,1	0,1	0,1	0,1	0,1	0,1	0,1	0,1	0,1	0,1
	VO25	1.Litsenziyalangan axborotni qayta ishlash vositalaridan foydalanish tartibining yo‘lga qo‘yilganligi. 2.Axborotni qayta ishlash vositalarida guruhli xavfsizlik siyosatining joriy qilinganligi. 3. Foydalanuvchi harakatlari monitoring qilinishi.	0,7	0,7	0,7	0,7	0,7	0,7	0,7	0,7	0,7	0,7	0,7	0,7	0,7	0,7	0,7	0,7	0,7
	VO26	1. Monitoring tizimining mavjudligi. 2.IDPS hujumni aniqlash va oldini olish vositalarini qo‘llanilganligi. 3.Foydalanilishi taqiqlangan saytlarga yoki sayt turlariga kirishni bloklanganligi. 4.Ichki va tashqi foydalanuvchilar uchun identifikatsiya / autentifikatsiya qilish qoidalari va tartib-taomillarini tartibga solinganligi.	0,4	0,4	0,4	0,4	0,4	0,4	0,4	0,4	0,4	0,4	0,4	0,4	0,4	0,4	-	0,4	0,4
	VO27	1.WSUS (windows server update services) tizimi offline/online rejimi mavjudligi. 2.Operatsion tizimlarni doimiy yangilash mavjudligi. 3.Chiqayotgan zaifliklarni monitoring va tahlil qilish tartibining mavjudligi.	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,7	-	0,7	0,7
	VO28	1.Litsenziyalangan dasturiy ta’minotdan foydalanish mavjudligi. 2.Rasmiy dasturiy ta’minotlardan foydalanilishi. 3.Tekshirilmagan dasturiy ta’minotlardan foydalanilmasligi.	0,3	0,3	0,3	0,3	0,3	0,3	0,3	0,3	0,3	0,3	0,3	0,3	0,3	0,3	-	0,3	0,3

5-jadval: Axborot xavfsizligi riskini tahlil qilishning miqdoriy usul natijasi

Tahdid turlari	Tahdid turlari	Tahdidning nomlanishi	Tahdidning sodir bo‘lish ehtimolligi	Tashkiliy-texnik tadbirlarning bajarilganlik holati	Salbiy oqibat yuzaga kelish riski
hemis.buxdu.uz 6 (axborotning qiymati – 8)					
Jismoniy tahdidlar	TP01	Yong‘in	0,2	0,18	0,2 (0,3)
	TP02	Suv toshishi	0,2	0,16	0,2 (0,3)
	TP03	Ifloslanish, zararli radiatsiya	0,3	0,15	0,3 (0,4)
	TP04	Katta baxtsiz hodisa	0,3	0,17	0,3 (0,4)
	TP05	Portlash, halokat	0,2	0,14	0,2 (0,2)
	TP06	Chang, korroziya, muzlash	0,1	0,17	0,1 (0,1)
Tabiiy tahdidlar	TN01	Iqlim hodisasi	0,4	0,12	0,3 (0,4)
	TN02	Seysmik hodisa	0,4	0,15	0,4 (0,5)
	TN03	Vulqon hodisasi	0	0,17	0 (0)
	TN04	Meteorologik hodisa	0,3	0,17	0,3 (0,4)
	TN05	Suv toshqini	0,4	0,17	0,4 (0,5)
	TN06	Pandemiya/epidemiya hodisasi	0,4	0,15	0,4 (0,5)
Infratuzilmaning ishlamay qolishi	TI01	Ta’minot tizimining ishdan chiqishi	0,6	0,3	1,1 (1,4)
	TI02	Sovutish yoki shamollatish tizimining ishlamay qolishi	0,7	0,23	0,9 (1,3)
	TI03	Energiya ta’minotining buzilishi	0,7	0,27	1,1 (1,5)
	TI04	Telekommunikatsiya tarmog‘ining ishdan chiqishi	0,8	0,37	1,8 (2,4)
	TI05	Telekommunikatsiya uskunalari ishlamay qolishi	0,8	0,33	1,6 (2,1)
	TI06	Elektromagnit nurlanish	0,4	0,1	0,2 (0,3)
	TI07	Termal nurlanish	0,4	0,1	0,2 (0,3)
	TI08	Elektromagnit impulslar	0,4	0,1	0,2 (0,3)
Texnik muvaffaqiyatsizliklar	TT01	Qurilma yoki tizimning ishdan chiqishi	0,7	0.4	1,7 (2,2)
	TT02	Axborot tizimining to‘yinganligi	0,5	0,28	0,8 (1,1)
	TT03	Axborot tizimini ta’mirlash qobiliyatini buzilishi	0,4	0,37	0,9 (1,2)
Xodimlar harakati	TH01	Terrorizm, hujumlar, sabotaj	0,2	0,33	0,4 (0,5)
	TH02	Ijtimoiy muhandislik	0,2	0,3	0,4 (0,5)
	TH03	Qurilmaning nurlanishini ushlab turish	0,4	0,5	1,2 (1,6)
	TH04	Masofaviy monitoring	0,2	0,42	0,5 (0,7)
	TH05	Tinglash	0,6	0,28	1 (1,3)
	TH06	Ma’lumotlarni tashuvchi vositalarni yoki hujjatlarni o‘g‘irlash	0,6	0,3	1,1 (1,4)
	TH07	Uskunani o‘g‘irlash	0,4	0,35	0,8 (1,1)
	TH08	Raqamli identifikatsiya ma’lumotlarini o‘g‘irlash	0,5	0,28	0,8 (1,1)

Tahdid turlari	Tahdid turlari	Tahdidning nomlanishi	Tahdidning sodir bo‘lish ehtimolligi	Tashkiliy-texnik tadbirlarning bajarilganlik holati	Salbiy oqibat yuzaga kelish riski
	TH09	Tashlab yuborilgan yoki takror ishlatilayotgan ma’lumot tashuvchi qurilmalardan ma’lumot olish	0,4	0.44	1 (1.4)
	TH10	Axborotni oshkor qilish	0,6	0.45	1,6 (2,2)
	TH11	Ishonchsiz manbalardan ma’lumotlarni kiritish	0,5	0,52	1,6 (2,1)
	TH12	Uskunani buzish	0,4	0,29	0,7 (0,9)
	TH13	Dasturiy ta’minotni buzish	0,4	0,33	0,8 (1)
	TH14	Veb-aloqa orqali Drive-by ekspluatatsiyasidan foydalanish	0,6	0,32	1,1 (1,5)
	TH15	Takroriy hujum, o‘rtadagi odam hujumi	0,5	0,33	1 (1,3)
	TH16	Shaxsiy ma’lumotlarni ruxsatsiz qayta ishlash	0,6	0,31	1,1 (1,5)
	TH17	Obyektlarga ruxsatsiz kirish	0,4	0,23	0,6 (0,7)
	TH18	Qurilmalardan ruxsatsiz foydalanish	0,4	0,26	0,6 (0,8)
	TH19	Qurilmalardan noto‘g‘ri foydalanish	0,6	0,2	0,7 (1)
	TH20	Qurilmalar yoki ma’lumot tashuvchilarni shikastlash	0,4	0,44	1 (1,4)
	TH21	Soxta dasturiy ta’minotni nusxalash	0,5	0,39	1,2 (1,6)
	TH22	Qalbaki yoki nusxalangan dasturiy ta’minotdan foydalanish	0,4	0,38	0,9 (1,2)
	TH23	Ma’lumotlarga shikast yetkazish	0,5	0,32	1 (1,3)
	TH24	Noqonuniy ma’lumotlarni qayta ishlash	0,4	0,45	1,1 (1,4)
	TH25	Zararli dasturlarni yuborish yoki tarqatish	0,6	0,325	1,1 (1,5)
	TH26	Joylashuvni aniqlash	0,2	0,25	0,3 (0,4)
Xizmatlar yoki funksiyalarni buzish	TC01	Foydalanishda xatoliklar	0,5	0,41	1,2 (1,6)
	TC02	Huquqlar yoki ruxsatlarni suiiste’mol qilish	0,6	0,25	0,9 (1,2)
	TC03	Huquqlar yoki ruxsatlarni soxtalashtirish	0,5	0,27	0,8 (1,1)
	TC04	Harakatlarni rad etish	0,7	0,39	1,6 (2,1)
Tashkiliy tahdidlar	TO01	Xodimlarning etishmasligi	0,5	0,37	1,1 (1,5)
	TO02	Resurslarning etishmasligi	0,6	0,33	1,3 (1,6)
	TO03	Xizmat ko‘rsatuvchining to‘lovga layoqatsizligi	0,4	0,37	0,9 (1,2)
	TO04	Qonunchilik yoki normativ-huquqiy hujjatlarning buzilishi	0,6	0,4	1,4 (1,9)
Saqlash tizimlari va infratuzilmasiga tahdidlar	TD01	Ruxsat etilmagan foydalanish	0,6	0,31	1,1 (1,5)
	TD02	Ruxsatsiz kirish	0,4	0,23	0,6 (0,7)
	TD03	Me’yoriy hujjatlarga rioya qilmaslik uchun yuridik javobgarlik	0,6	0,4	1,4 (1,9)
	TD04	Saqlash tizimlariga DoS va DDoS hujumlar	0.7	-	-
	TD05	Ma’lumotlarga zarar etkazish, o‘zgartirish va yo‘q qilish	0,6	0,3	1,1 (1,4)
	TD06	Ma’lumotlar sizib chiqishi	0,6	0,45	1,6 (2,2)
	TD07	Axborot tashuvchi yoki saqlovchi vositani o‘g‘irlash yoki tasodifiy yo‘qotish	0,4	0,44	1 (1,4)
	TD08	Zararli dastur hujumi yoki inyeksiyasi	0,6	0,325	1,1 (1,5)

Tahdid turlari	Tahdid turlari	Tahdidning nomlanishi	Tahdidning sodir bo‘lish ehtimolligi	Tashkiliy-texnik tadbirlarning bajarilganlik holati	Salbiy oqibat yuzaga kelish riski
	TD09	Noto‘g‘ri ishlov berish yoki foydalanish tugagandan keyin utilizatsiya qilish	0,4	0.44	1 (1.4)
masofaviy.buxdu.uz 6 (axborotning qiymati – 8)					
Jismoniy tahdidlar	TP01	Yong‘in	0,2	0,18	0,2 (0,3)
	TP02	Suv toshishi	0,2	0,16	0,2 (0,3)
	TP03	Ifloslanish, zararli radiatsiya	0,3	0,15	0,3 (0,4)
	TP04	Katta baxtsiz hodisa	0,3	0,17	0,3 (0,4)
	TP05	Portlash, halokat	0,2	0,14	0,2 (0,2)
	TP06	Chang, korroziya, muzlash	0,1	0,17	0,1 (0,1)
Tabiiy tahdidlar	TN01	Iqlim hodisasi	0,4	0,12	0,3 (0,4)
	TN02	Seysmik hodisa	0,4	0,15	0,4 (0,5)
	TN03	Vulqon hodisasi	0	0,17	0 (0)
	TN04	Meteorologik hodisa	0,3	0,17	0,3 (0,4)
	TN05	Suv toshqini	0,4	0,17	0,4 (0,5)
	TN06	Pandemiya/epidemiya hodisasi	0,4	0,15	0,4 (0,5)
Infratuzilmaning ishlamay qolishi	TI01	Ta’minot tizimining ishdan chiqishi	0,6	0,3	1,1 (1,4)
	TI02	Sovutish yoki shamollatish tizimining ishlamay qolishi	0,7	0,23	0,9 (1,3)
	TI03	Energiya ta’minotining buzilishi	0,7	0,27	1,1 (1,5)
	TI04	Telekommunikatsiya tarmog‘ining ishdan chiqishi	0,8	0,37	1,8 (2,4)
	TI05	Telekommunikatsiya uskunalari ishlamay qolishi	0,8	0,33	1,6 (2,1)
	TI06	Elektromagnit nurlanish	0,4	0,1	0,2 (0,3)
	TI07	Termal nurlanish	0,4	0,1	0,2 (0,3)
	TI08	Elektromagnit impulslar	0,4	0,1	0,2 (0,3)
Texnik muvaffaqiyatsizliklar	TT01	Qurilma yoki tizimning ishdan chiqishi	0,7	0.4	1,7 (2,2)
	TT02	Axborot tizimining to‘yinganligi	0,5	0,28	0,8 (1,1)
	TT03	Axborot tizimini ta’mirlash qobiliyatini buzilishi	0,4	0,37	0,9 (1,2)
Xodimlar harakati	TH01	Terrorizm, hujumlar, sabotaj	0,2	0,33	0,4 (0,5)
	TH02	Ijtimoiy muhandislik	0,2	0,3	0,4 (0,5)
	TH03	Qurilmaning nurlanishini ushlab turish	0,4	0,5	1,2 (1,6)
	TH04	Masofaviy monitoring	0,2	0,42	0,5 (0,7)
	TH05	Tinglash	0,6	0,28	1 (1,3)
	TH06	Ma’lumotlarni tashuvchi vositalarni yoki hujjatlarni o‘g‘irlash	0,6	0,3	1,1 (1,4)
	TH07	Uskunani o‘g‘irlash	0,4	0,35	0,8 (1,1)
	TH08	Raqamli identifikatorni yoki identifikatsiya ma’lumotlarini o‘g‘irlash	0,5	0,28	0,8 (1,1)
	TH09	Tashlab yuborilgan yoki takror ishlatilayotgan ma’lumot tashuvchi qurilmalardan ma’lumot olish	0,4	0.44	1 (1.4)

Tahdid turlari	Tahdid turlari	Tahdidning nomlanishi	Tahdidning sodir bo‘lish ehtimolligi	Tashkiliy-texnik tadbirlarning bajarilganlik holati	Salbiy oqibat yuzaga kelish riski
	TH10	Axborotni oshkor qilish	0,6	0.45	1,6 (2,2)
	TH11	Ishonchsiz manbalardan ma’lumotlarni kiritish	0,5	0,52	1,6 (2,1)
	TH12	Uskunani buzish	0,4	0,29	0,7 (0,9)
	TH13	Dasturiy ta’minotni buzish	0,4	0,33	0,8 (1)
	TH14	Veb-aloqa orqali Drive-by ekspluatatsiyasidan foydalanish	0,6	0,32	1,1 (1,5)
	TH15	Takroriy hujum, o‘rtadagi odam hujumi	0,5	0,33	1 (1,3)
	TH16	Shaxsiy ma’lumotlarni ruxsatsiz qayta ishlash	0,6	0,31	1,1 (1,5)
	TH17	Obyektlarga ruxsatsiz kirish	0,4	0,23	0,6 (0,7)
	TH18	Qurilmalardan ruxsatsiz foydalanish	0,4	0,26	0,6 (0,8)
	TH19	Qurilmalardan noto‘g‘ri foydalanish	0,6	0,2	0,7 (1)
	TH20	Qurilmalar yoki ma’lumot tashuvchilarni shikastlash	0,4	0,44	1 (1,4)
	TH21	Soxta dasturiy ta’minotni nusxalash	0,5	0,39	1,2 (1,6)
	TH22	Qalbaki yoki nusxalangan dasturiy ta’minotdan foydalanish	0,4	0,38	0,9 (1,2)
	TH23	Ma’lumotlarga shikast yetkazish	0,5	0,32	1 (1,3)
	TH24	Noqonuniy ma’lumotlarni qayta ishlash	0,4	0,45	1,1 (1,4)
	TH25	Zararli dasturlarni yuborish yoki tarqatish	0,6	0,325	1,1 (1,5)
	TH26	Joylashuvni aniqlash	0,2	0,25	0,3 (0,4)
Xizmatlar yoki funksiyalarni buzish	TC01	Foydalanishda xatoliklar	0,5	0,41	1,2 (1,6)
	TC02	Huquqlar yoki ruxsatlarni suiiste’mol qilish	0,6	0,25	0,9 (1,2)
	TC03	Huquqlar yoki ruxsatlarni soxtalashtirish	0,5	0,27	0,8 (1,1)
	TC04	Harakatlarni rad etish	0,7	0,39	1,6 (2,1)
Tashkiliy tahdidlar	TO01	Xodimlarning etishmasligi	0,5	0,37	1,1 (1,5)
	TO02	Resurslarning etishmasligi	0,6	0,33	1,3 (1,6)
	TO03	Xizmat ko‘rsatuvchining to‘lovga layoqatsizligi	0,4	0,37	0,9 (1,2)
	TO04	Qonunchilik yoki normativ-huquqiy hujjatlarning buzilishi	0,6	0,4	1,4 (1,9)
Saqlash tizimlari va infratuzilmasiga tahdidlar	TD01	Ruxsat etilmagan foydalanish	0,6	0,43	0,8 (1,3)
	TD02	Ruxsatsiz kirish	0,4	0,2	0,2 (0,4)
	TD03	Qonunlar va me’yoriy hujjatlarga rioya qilmaslik uchun yuridik javobgarlik	0,6	0,4	0,7 (1,2)
	TD04	Saqlash tizimlariga DoS va DDoS hujumlar	0.7	0,6	1,26 (2,1)
	TD05	Ma’lumotlarga zarar etkazish, o‘zgartirish va yo‘q qilish	0,6	0,3	0,5 (0,9)
	TD06	Ma’lumotlar sizib chiqishi	0,6	0,5	0,9 (1,5)
	TD07	Axborot tashuvchi yoki saqlovchi vositani o‘g‘irlash yoki tasodifiy yo‘qotish	0,4	0,54	0,6 (1,1)
	TD08	Zararli dastur hujumi yoki inyeksiyasi	0,6	0,39	0.7 (1,2)
	TD09	Noto‘g‘ri ishlov berish yoki foydalanish tugagandan keyin utilizatsiya qilish	0,4	0,4	0,5 (1)

Tahdid turlari	Tahdid turlari	Tahdidning nomlanishi	Tahdidning sodir bo‘lish ehtimolligi	Tashkiliy-texnik tadbirlarning bajarilganlik holati	Salbiy oqibat yuzaga kelish riski
uniwork.buxdu.uz 6 (axborotning qiymati – 8)					
Jismoniy tahdidlar	TP01	Yong‘in	0,2	0,18	0,2 (0,3)
	TP02	Suv toshishi	0,2	0,16	0,2 (0,3)
	TP03	Ifloslanish, zararli radiatsiya	0,3	0,15	0,3 (0,4)
	TP04	Katta baxtsiz hodisa	0,3	0,17	0,3 (0,4)
	TP05	Portlash, halokat	0,2	0,14	0,2 (0,2)
	TP06	Chang, korroziya, muzlash	0,1	0,17	0,1 (0,1)
Tabiiy tahdidlar	TN01	Iqlim hodisasi	0,4	0,12	0,3 (0,4)
	TN02	Seysmik hodisa	0,4	0,15	0,4 (0,5)
	TN03	Vulqon hodisasi	0	0,17	0 (0)
	TN04	Meteorologik hodisa	0,3	0,17	0,3 (0,4)
	TN05	Suv toshqini	0,4	0,17	0,4 (0,5)
	TN06	Pandemiya/epidemiya hodisasi	0,4	0,15	0,4 (0,5)
Infratuzilmaning ishlamay qolishi	TI01	Ta’minot tizimining ishdan chiqishi	0,6	0,3	1,1 (1,4)
	TI02	Sovutish yoki shamollatish tizimining ishlamay qolishi	0,7	0,23	0,9 (1,3)
	TI03	Energiya ta’minotining buzilishi	0,7	0,27	1,1 (1,5)
	TI04	Telekommunikatsiya tarmog‘ining ishdan chiqishi	0,8	0,37	1,8 (2,4)
	TI05	Telekommunikatsiya uskunalari ishlamay qolishi	0,8	0,33	1,6 (2,1)
	TI06	Elektromagnit nurlanish	0,4	0,1	0,2 (0,3)
	TI07	Termal nurlanish	0,4	0,1	0,2 (0,3)
	TI08	Elektromagnit impulslar	0,4	0,1	0,2 (0,3)
Texnik muvaffaqiyatsizliklar	TT01	Qurilma yoki tizimning ishdan chiqishi	0,7	0.4	1,7 (2,2)
	TT02	Axborot tizimining to‘yinganligi	0,5	0,28	0,8 (1,1)
	TT03	Axborot tizimini ta’mirlash qobiliyatini buzilishi	0,4	0,37	0,9 (1,2)
Xodimlar harakati	TH01	Terrorizm, hujumlar, sabotaj	0,2	0,33	0,4 (0,5)
	TH02	Ijtimoiy muhandislik	0,2	0,3	0,4 (0,5)
	TH03	Qurilmaning nurlanishini ushlab turish	0,4	0,5	1,2 (1,6)
	TH04	Masofaviy monitoring	0,2	0,42	0,5 (0,7)
	TH05	Tinglash	0,6	0,28	1 (1,3)
	TH06	Ma’lumotlarni tashuvchi vositalarni yoki hujjatlarni o‘g‘irlash	0,6	0,3	1,1 (1,4)
	TH07	Uskunani o‘g‘irlash	0,4	0,35	0,8 (1,1)
	TH08	Raqamli identifikatsiya ma’lumotlarini o‘g‘irlash	0,5	0,28	0,8 (1,1)
	TH09	Tashlab yuborilgan yoki takror ishlatilayotgan ma’lumot tashuvchi qurilmalardan ma’lumot olish	0,4	0.44	1 (1.4)
	TH10	Axborotni oshkor qilish	0,6	0.45	1,6 (2,2)
	TH11	Ishonchsiz manbalardan ma’lumotlarni kiritish	0,5	0,52	1,6 (2,1)
	TH12	Uskunani buzish	0,4	0,29	0,7 (0,9)

Tahdid turlari	Tahdid turlari	Tahdidning nomlanishi	Tahdidning sodir bo‘lish ehtimolligi	Tashkiliy-texnik tadbirlarning bajarilganlik holati	Salbiy oqibat yuzaga kelish riski
	TH13	Dasturiy ta’minotni buzish	0,4	0,33	0,8 (1)
	TH14	Veb-aloqa orqali Drive-by ekspluatatsiyasidan foydalanish	0,6	0,32	1,1 (1,5)
	TH15	Takroriy hujum, o‘rtadagi odam hujumi	0,5	0,33	1 (1,3)
	TH16	Shaxsiy ma’lumotlarni ruxsatsiz qayta ishlash	0,6	0,31	1,1 (1,5)
	TH17	Obyektlarga ruxsatsiz kirish	0,4	0,23	0,6 (0,7)
	TH18	Qurilmalardan ruxsatsiz foydalanish	0,4	0,26	0,6 (0,8)
	TH19	Qurilmalardan noto‘g‘ri foydalanish	0,6	0,2	0,7 (1)
	TH20	Qurilmalar yoki ma’lumot tashuvchilarni shikastlash	0,4	0,44	1 (1,4)
	TH21	Soxta dasturiy ta’minotni nusxalash	0,5	0,39	1,2 (1,6)
	TH22	Qalbaki yoki nusxalangan dasturiy ta’minotdan foydalanish	0,4	0,38	0,9 (1,2)
	TH23	Ma’lumotlarga shikast yetkazish	0,5	0,32	1 (1,3)
	TH24	Noqonuniy ma’lumotlarni qayta ishlash	0,4	0,45	1,1 (1,4)
	TH25	Zararli dasturlarni yuborish yoki tarqatish	0,6	0,325	1,1 (1,5)
	TH26	Joylashuvni aniqlash	0,2	0,25	0,3 (0,4)
Xizmatlar yoki funksiyalarni buzish	TC01	Foydalanishda xatoliklar	0,5	0,41	1,2 (1,6)
	TC02	Huquqlar yoki ruxsatlarni suiiste’mol qilish	0,6	0,25	0,9 (1,2)
	TC03	Huquqlar yoki ruxsatlarni soxtalashtirish	0,5	0,27	0,8 (1,1)
	TC04	Harakatlarni rad etish	0,7	0,39	1,6 (2,1)
Tashkiliy tahdidlar	TO01	Xodimlarning etishmasligi	0,5	0,37	1,1 (1,5)
	TO02	Resurslarning etishmasligi	0,6	0,33	1,3 (1,6)
	TO03	Xizmat ko‘rsatuvchining to‘lovga layoqatsizligi	0,4	0,37	0,9 (1,2)
	TO04	Qonunchilik yoki normativ-huquqiy hujjatlarning buzilishi	0,6	0,4	1,4 (1,9)
Saqlash tizimlari va infratuzilmasiga tahdidlar	TD01	Ruxsat etilmagan foydalanish	0,6	0,43	1,8 (1,8)
	TD02	Ruxsatsiz kirish	0,4	0,19	0,5 (0,5)
	TD03	Qonunlar va me’yoriy hujjatlarga rioya qilmaslik uchun yuridik javobgarlik	0,6	0,4	1,7 (1,7)
	TD04	Saqlash tizimlariga DoS va DDoS hujumlar	0.7	-	-
	TD05	Ma’lumotlarga zarar etkazish, o‘zgartirish va yo‘q qilish	0,6	0,31	1,3 (1,3)
	TD06	Ma’lumotlar sizib chiqishi	0,6	0,6	2,5 (2,8)
	TD07	Axborot tashuvchi yoki saqlovchi vositani o‘g‘irlash yoki tasodifiy yo‘qotish	0,4	0,5	1,4 (1,4)
	TD08	Zararli dastur hujumi yoki inyeksiyasi	0,6	0,4	1,7 (1,7)
	TD09	Noto‘g‘ri ishlov berish yoki foydalanish tugagandan keyin utilizatsiya qilish	0,4	0,42	1,2 (1,2)
moodle.buxdu.uz 3 (axborotning qiymati – 5)					
Jismoniy tahdidlar	TP01	Yong‘in	0,2	0,18	0,2 (0,3)
	TP02	Suv toshishi	0,2	0,16	0,2 (0,3)

Tahdid turlari	Tahdid turlari	Tahdidning nomlanishi	Tahdidning sodir bo‘lish ehtimolligi	Tashkiliy-texnik tadbirlarning bajarilganlik holati	Salbiy oqibat yuzaga kelish riski
	TP03	Ifloslanish, zararli radiatsiya	0,3	0,15	0,3 (0,4)
	TP04	Katta baxtsiz hodisa	0,3	0,17	0,3 (0,4)
	TP05	Portlash, halokat	0,2	0,14	0,2 (0,2)
	TP06	Chang, korroziya, muzlash	0,1	0,17	0,1 (0,1)
Tabiiy tahdidlar	TN01	Iqlim hodisasi	0,4	0,12	0,3 (0,4)
	TN02	Seysmik hodisa	0,4	0,15	0,4 (0,5)
	TN03	Vulqon hodisasi	0	0,17	0 (0)
	TN04	Meteorologik hodisa	0,3	0,17	0,3 (0,4)
	TN05	Suv toshqini	0,4	0,17	0,4 (0,5)
	TN06	Pandemiya/epidemiya hodisasi	0,4	0,15	0,4 (0,5)
Infratuzilmaning ishlamay qolishi	TI01	Ta’minot tizimining ishdan chiqishi	0,6	0,3	1,1 (1,4)
	TI02	Sovutish yoki shamollatish tizimining ishlamay qolishi	0,7	0,23	0,9 (1,3)
	TI03	Energiya ta’minotining buzilishi	0,7	0,27	1,1 (1,5)
	TI04	Telekommunikatsiya tarmog‘ining ishdan chiqishi	0,8	0,37	1,8 (2,4)
	TI05	Telekommunikatsiya uskunalari ishlamay qolishi	0,8	0,33	1,6 (2,1)
	TI06	Elektromagnit nurlanish	0,4	0,1	0,2 (0,3)
	TI07	Termal nurlanish	0,4	0,1	0,2 (0,3)
	TI08	Elektromagnit impulslar	0,4	0,1	0,2 (0,3)
Texnik muvaffaqiyatsizliklar	TT01	Qurilma yoki tizimning ishdan chiqishi	0,7	0.4	1,7 (2,2)
	TT02	Axborot tizimining to‘yinganligi	0,5	0,28	0,8 (1,1)
	TT03	Axborot tizimini ta’mirlash qobiliyatini buzilishi	0,4	0,37	0,9 (1,2)
Xodimlar harakati	TH01	Terrorizm, hujumlar, sabotaj	0,2	0,33	0,4 (0,5)
	TH02	Ijtimoiy muhandislik	0,2	0,3	0,4 (0,5)
	TH03	Qurilmaning nurlanishini ushlab turish	0,4	0,5	1,2 (1,6)
	TH04	Masofaviy monitoring	0,2	0,42	0,5 (0,7)
	TH05	Tinglash	0,6	0,28	1 (1,3)
	TH06	Ma’lumotlarni tashuvchi vositalarni yoki hujjatlarni o‘g‘irlash	0,6	0,3	1,1 (1,4)
	TH07	Uskunani o‘g‘irlash	0,4	0,35	0,8 (1,1)
	TH08	Raqamli identifikatsiya ma’lumotlarini o‘g‘irlash	0,5	0,28	0,8 (1,1)
	TH09	Tashlab yuborilgan yoki takror ishlatilayotgan ma’lumot tashuvchi qurilmalardan ma’lumot olish	0,4	0.44	1 (1.4)
	TH10	Axborotni oshkor qilish	0,6	0.45	1,6 (2,2)
	TH11	Ishonchsiz manbalardan ma’lumotlarni kiritish	0,5	0,52	1,6 (2,1)
	TH12	Uskunani buzish	0,4	0,29	0,7 (0,9)
	TH13	Dasturiy ta’minotni buzish	0,4	0,33	0,8 (1)
	TH14	Veb-aloqa orqali Drive-by ekspluatatsiyasidan foydalanish	0,6	0,32	1,1 (1,5)
	TH15	Takroriy hujum, o‘rtadagi odam hujumi	0,5	0,33	1 (1,3)

Tahdid turlari	Tahdid turlari	Tahdidning nomlanishi	Tahdidning sodir bo‘lish ehtimolligi	Tashkiliy-texnik tadbirlarning bajarilganlik holati	Salbiy oqibat yuzaga kelish riski
	TH16	Shaxsiy ma’lumotlarni ruxsatsiz qayta ishlash	0,6	0,31	1,1 (1,5)
	TH17	Obyektlarga ruxsatsiz kirish	0,4	0,23	0,6 (0,7)
	TH18	Qurilmalardan ruxsatsiz foydalanish	0,4	0,26	0,6 (0,8)
	TH19	Qurilmalardan noto‘g‘ri foydalanish	0,6	0,2	0,7 (1)
	TH20	Qurilmalar yoki ma’lumot tashuvchilarni shikastlash	0,4	0,44	1 (1,4)
	TH21	Soxta dasturiy ta’minotni nusxalash	0,5	0,39	1,2 (1,6)
	TH22	Qalbaki yoki nusxalangan dasturiy ta’minotdan foydalanish	0,4	0,38	0,9 (1,2)
	TH23	Ma’lumotlarga shikast yetkazish	0,5	0,32	1 (1,3)
	TH24	Noqonuniy ma’lumotlarni qayta ishlash	0,4	0,45	1,1 (1,4)
	TH25	Zararli dasturlarni yuborish yoki tarqatish	0,6	0,325	1,1 (1,5)
	TH26	Joylashuvni aniqlash	0,2	0,25	0,3 (0,4)
Xizmatlar yoki funksiyalarni buzish	TC01	Foydalanishda xatoliklar	0,5	0,41	1,2 (1,6)
	TC02	Huquqlar yoki ruxsatlarni suiiste’mol qilish	0,6	0,25	0,9 (1,2)
	TC03	Huquqlar yoki ruxsatlarni soxtalashtirish	0,5	0,27	0,8 (1,1)
	TC04	Harakatlarni rad etish	0,7	0,39	1,6 (2,1)
Tashkiliy tahdidlar	TO01	Xodimlarning etishmasligi	0,5	0,37	1,1 (1,5)
	TO02	Resurslarning etishmasligi	0,6	0,33	1,3 (1,6)
	TO03	Xizmat ko‘rsatuvchining to‘lovga layoqatsizligi	0,4	0,37	0,9 (1,2)
	TO04	Qonunchilik yoki normativ-huquqiy hujjatlarning buzilishi	0,6	0,4	1,4 (1,9)
Saqlash tizimlari va infratuzilmasiga tahdidlar	TD01	Ruxsat etilmagan foydalanish	0,6	0,4	1,6 (1,9)
	TD02	Ruxsatsiz kirish	0,4	0,2	0,5 (0,6)
	TD03	Qonunlar va me’yoriy hujjatlarga rioya qilmaslik uchun yuridik javobgarlik	0,6	0,38	1,6 (1,9)
	TD04	Saqlash tizimlariga DoS va DDoS hujumlar	0.7	0,3	1,5 (1,7)
	TD05	Ma’lumotlarga zarar etkazish, o‘zgartirish va yo‘q qilish	0,6	0,38	1,6 (1,9)
	TD06	Ma’lumotlar sizib chiqishi	0,6	0,45	1,9 (1,9)
	TD07	Axborot tashuvchi yoki saqlovchi vositani o‘g‘irlash yoki tasodifiy yo‘qotish	0,4	0,61	1,6 (1,9)
	TD08	Zararli dastur hujumi yoki inyeksiyasi	0,6	0,38	1,6 (1,9)
	TD09	Noto‘g‘ri ishlov berish yoki foydalanish tugagandan keyin utilizatsiya qilish	0,4	0,4	1,1 (1,2)
student.buxdu.uz 7 (axborotning qiymati – 7)					
Jismoniy tahdidlar	TP02	Suv toshishi	0,2	0,14	0,1 (0,1)
	TP03	Ifloslanish, zararli radiatsiya	0,3	0,12	0,1 (0,2)
	TP04	Katta baxtsiz hodisa	0,3	0,14	0,1 (0,2)
	TP05	Portlash, halokat	0,2	0,13	0,1 (0,1)
	TP06	Chang, korroziya, muzlash	0,1	0,14	0 (0,1)

Tahdid turlari	Tahdid turlari	Tahdidning nomlanishi	Tahdidning sodir bo‘lish ehtimolligi	Tashkiliy-texnik tadbirlarning bajarilganlik holati	Salbiy oqibat yuzaga kelish riski
Tabiiy tahdidlar	TN01	Iqlim hodisasi	0,4	0,12	0,1 (0,2)
	TN02	Seysmik hodisa	0,4	0,15	0,2 (0,3)
	TN03	Vulqon hodisasi	0	0,13	0 (0)
	TN04	Meteorologik hodisa	0,3	0,13	0,1 (0,2)
	TN05	Suv toshqini	0,4	0,1	0,1 (0,2)
	TN06	Pandemiya/epidemiya hodisasi	0,4	0,15	0,2 (0,3)
Infratuzilmaning ishlamay qolishi	TI01	Ta’minot tizimining ishdan chiqishi	0,6	0,3	0,5 (1,1)
	TI02	Sovutish yoki shamollatish tizimining ishlamay qolishi	0,7	0,32	0,6 (1,1)
	TI03	Energiya ta’minotining buzilishi	0,7	0,35	0,7 (1,2)
	TI04	Telekommunikatsiya tarmog‘ining ishdan chiqishi	0,8	0,37	0,8 (1,5)
	TI05	Telekommunikatsiya uskunalari ishlamay qolishi	0,8	0,4	1 (1,6)
	TI06	Elektromagnit nurlanish	0,4	0,1	0,1 (0,2)
	TI07	Termal nurlanish	0,4	0,1	0,1 (0,2)
	TI08	Elektromagnit impulslar	0,4	0,1	0,1 (0,2)
Texnik muvaffaqiyatsizliklar	TT01	Qurilma yoki tizimning ishdan chiqishi	0,7	0.43	0,9 (1,5)
	TT02	Axborot tizimining to‘yinganligi	0,5	0,34	0,5 (0,8)
	TT03	Axborot tizimini ta’mirlash qobiliyatini buzilishi	0,4	0,36	0,4 (0,7)
Xodimlar harakati	TH01	Terrorizm, hujumlar, sabotaj	0,2	0,49	0,3 (0,5)
	TH02	Ijtimoiy muhandislik	0,2	0,45	0,3 (0,4)
	TH03	Qurilmaning nurlanishini ushlab turish	0,4	0,65	0,8 (1,3)
	TH04	Masofaviy monitoring	0,2	0,42	0,2 (0,4)
	TH05	Tinglash	0,6	0,26	0,5 (0,8)
	TH06	Ma’lumotlarni tashuvchi vositalarni yoki hujjatlarni o‘g‘irlash	0,6	0,3	0,5 (0,9)
	TH07	Uskunani o‘g‘irlash	0,4	0,35	0,8 (1,1)
	TH08	Raqamli identifikatorni yoki identifikatsiya ma’lumotlarini o‘g‘irlash	0,5	0,3	0,4 (0,7)
	TH09	Tashlab yuborilgan yoki takror ishlatilayotgan ma’lumot tashuvchi qurilmalardan ma’lumot olish	0,4	0,4	0,5 (1)
	TH10	Axborotni oshkor qilish	0,6	0,5	0,9 (1,5)
	TH11	Ishonchsiz manbalardan ma’lumotlarni kiritish	0,5	0,5	0,7 (1,2
	TH12	Uskunani buzish	0,4	0,32	0,4 (0,6)
	TH13	Dasturiy ta’minotni buzish	0,4	0,38	0,4 (0,8)
	TH14	Veb-aloqa orqali Drive-by ekspluatatsiyasidan foydalanish	0,6	0,4	0,7 (1,2)
	TH15	Takroriy hujum, o‘rtadagi odam hujumi	0,5	0,33	0,5 (0,8)
	TH16	Shaxsiy ma’lumotlarni ruxsatsiz qayta ishlash	0,6	0,43	0,8 (1,3)
	TH17	Obyektlarga ruxsatsiz kirish	0,4	0,2	0,2 (0,4)
	TH18	Qurilmalardan ruxsatsiz foydalanish	0,4	0,27	0,3 (0,5)

Tahdid turlari	Tahdid turlari	Tahdidning nomlanishi	Tahdidning sodir bo‘lish ehtimolligi	Tashkiliy-texnik tadbirlarning bajarilganlik holati	Salbiy oqibat yuzaga kelish riski
	TH19	Qurilmalardan noto‘g‘ri foydalanish	0,6	0,44	0,8 (1,3)
	TH20	Qurilmalar yoki ma’lumot tashuvchilarni shikastlash	0,4	0,54	0,6 (1,1)
	TH21	Soxta dasturiy ta’minotni nusxalash	0,5	0,32	0,5 (0,8)
	TH22	Qalbaki yoki nusxalangan dasturiy ta’minotdan foydalanish	0,4	0,5	0,6 (1)
	TH23	Ma’lumotlarga shikast yetkazish	0,5	0,32	1 (1,3)
	TH24	Noqonuniy ma’lumotlarni qayta ishlash	0,4	0,49	0.6 (1)
	TH25	Zararli dasturlarni yuborish yoki tarqatish	0,6	0,39	0.7 (1,2)
	TH26	Joylashuvni aniqlash	0,2	0,25	0,1 (0,2)
Xizmatlar yoki funksiyalarni buzish	TC01	Foydalanishda xatoliklar	0,5	0,41	1,2 (1,6)
	TC02	Huquqlar yoki ruxsatlarni suiiste’mol qilish	0,6	0,34	0,6 (1)
	TC03	Huquqlar yoki ruxsatlarni soxtalashtirish	0,5	0,38	0,6 (0.9)
	TC04	Harakatlarni rad etish	0,7	0,33	0,7 (1,1)
Tashkiliy tahdidlar	TO01	Xodimlarning etishmasligi	0,5	0,3	0,4 (0,7)
	TO02	Resurslarning etishmasligi	0,6	0,33	0,6 (1)
	TO03	Xizmat ko‘rsatuvchining to‘lovga layoqatsizligi	0,4	0,37	0,4 (0,7)
	TO04	Qonunchilik yoki normativ-huquqiy hujjatlarning buzilishi	0,6	0,4	0,7 (1,2)
Saqlash tizimlari va infratuzilmasiga tahdidlar	TD01	Ruxsat etilmagan foydalanish	0,6	0,4	1,6 (1,9)
	TD02	Ruxsatsiz kirish	0,4	0,2	0,5 (0,6)
	TD03	Qonunlar va me’yoriy hujjatlarga rioya qilmaslik uchun yuridik javobgarlik	0,6	0,38	1,6 (1,9)
	TD04	Saqlash tizimlariga DoS va DDoS hujumlar	0.7	0,3	1,5 (1,7)
	TD05	Ma’lumotlarga zarar etkazish, o‘zgartirish va yo‘q qilish	0,6	0,38	1,6 (1,9)
	TD06	Ma’lumotlar sizib chiqishi	0,6	0,45	1,9 (1,9)
	TD07	Axborot tashuvchi yoki saqlovchi vositani o‘g‘irlash yoki tasodifiy yo‘qotish	0,4	0,61	1,6 (1,9)
	TD08	Zararli dastur hujumi yoki inyeksiyasi	0,6	0,38	1,6 (1,9)
	TD09	Noto‘g‘ri ishlov berish yoki foydalanish tugagandan keyin utilizatsiya qilish	0,4	0,4	1,1 (1,2)
buxdu.uz 3 (axborotning qiymati – 5)					
Jismoniy tahdidlar	TP02	Suv toshishi	0,2	0,14	0,1 (0,1)
	TP03	Ifloslanish, zararli radiatsiya	0,3	0,12	0,1 (0,2)
	TP04	Katta baxtsiz hodisa	0,3	0,14	0,1 (0,2)
	TP05	Portlash, halokat	0,2	0,13	0,1 (0,1)
	TP06	Chang, korroziya, muzlash	0,1	0,14	0 (0,1)
Tabiiy tahdidlar	TN01	Iqlim hodisasi	0,4	0,12	0,1 (0,2)
	TN02	Seysmik hodisa	0,4	0,15	0,2 (0,3)

Tahdid turlari	Tahdid turlari	Tahdidning nomlanishi	Tahdidning sodir bo‘lish ehtimolligi	Tashkiliy-texnik tadbirlarning bajarilganlik holati	Salbiy oqibat yuzaga kelish riski
	TN03	Vulqon hodisasi	0	0,13	0 (0)
	TN04	Meteorologik hodisa	0,3	0,13	0,1 (0,2)
	TN05	Suv toshqini	0,4	0,1	0,1 (0,2)
	TN06	Pandemiya/epidemiya hodisasi	0,4	0,15	0,2 (0,3)
Infratuzilmaning ishlamay qolishi	TI01	Ta’minot tizimining ishdan chiqishi	0,6	0,3	0,5 (1,1)
	TI02	Sovutish yoki shamollatish tizimining ishlamay qolishi	0,7	0,32	0,6 (1,1)
	TI03	Energiya ta’minotining buzilishi	0,7	0,35	0,7 (1,2)
	TI04	Telekommunikatsiya tarmog‘ining ishdan chiqishi	0,8	0,37	0,8 (1,5)
	TI05	Telekommunikatsiya uskunalari ishlamay qolishi	0,8	0,4	1 (1,6)
	TI06	Elektromagnit nurlanish	0,4	0,1	0,1 (0,2)
	TI07	Termal nurlanish	0,4	0,1	0,1 (0,2)
	TI08	Elektromagnit impulslar	0,4	0,1	0,1 (0,2)
Texnik muvaffaqiyatsizliklar	TT01	Qurilma yoki tizimning ishdan chiqishi	0,7	0.43	0,9 (1,5)
	TT02	Axborot tizimining to‘yinganligi	0,5	0,34	0,5 (0,8)
	TT03	Axborot tizimini ta’mirlash qobiliyatini buzilishi	0,4	0,36	0,4 (0,7)
Xodimlar harakati	TH01	Terrorizm, hujumlar, sabotaj	0,2	0,49	0,3 (0,5)
	TH02	Ijtimoiy muhandislik	0,2	0,45	0,3 (0,4)
	TH03	Qurilmaning nurlanishini ushlab turish	0,4	0,65	0,8 (1,3)
	TH04	Masofaviy monitoring	0,2	0,42	0,2 (0,4)
	TH05	Tinglash	0,6	0,26	0,5 (0,8)
	TH06	Ma’lumotlarni tashuvchi vositalarni yoki hujjatlarni o‘g‘irlash	0,6	0,3	0,5 (0,9)
	TH07	Uskunani o‘g‘irlash	0,4	0,35	0,8 (1,1)
	TH08	Raqamli identifikatorni yoki identifikatsiya ma’lumotlarini o‘g‘irlash	0,5	0,3	0,4 (0,7)
	TH09	Tashlab yuborilgan yoki takror ishlatilayotgan ma’lumot tashuvchi qurilmalardan ma’lumot olish	0,4	0,4	0,5 (1)
	TH10	Axborotni oshkor qilish	0,6	0,5	0,9 (1,5)
	TH11	Ishonchsiz manbalardan ma’lumotlarni kiritish	0,5	0,5	0,7 (1,2
	TH12	Uskunani buzish	0,4	0,32	0,4 (0,6)
	TH13	Dasturiy ta’minotni buzish	0,4	0,38	0,4 (0,8)
	TH14	Veb-aloqa orqali Drive-by ekspluatatsiyasidan foydalanish	0,6	0,4	0,7 (1,2)
	TH15	Takroriy hujum, o‘rtadagi odam hujumi	0,5	0,33	0,5 (0,8)
	TH16	Shaxsiy ma’lumotlarni ruxsatsiz qayta ishlash	0,6	0,43	0,8 (1,3)
	TH17	Obyektlarga ruxsatsiz kirish	0,4	0,2	0,2 (0,4)
	TH18	Qurilmalardan ruxsatsiz foydalanish	0,4	0,27	0,3 (0,5)
	TH19	Qurilmalardan noto‘g‘ri foydalanish	0,6	0,44	0,8 (1,3)
	TH20	Qurilmalar yoki ma’lumot tashuvchilarni shikastlash	0,4	0,54	0,6 (1,1)

Tahdid turlari	Tahdid turlari	Tahdidning nomlanishi	Tahdidning sodir bo‘lish ehtimolligi	Tashkiliy-texnik tadbirlarning bajarilganlik holati	Salbiy oqibat yuzaga kelish riski
	TH21	Soxta dasturiy ta’minotni nusxalash	0,5	0,32	0,5 (0,8)
	TH22	Qalbaki yoki nusxalangan dasturiy ta’minotdan foydalanish	0,4	0,5	0,6 (1)
	TH23	Ma’lumotlarga shikast yetkazish	0,5	0,32	1 (1,3)
	TH24	Noqonuniy ma’lumotlarni qayta ishlash	0,4	0,49	0.6 (1)
	TH25	Zararli dasturlarni yuborish yoki tarqatish	0,6	0,39	0.7 (1,2)
	TH26	Joylashuvni aniqlash	0,2	0,25	0,1 (0,2)
Xizmatlar yoki funksiyalarni buzish	TC01	Foydalanishda xatoliklar	0,5	0,41	1,2 (1,6)
	TC02	Huquqlar yoki ruxsatlarni suiiste’mol qilish	0,6	0,34	0,6 (1)
	TC03	Huquqlar yoki ruxsatlarni soxtalashtirish	0,5	0,38	0,6 (0.9)
	TC04	Harakatlarni rad etish	0,7	0,33	0,7 (1,1)
Tashkiliy tahdidlar	TO01	Xodimlarning etishmasligi	0,5	0,3	0,4 (0,7)
	TO02	Resurslarning etishmasligi	0,6	0,33	0,6 (1)
	TO03	Xizmat ko‘rsatuvchining to‘lovga layoqatsizligi	0,4	0,37	0,4 (0,7)
	TO04	Qonunchilik yoki normativ-huquqiy hujjatlarning buzilishi	0,6	0,4	0,7 (1,2)
Saqlash tizimlari va infratuzilmasiga tahdidlar	TD01	Ruxsat etilmagan foydalanish	0,6	0,4	1,6 (1,9)
	TD02	Ruxsatsiz kirish	0,4	0,2	0,5 (0,6)
	TD03	Qonunlar va me’yoriy hujjatlarga rioya qilmaslik uchun yuridik javobgarlik	0,6	0,38	1,6 (1,9)
	TD04	Saqlash tizimlariga DoS va DDoS hujumlar	0.7	0,3	1,5 (1,7)
	TD05	Ma’lumotlarga zarar etkazish, o‘zgartirish va yo‘q qilish	0,6	0,38	1,6 (1,9)
	TD06	Ma’lumotlar sizib chiqishi	0,6	0,45	1,9 (1,9)
	TD07	Axborot tashuvchi yoki saqlovchi vositani o‘g‘irlash yoki tasodifiy yo‘qotish	0,4	0,61	1,6 (1,9)
	TD08	Zararli dastur hujumi yoki inyeksiyasi	0,6	0,38	1,6 (1,9)
	TD09	Noto‘g‘ri ishlov berish yoki foydalanish tugagandan keyin utilizatsiya qilish	0,4	0,4	1,1 (1,2)
Korporativ elektron pochta 3 (axborotning qiymati – 5)					
Jismoniy tahdidlar	TP02	Suv toshishi	0,2	0,14	0,1 (0,1)
	TP03	Ifloslanish, zararli radiatsiya	0,3	0,12	0,1 (0,2)
	TP04	Katta baxtsiz hodisa	0,3	0,14	0,1 (0,2)
	TP05	Portlash, halokat	0,2	0,13	0,1 (0,1)
	TP06	Chang, korroziya, muzlash	0,1	0,14	0 (0,1)
Tabiiy tahdidlar	TN01	Iqlim hodisasi	0,4	0,12	0,1 (0,2)
	TN02	Seysmik hodisa	0,4	0,15	0,2 (0,3)
	TN03	Vulqon hodisasi	0	0,13	0 (0)
	TN04	Meteorologik hodisa	0,3	0,13	0,1 (0,2)
	TN05	Suv toshqini	0,4	0,1	0,1 (0,2)

Tahdid turlari	Tahdid turlari	Tahdidning nomlanishi	Tahdidning sodir bo‘lish ehtimolligi	Tashkiliy-texnik tadbirlarning bajarilganlik holati	Salbiy oqibat yuzaga kelish riski
	TN06	Pandemiya/epidemiya hodisasi	0,4	0,15	0,2 (0,3)
Infratuzilmaning ishlamay qolishi	TI01	Ta’minot tizimining ishdan chiqishi	0,6	0,3	0,5 (1,1)
	TI02	Sovutish yoki shamollatish tizimining ishlamay qolishi	0,7	0,32	0,6 (1,1)
	TI03	Energiya ta’minotining buzilishi	0,7	0,35	0,7 (1,2)
	TI04	Telekommunikatsiya tarmog‘ining ishdan chiqishi	0,8	0,37	0,8 (1,5)
	TI05	Telekommunikatsiya uskunalari ishlamay qolishi	0,8	0,4	1 (1,6)
	TI06	Elektromagnit nurlanish	0,4	0,1	0,1 (0,2)
	TI07	Termal nurlanish	0,4	0,1	0,1 (0,2)
	TI08	Elektromagnit impulslar	0,4	0,1	0,1 (0,2)
Texnik muvaffaqiyatsizliklar	TT01	Qurilma yoki tizimning ishdan chiqishi	0,7	0.43	0,9 (1,5)
	TT02	Axborot tizimining to‘yinganligi	0,5	0,34	0,5 (0,8)
	TT03	Axborot tizimini ta’mirlash qobiliyatini buzilishi	0,4	0,36	0,4 (0,7)
Xodimlar harakati	TH01	Terrorizm, hujumlar, sabotaj	0,2	0,49	0,3 (0,5)
	TH02	Ijtimoiy muhandislik	0,2	0,45	0,3 (0,4)
	TH03	Qurilmaning nurlanishini ushlab turish	0,4	0,65	0,8 (1,3)
	TH04	Masofaviy monitoring	0,2	0,42	0,2 (0,4)
	TH05	Tinglash	0,6	0,26	0,5 (0,8)
	TH06	Ma’lumotlarni tashuvchi vositalarni yoki hujjatlarni o‘g‘irlash	0,6	0,3	0,5 (0,9)
	TH07	Uskunani o‘g‘irlash	0,4	0,35	0,8 (1,1)
	TH08	Raqamli identifikatorni yoki identifikatsiya ma’lumotlarini o‘g‘irlash	0,5	0,3	0,4 (0,7)
	TH09	Tashlab yuborilgan yoki takror ishlatilayotgan ma’lumot tashuvchi qurilmalardan ma’lumot olish	0,4	0,4	0,5 (1)
	TH10	Axborotni oshkor qilish	0,6	0,5	0,9 (1,5)
	TH11	Ishonchsiz manbalardan ma’lumotlarni kiritish	0,5	0,5	0,7 (1,2
	TH12	Uskunani buzish	0,4	0,32	0,4 (0,6)
	TH13	Dasturiy ta’minotni buzish	0,4	0,38	0,4 (0,8)
	TH14	Veb-aloqa orqali Drive-by ekspluatatsiyasidan foydalanish	0,6	0,4	0,7 (1,2)
	TH15	Takroriy hujum, o‘rtadagi odam hujumi	0,5	0,33	0,5 (0,8)
	TH16	Shaxsiy ma’lumotlarni ruxsatsiz qayta ishlash	0,6	0,43	0,8 (1,3)
	TH17	Obyektlarga ruxsatsiz kirish	0,4	0,2	0,2 (0,4)
	TH18	Qurilmalardan ruxsatsiz foydalanish	0,4	0,27	0,3 (0,5)
	TH19	Qurilmalardan noto‘g‘ri foydalanish	0,6	0,44	0,8 (1,3)
	TH20	Qurilmalar yoki ma’lumot tashuvchilarni shikastlash	0,4	0,54	0,6 (1,1)
	TH21	Soxta dasturiy ta’minotni nusxalash	0,5	0,32	0,5 (0,8)

Tahdid turlari	Tahdid turlari	Tahdidning nomlanishi	Tahdidning sodir bo‘lish ehtimolligi	Tashkiliy-texnik tadbirlarning bajarilganlik holati	Salbiy oqibat yuzaga kelish riski
	TH22	Qalbaki yoki nusxalangan dasturiy ta’minotdan foydalanish	0,4	0,5	0,6 (1)
	TH23	Ma’lumotlarga shikast yetkazish	0,5	0,32	1 (1,3)
	TH24	Noqonuniy ma’lumotlarni qayta ishlash	0,4	0,49	0.6 (1)
	TH25	Zararli dasturlarni yuborish yoki tarqatish	0,6	0,39	0.7 (1,2)
	TH26	Joylashuvni aniqlash	0,2	0,25	0,1 (0,2)
Xizmatlar yoki funksiyalarni buzish	TC01	Foydalanishda xatoliklar	0,5	0,41	1,2 (1,6)
	TC02	Huquqlar yoki ruxsatlarni suiiste’mol qilish	0,6	0,34	0,6 (1)
	TC03	Huquqlar yoki ruxsatlarni soxtalashtirish	0,5	0,38	0,6 (0.9)
	TC04	Harakatlarni rad etish	0,7	0,33	0,7 (1,1)
Tashkiliy tahdidlar	TO01	Xodimlarning etishmasligi	0,5	0,3	0,4 (0,7)
	TO02	Resurslarning etishmasligi	0,6	0,33	0,6 (1)
	TO03	Xizmat ko‘rsatuvchining to‘lovga layoqatsizligi	0,4	0,37	0,4 (0,7)
	TO04	Qonunchilik yoki normativ-huquqiy hujjatlarning buzilishi	0,6	0,4	0,7 (1,2)
Saqlash tizimlari va infratuzilmasiga tahdidlar	TD01	Ruxsat etilmagan foydalanish	0,6	0,4	1,6 (1,9)
	TD02	Ruxsatsiz kirish	0,4	0,2	0,5 (0,6)
	TD03	Qonunlar va me’yoriy hujjatlarga rioya qilmaslik uchun yuridik javobgarlik	0,6	0,38	1,6 (1,9)
	TD04	Saqlash tizimlariga DoS va DDoS hujumlar	0.7	0,3	1,5 (1,7)
	TD05	Ma’lumotlarga zarar etkazish, o‘zgartirish va yo‘q qilish	0,6	0,38	1,6 (1,9)
	TD06	Ma’lumotlar sizib chiqishi	0,6	0,45	1,9 (1,9)
	TD07	Axborot tashuvchi yoki saqlovchi vositani o‘g‘irlash yoki tasodifiy yo‘qotish	0,4	0,61	1,6 (1,9)
	TD08	Zararli dastur hujumi yoki inyeksiyasi	0,6	0,38	1,6 (1,9)
	TD09	Noto‘g‘ri ishlov berish yoki foydalanish tugagandan keyin utilizatsiya qilish	0,4	0,4	1,1 (1,2)
journal.buxdu.uz 3 (axborotning qiymati – 5)					
Jismoniy tahdidlar	TP02	Suv toshishi	0,2	0,14	0,1 (0,1)
	TP03	Ifloslanish, zararli radiatsiya	0,3	0,12	0,1 (0,2)
	TP04	Katta baxtsiz hodisa	0,3	0,14	0,1 (0,2)
	TP05	Portlash, halokat	0,2	0,13	0,1 (0,1)
	TP06	Chang, korroziya, muzlash	0,1	0,14	0 (0,1)
Tabiiy tahdidlar	TN01	Iqlim hodisasi	0,4	0,12	0,1 (0,2)
	TN02	Seysmik hodisa	0,4	0,15	0,2 (0,3)
	TN03	Vulqon hodisasi	0	0,13	0 (0)

Tahdid turlari	Tahdid turlari	Tahdidning nomlanishi	Tahdidning sodir bo‘lish ehtimolligi	Tashkiliy-texnik tadbirlarning bajarilganlik holati	Salbiy oqibat yuzaga kelish riski
	TN04	Meteorologik hodisa	0,3	0,13	0,1 (0,2)
	TN05	Suv toshqini	0,4	0,1	0,1 (0,2)
	TN06	Pandemiya/epidemiya hodisasi	0,4	0,15	0,2 (0,3)
Infratuzilmaning ishlamay qolishi	TI01	Ta’minot tizimining ishdan chiqishi	0,6	0,3	0,5 (1,1)
	TI02	Sovutish yoki shamollatish tizimining ishlamay qolishi	0,7	0,32	0,6 (1,1)
	TI03	Energiya ta’minotining buzilishi	0,7	0,35	0,7 (1,2)
	TI04	Telekommunikatsiya tarmog‘ining ishdan chiqishi	0,8	0,37	0,8 (1,5)
	TI05	Telekommunikatsiya uskunalari ishlamay qolishi	0,8	0,4	1 (1,6)
	TI06	Elektromagnit nurlanish	0,4	0,1	0,1 (0,2)
	TI07	Termal nurlanish	0,4	0,1	0,1 (0,2)
	TI08	Elektromagnit impulslar	0,4	0,1	0,1 (0,2)
Texnik muvaffaqiyatsizliklar	TT01	Qurilma yoki tizimning ishdan chiqishi	0,7	0.43	0,9 (1,5)
	TT02	Axborot tizimining to‘yinganligi	0,5	0,34	0,5 (0,8)
	TT03	Axborot tizimini ta’mirlash qobiliyatini buzilishi	0,4	0,36	0,4 (0,7)
Xodimlar harakati	TH01	Terrorizm, hujumlar, sabotaj	0,2	0,49	0,3 (0,5)
	TH02	Ijtimoiy muhandislik	0,2	0,45	0,3 (0,4)
	TH03	Qurilmaning nurlanishini ushlab turish	0,4	0,65	0,8 (1,3)
	TH04	Masofaviy monitoring	0,2	0,42	0,2 (0,4)
	TH05	Tinglash	0,6	0,26	0,5 (0,8)
	TH06	Ma’lumotlarni tashuvchi vositalarni yoki hujjatlarni o‘g‘irlash	0,6	0,3	0,5 (0,9)
	TH07	Uskunani o‘g‘irlash	0,4	0,35	0,8 (1,1)
	TH08	Raqamli identifikatorni yoki identifikatsiya ma’lumotlarini o‘g‘irlash	0,5	0,3	0,4 (0,7)
	TH09	Tashlab yuborilgan yoki takror ishlatilayotgan ma’lumot tashuvchi qurilmalardan ma’lumot olish	0,4	0,4	0,5 (1)
	TH10	Axborotni oshkor qilish	0,6	0,5	0,9 (1,5)
	TH11	Ishonchsiz manbalardan ma’lumotlarni kiritish	0,5	0,5	0,7 (1,2
	TH12	Uskunani buzish	0,4	0,32	0,4 (0,6)
	TH13	Dasturiy ta’minotni buzish	0,4	0,38	0,4 (0,8)
	TH14	Veb-aloqa orqali Drive-by ekspluatatsiyasidan foydalanish	0,6	0,4	0,7 (1,2)
	TH15	Takroriy hujum, o‘rtadagi odam hujumi	0,5	0,33	0,5 (0,8)
	TH16	Shaxsiy ma’lumotlarni ruxsatsiz qayta ishlash	0,6	0,43	0,8 (1,3)
	TH17	Obyektlarga ruxsatsiz kirish	0,4	0,2	0,2 (0,4)
	TH18	Qurilmalardan ruxsatsiz foydalanish	0,4	0,27	0,3 (0,5)
	TH19	Qurilmalardan noto‘g‘ri foydalanish	0,6	0,44	0,8 (1,3)

Tahdid turlari	Tahdid turlari	Tahdidning nomlanishi	Tahdidning sodir bo‘lish ehtimolligi	Tashkiliy-texnik tadbirlarning bajarilganlik holati	Salbiy oqibat yuzaga kelish riski
	TH20	Qurilmalar yoki ma’lumot tashuvchilarni shikastlash	0,4	0,54	0,6 (1,1)
	TH21	Soxta dasturiy ta’minotni nusxalash	0,5	0,32	0,5 (0,8)
	TH22	Qalbaki yoki nusxalangan dasturiy ta’minotdan foydalanish	0,4	0,5	0,6 (1)
	TH23	Ma’lumotlarga shikast yetkazish	0,5	0,32	1 (1,3)
	TH24	Noqonuniy ma’lumotlarni qayta ishlash	0,4	0,49	0.6 (1)
	TH25	Zararli dasturlarni yuborish yoki tarqatish	0,6	0,39	0.7 (1,2)
	TH26	Joylashuvni aniqlash	0,2	0,25	0,1 (0,2)
Xizmatlar yoki funksiyalarni buzish	TC01	Foydalanishda xatoliklar	0,5	0,41	1,2 (1,6)
	TC02	Huquqlar yoki ruxsatlarni suiiste’mol qilish	0,6	0,34	0,6 (1)
	TC03	Huquqlar yoki ruxsatlarni soxtalashtirish	0,5	0,38	0,6 (0.9)
	TC04	Harakatlarni rad etish	0,7	0,33	0,7 (1,1)
Tashkiliy tahdidlar	TO01	Xodimlarning etishmasligi	0,5	0,3	0,4 (0,7)
	TO02	Resurslarning etishmasligi	0,6	0,33	0,6 (1)
	TO03	Xizmat ko‘rsatuvchining to‘lovga layoqatsizligi	0,4	0,37	0,4 (0,7)
	TO04	Qonunchilik yoki normativ-huquqiy hujjatlarning buzilishi	0,6	0,4	0,7 (1,2)
Saqlash tizimlari va infratuzilmasiga tahdidlar	TD01	Ruxsat etilmagan foydalanish	0,6	0,4	1,6 (1,9)
	TD02	Ruxsatsiz kirish	0,4	0,2	0,5 (0,6)
	TD03	Qonunlar va me’yoriy hujjatlarga rioya qilmaslik uchun yuridik javobgarlik	0,6	0,38	1,6 (1,9)
	TD04	Saqlash tizimlariga DoS va DDoS hujumlar	0.7	0,3	1,5 (1,7)
	TD05	Ma’lumotlarga zarar etkazish, o‘zgartirish va yo‘q qilish	0,6	0,38	1,6 (1,9)
	TD06	Ma’lumotlar sizib chiqishi	0,6	0,45	1,9 (1,9)
	TD07	Axborot tashuvchi yoki saqlovchi vositani o‘g‘irlash yoki tasodifiy yo‘qotish	0,4	0,61	1,6 (1,9)
	TD08	Zararli dastur hujumi yoki inyeksiyasi	0,6	0,38	1,6 (1,9)
	TD09	Noto‘g‘ri ishlov berish yoki foydalanish tugagandan keyin utilizatsiya qilish	0,4	0,4	1,1 (1,2)
fayl server 7 (axborotning qiymati – 7)					
Jismoniy tahdidlar	TP01	Yong‘in	0,2	0,18	0,2 (0,2)
	TP02	Suv toshishi	0,2	0,15	0,4 (0,4)
	TP03	Ifloslanish, zararli radiatsiya	0,3	0,15	0,3 (0,3)
	TP04	Katta baxtsiz hodisa	0,3	0,28	0,5 (0,5)
	TP05	Portlash, halokat	0,2	0,13	0,2 (0,2)
	TP06	Chang, korroziya, muzlash	0,1	0,17	0,1 (0,1)

Tahdid turlari	Tahdid turlari	Tahdidning nomlanishi	Tahdidning sodir bo‘lish ehtimolligi	Tashkiliy-texnik tadbirlarning bajarilganlik holati	Salbiy oqibat yuzaga kelish riski
Tabiiy tahdidlar	TN01	Iqlim hodisasi	0,4	0,15	0,4 (0,4)
	TN02	Seysmik hodisa	0,4	0,15	0,4 (0,4)
	TN03	Vulqon hodisasi	0	0,13	0 (0)
	TN04	Meteorologik hodisa	0,3	0,13	0,3 (0,3)
	TN05	Suv toshqini	0,4	0,1	0,3 (0,3)
	TN06	Pandemiya/epidemiya hodisasi	0,4	0,15	0,4 (0,4)
Infratuzilmaning ishlamay qolishi	TI01	Ta’minot tizimining ishdan chiqishi	0,6	0,37	1,5 (1,5)
	TI02	Sovutish yoki shamollatish tizimining ishlamay qolishi	0,7	0,23	1,1 (1,1)
	TI03	Energiya ta’minotining buzilishi	0,7	0,38	1,8 (1,8)
	TI04	Telekommunikatsiya tarmog‘ining ishdan chiqishi	0,8	0,47	2,6 (2,6)
	TI05	Telekommunikatsiya uskunalari ishlamay qolishi	0,8	0,3	1,7 (1,7)
	TI06	Elektromagnit nurlanish	0,4	0,1	0,3 (0,3)
	TI07	Termal nurlanish	0,4	0,1	0,3 (0,3)
	TI08	Elektromagnit impulslar	0,4	0,1	0,3 (0,3)
Texnik muvaffaqiyatsizliklar	TT01	Qurilma yoki tizimning ishdan chiqishi	0,7	0,46	2.2 (2,2)
	TT02	Axborot tizimining to‘yinganligi	0,5	0,42	1,5 (1,5)
	TT03	Axborot tizimini ta’mirlash qobiliyatini buzilishi	0,4	0,41	1,1 (1,1)
Xodimlar harakati	TH01	Terrorizm, hujumlar, sabotaj	0,2	0,26	0,3 (0,3)
	TH02	Ijtimoiy muhandislik	0,2	0,26	0,3 (0,3)
	TH03	Qurilmaning nurlanishini ushlab turish	0,4	0,4	1,1 (1,1)
	TH04	Masofaviy monitoring	0,2	0,4	0,6 (0,6)
	TH05	Tinglash	0,6	0,26	1,1 (1,1)
	TH06	Ma’lumotlarni tashuvchi vositalarni yoki hujjatlarni o‘g‘irlash	0,6	0,31	1,3 (1,3)
	TH07	Uskunani o‘g‘irlash	0,4	0,34	0,9 (0,9)
	TH08	Raqamli identifikatorni yoki identifikatsiya ma’lumotlarini o‘g‘irlash	0,5	0,31	1,1 (1,1)
	TH09	Tashlab yuborilgan yoki takror ishlatilayotgan ma’lumot tashuvchi qurilmalardan ma’lumot olish	0,4	0,42	1,2 (1,2)
	TH10	Axborotni oshkor qilish	0,6	0,45	1,9 (1,9)
	TH11	Ishonchsiz manbalardan ma’lumotlarni kiritish	0,5	0,47	1,6 (1,6)
	TH12	Uskunani buzish	0,4	0,32	0,9 (0,9)
	TH13	Dasturiy ta’minotni buzish	0,4	0,36	1 (1)
	TH14	Veb-aloqa orqali Drive-by ekspluatatsiyasidan foydalanish	0,6	0,38	1,6 (1,6)
	TH15	Takroriy hujum, o‘rtadagi odam hujumi	0,5	0,33	1,2 (1,2)
	TH16	Shaxsiy ma’lumotlarni ruxsatsiz qayta ishlash	0,6	0,43	1,8 (1,8)
	TH17	Obyektlarga ruxsatsiz kirish	0,4	0,19	0,5 (0,5)
	TH18	Qurilmalardan ruxsatsiz foydalanish	0,4	0,26	0,7 (0,7)

Tahdid turlari	Tahdid turlari	Tahdidning nomlanishi	Tahdidning sodir bo‘lish ehtimolligi	Tashkiliy-texnik tadbirlarning bajarilganlik holati	Salbiy oqibat yuzaga kelish riski
	TH19	Qurilmalardan noto‘g‘ri foydalanish	0,6	0,4	1,7 (1,7)
	TH20	Qurilmalar yoki ma’lumot tashuvchilarni shikastlash	0,4	0,5	1,4 (1,4)
	TH21	Soxta dasturiy ta’minotni nusxalash	0,5	0,3	1 (1)
	TH22	Qalbaki yoki nusxalangan dasturiy ta’minotdan foydalanish	0,4	0,54	1,5 (1,5)
	TH23	Ma’lumotlarga shikast yetkazish	0,5	0,31	1,1 (1,1)
	TH24	Noqonuniy ma’lumotlarni qayta ishlash	0,4	0,44	1,2 (1,2)
	TH25	Zararli dasturlarni yuborish yoki tarqatish	0,6	0,4	1,7 (1,7)
	TH26	Joylashuvni aniqlash	0,2	0,28	0,4 (0,4)
Xizmatlar yoki funksiyalarni buzish	TC01	Foydalanishda xatoliklar	0,5	0,46	1,6 (1,6)
	TC02	Huquqlar yoki ruxsatlarni suiiste’mol qilish	0,6	0,44	1,8 (1,8)
	TC03	Huquqlar yoki ruxsatlarni soxtalashtirish	0,5	0,32	1,1 (1,1)
	TC04	Harakatlarni rad etish	0,7	0,4	2 (2)
Tashkiliy tahdidlar	TO01	Xodimlarning etishmasligi	0,5	0,3	1,2 (1,2)
	TO02	Resurslarning etishmasligi	0,6	0,33	1,4 (1,4)
	TO03	Xizmat ko‘rsatuvchining to‘lovga layoqatsizligi	0,4	0,37	1 (1)
	TO04	Qonunchilik yoki normativ-huquqiy hujjatlarning buzilishi	0,6	0,4	1,7 (1,7)
Saqlash tizimlari va infratuzilmasiga tahdidlar	TD01	Ruxsat etilmagan foydalanish	0,6	0,30	1,3 (1,4)
	TD02	Ruxsatsiz kirish	0,4	0,13	0,4 (0,4)
	TD03	Qonunlar va me’yoriy hujjatlarga rioya qilmaslik uchun yuridik javobgarlik	0,6	0,4	1,7 (1,9)
	TD04	Saqlash tizimlariga DoS va DDoS hujumlar	0.7	-	-
	TD05	Ma’lumotlarga zarar etkazish, o‘zgartirish va yo‘q qilish	0,6	0,33	1,4 (1,6)
	TD06	Ma’lumotlar sizib chiqishi	0,6	0,47	2 (2,3)
	TD07	Axborot tashuvchi yoki saqlovchi vositani o‘g‘irlash yoki tasodifiy yo‘qotish	0,4	0,42	1,2 (1,3)
	TD08	Zararli dastur hujumi yoki inyeksiyasi	0,6	0,33	1,4 (1,6)
	TD09	Noto‘g‘ri ishlov berish yoki foydalanish tugagandan keyin utilizatsiya qilish	0,4	0,44	1,2 (1,4)
IP telefoniya 7 (axborotning qiymati – 7)					
Jismoniy tahdidlar	TP01	Yong‘in	0,2	0,19	0,2 (0,3)
	TP02	Suv toshishi	0,2	0,2	0,2 (0,3)
	TP03	Ifloslanish, zararli radiatsiya	0,3	0,2	0,4 (0,5)
	TP04	Katta baxtsiz hodisa	0,3	0,22	0,4 (0,5)
	TP05	Portlash, halokat	0,2	0,13	0,1 (0,2)
	TP06	Chang, korroziya, muzlash	0,1	0,2	0,1 (0,2)
Tabiiy tahdidlar	TN01	Iqlim hodisasi	0,4	0,1	0,2 (0,3)
	TN02	Seysmik hodisa	0,4	0,18	0,5 (0,6)

Tahdid turlari	Tahdid turlari	Tahdidning nomlanishi	Tahdidning sodir bo‘lish ehtimolligi	Tashkiliy-texnik tadbirlarning bajarilganlik holati	Salbiy oqibat yuzaga kelish riski
	TN03	Vulqon hodisasi	0	0,25	0 (0)
	TN04	Meteorologik hodisa	0,3	0,2	0,4 (0,5)
	TN05	Suv toshqini	0,4	0,1	0,2 (0,3)
	TN06	Pandemiya/epidemiya hodisasi	0,4	0,2	0,5 (0,6)
Infratuzilmaning ishlamay qolishi	TI01	Ta’minot tizimining ishdan chiqishi	0,6	0,37	1,5 (1.8)
	TI02	Sovutish yoki shamollatish tizimining ishlamay qolishi	0,7	0,27	1,5 (1,7)
	TI03	Energiya ta’minotining buzilishi	0,7	0,42	1,9 (2,2)
	TI04	Telekommunikatsiya tarmog‘ining ishdan chiqishi	0,8	0,4	2,2 (2,5)
	TI05	Telekommunikatsiya uskunalari ishlamay qolishi	0,8	0,4	2,2 (2,5)
	TI06	Elektromagnit nurlanish	0,4	0,12	0,2 (0,3)
	TI07	Termal nurlanish	0,4	0,11	0,2 (0,3)
	TI08	Elektromagnit impulslar	0,4	0,1	0,2 (0,3)
Texnik muvaffaqiyatsizliklar	TT01	Qurilma yoki tizimning ishdan chiqishi	0,7	0,538	2,4 (2,8)
	TT02	Axborot tizimining to‘yinganligi	0,5	0,4	1,4 (1,6)
	TT03	Axborot tizimini ta’mirlash qobiliyatini buzilishi	0,4	0,41	1,1 (1,3)
Xodimlar harakati	TH01	Terrorizm, hujumlar, sabotaj	0,2	0,4	0,5 (0,6)
	TH02	Ijtimoiy muhandislik	0,2	0,3	0,4 (0,6)
	TH03	Qurilmaning nurlanishini ushlab turish	0,4	0,51	1,4 (1,6)
	TH04	Masofaviy monitoring	0,2	0,4	0,5 (0,6)
	TH05	Tinglash	0,6	0,3	1,2 (1,4)
	TH06	Ma’lumotlarni tashuvchi vositalarni yoki hujjatlarni o‘g‘irlash	0,6	0,38	1,6 (1,9)
	TH07	Uskunani o‘g‘irlash	0,4	0,38	1,1 (1,2)
	TH08	Raqamli identifikatorni yoki identifikatsiya ma’lumotlarini o‘g‘irlash	0,5	0,38	1,4 (1,6)
	TH09	Tashlab yuborilgan yoki takror ishlatilayotgan ma’lumot tashuvchi qurilmalardan ma’lumot olish	0,4	0,4	1,1 (1,2)
	TH10	Axborotni oshkor qilish	0,6	0,6	2,5 (2,8)
	TH11	Ishonchsiz manbalardan ma’lumotlarni kiritish	0,5	0,52	1,7 (2)
	TH12	Uskunani buzish	0,4	0,33	0,8 (0,9)
	TH13	Dasturiy ta’minotni buzish	0,4	0,42	1,1 (1,2)
	TH14	Veb-aloqa orqali Drive-by ekspluatatsiyasidan foydalanish	0,6	0,38	1,6 (1,9)
	TH15	Takroriy hujum, o‘rtadagi odam hujumi	0,5	0,38	1,4 (1,6)
	TH16	Shaxsiy ma’lumotlarni ruxsatsiz qayta ishlash	0,6	0,4	1,6 (1,9)
	TH17	Obyektlarga ruxsatsiz kirish	0,4	0,2	0,5 (0,6)
	TH18	Qurilmalardan ruxsatsiz foydalanish	0,4	0,3	0,8 (0,9)
	TH19	Qurilmalardan noto‘g‘ri foydalanish	0,6	0,21	0,8 (0,9)
	TH20	Qurilmalar yoki ma’lumot tashuvchilarni shikastlash	0,4	0,61	1,6 (1,9)

Tahdid turlari	Tahdid turlari	Tahdidning nomlanishi	Tahdidning sodir bo‘lish ehtimolligi	Tashkiliy-texnik tadbirlarning bajarilganlik holati	Salbiy oqibat yuzaga kelish riski
	TH21	Soxta dasturiy ta’minotni nusxalash	0,5	0,39	1,6 (1,9)
	TH22	Qalbaki yoki nusxalangan dasturiy ta’minotdan foydalanish	0,4	0,5	1,4 (1,6)
	TH23	Ma’lumotlarga shikast yetkazish	0,5	0,42	1,4 (1,6)
	TH24	Noqonuniy ma’lumotlarni qayta ishlash	0,4	0,41	1,1 (1,3)
	TH25	Zararli dasturlarni yuborish yoki tarqatish	0,6	0,38	1,6 (1,9)
	TH26	Joylashuvni aniqlash	0,2	0,31	0,4 (0,5)
Xizmatlar yoki funksiyalarni buzish	TC01	Foydalanishda xatoliklar	0,5	0,4	1,6 (1,9)
	TC02	Huquqlar yoki ruxsatlarni suiiste’mol qilish	0,6	0,3	1,2 (1,4)
	TC03	Huquqlar yoki ruxsatlarni soxtalashtirish	0,5	0.41	1,6 (1,9)
	TC04	Harakatlarni rad etish	0,7	0,41	2 (2,3)
Tashkiliy tahdidlar	TO01	Xodimlarning etishmasligi	0,5	0,4	1,6 (1,9)
	TO02	Resurslarning etishmasligi	0,6	0,31	1,2 (1,4)
	TO03	Xizmat ko‘rsatuvchining to‘lovga layoqatsizligi	0,4	0,28	0,8 (0,9)
	TO04	Qonunchilik yoki normativ-huquqiy hujjatlarning buzilishi	0,6	0,38	1,6 (1,9)
Saqlash tizimlari va infratuzilmasiga tahdidlar	TD01	Ruxsat etilmagan foydalanish	0,6	0,30	1,3 (1,6)
	TD02	Ruxsatsiz kirish	0,4	0,13	0,4 (0,5)
	TD03	Qonunlar va me’yoriy hujjatlarga rioya qilmaslik uchun yuridik javobgarlik	0,6	0,4	1,7 (2,2)
	TD04	Saqlash tizimlariga DoS va DDoS hujumlar	0.7	-	-
	TD05	Ma’lumotlarga zarar etkazish, o‘zgartirish va yo‘q qilish	0,6	0,33	1,4 (1,8)
	TD06	Ma’lumotlar sizib chiqishi	0,6	0,47	2 (2,5)
	TD07	Axborot tashuvchi yoki saqlovchi vositani o‘g‘irlash yoki tasodifiy yo‘qotish	0,4	0,42	1,2 (1,5)
	TD08	Zararli dastur hujumi yoki inyeksiyasi	0,6	0,33	1,4 (1,8)
	TD09	Noto‘g‘ri ishlov berish yoki foydalanish tugagandan keyin utilizatsiya qilish	0,4	0,44	1,2 (1,6)
Ishchi stansiyalar 3 (axborotning qiymati – 5)					
Jismoniy tahdidlar	TP01	Yong‘in	0,2	0,26	0,1 (0,3)
	TP02	Suv toshishi	0,2	0,3	0,1 (0,3)
	TP03	Ifloslanish, zararli radiatsiya	0,3	0,31	0,3 (0,4)
	TP04	Katta baxtsiz hodisa	0,3	0,33	0,3 (0,4)
	TP05	Portlash, halokat	0,2	0,19	0,1 (0,2)
	TP06	Chang, korroziya, muzlash	0,1	0,37	0,1 (0,2)
Tabiiy tahdidlar	TN01	Iqlim hodisasi	0,4	0,19	0,2 (0,4)
	TN02	Seysmik hodisa	0,4	0,3	0,3 (0,6)
	TN03	Vulqon hodisasi	0	0,2	0 (0)
	TN04	Meteorologik hodisa	0,3	0,22	0,1 (0,3)

Tahdid turlari	Tahdid turlari	Tahdidning nomlanishi	Tahdidning sodir bo‘lish ehtimolligi	Tashkiliy-texnik tadbirlarning bajarilganlik holati	Salbiy oqibat yuzaga kelish riski
	TN05	Suv toshqini	0,4	0,18	0,2 (0,4)
	TN06	Pandemiya/epidemiya hodisasi	0,4	0,31	0,3 (0,6)
Infratuzilmaning ishlamay qolishi	TI01	Ta’minot tizimining ishdan chiqishi	0,6	0,5	0,9 (1,5)
	TI02	Sovutish yoki shamollatish tizimining ishlamay qolishi	0,7	0,48	1,1 (1,7)
	TI03	Energiya ta’minotining buzilishi	0,7	0,4	0,8 (1,4)
	TI04	Telekommunikatsiya tarmog‘ining ishdan chiqishi	0,8	0,42	0,9 (1,6)
	TI05	Telekommunikatsiya uskunalari ishlamay qolishi	0,8	0,41	0,9 (1,6)
	TI06	Elektromagnit nurlanish	0,4	0,3	0,4 (0,6)
	TI07	Termal nurlanish	0,4	0,5	0,6 (1)
	TI08	Elektromagnit impulslar	0,4	0,33	0,3 (0,6)
Texnik muvaffaqiyatsizliklar	TT01	Qurilma yoki tizimning ishdan chiqishi	0,7	0,61	1,3 (2,1)
	TT02	Axborot tizimining to‘yinganligi	0,5	0,41	0,6 (1)
	TT03	Axborot tizimini ta’mirlash qobiliyatini buzilishi	0,4	0,38	0,5 (0,8)
Xodimlar harakati	TH01	Terrorizm, hujumlar, sabotaj	0,2	0,39	0,2 (0,4)
	TH02	Ijtimoiy muhandislik	0,2	0,4	0,2 (0,4)
	TH03	Qurilmaning nurlanishini ushlab turish	0,4	0,6	0,7 (1,2)
	TH04	Masofaviy monitoring	0,2	0.42	0.2 (0.4)
	TH05	Tinglash	0,6	0.31	0.5 (0.9)
	TH06	Ma’lumotlarni tashuvchi vositalarni yoki hujjatlarni o‘g‘irlash	0,6	0,4	0.7 (1.2)
	TH07	Uskunani o‘g‘irlash	0,4	0,4	0.4 (0.8)
	TH08	Raqamli identifikatorni yoki identifikatsiya ma’lumotlarini o‘g‘irlash	0,5	0.42	0.6 (1)
	TH09	Tashlab yuborilgan yoki takror ishlatilayotgan ma’lumot tashuvchi qurilmalardan ma’lumot olish	0,4	0.6	0.7 (1.2)
	TH10	Axborotni oshkor qilish	0,6	0.5	0,9 (1,5)
	TH11	Ishonchsiz manbalardan ma’lumotlarni kiritish	0,5	0	0 (0)
	TH12	Uskunani buzish	0,4	0.28	0,3 (0,6)
	TH13	Dasturiy ta’minotni buzish	0,4	0,39	0,4 (0,8)
	TH14	Veb-aloqa orqali Drive-by ekspluatatsiyasidan foydalanish	0,6	0,4	0,7 (1,2)
	TH15	Takroriy hujum, o‘rtadagi odam hujumi	0,5	0,42	0,6 (1)
	TH16	Shaxsiy ma’lumotlarni ruxsatsiz qayta ishlash	0,6	0,33	0,5 (0,9)
	TH17	Obyektlarga ruxsatsiz kirish	0,4	0,22	0,2 (0,4)
	TH18	Qurilmalardan ruxsatsiz foydalanish	0,4	0,29	0,3 (0,6)
	TH19	Qurilmalardan noto‘g‘ri foydalanish	0,6	0,18	0,3 (0,6)
	TH20	Qurilmalar yoki ma’lumot tashuvchilarni shikastlash	0,4	0,61	0,7 (1,2)
	TH21	Soxta dasturiy ta’minotni nusxalash	0,5	0,4	0,6 (1)
	TH22	Qalbaki yoki nusxalangan dasturiy ta’minotdan foydalanish	0,4	0,51	0,6 (1)

Tahdid turlari	Tahdid turlari	Tahdidning nomlanishi	Tahdidning sodir bo‘lish ehtimolligi	Tashkiliy-texnik tadbirlarning bajarilganlik holati	Salbiy oqibat yuzaga kelish riski
	TH23	Ma’lumotlarga shikast yetkazish	0,5	0,42	0,6 (1)
	TH24	Noqonuniy ma’lumotlarni qayta ishlash	0,4	0,5	0,6 (1)
	TH25	Zararli dasturlarni yuborish yoki tarqatish	0,6	0,42	0,7 (1,2)
	TH26	Joylashuvni aniqlash	0,2	0,27	0,1 (0,3)
Xizmatlar yoki funksiyalarni buzish	TC01	Foydalanishda xatoliklar	0,5	0,55	0,9 (1,5)
	TC02	Huquqlar yoki ruxsatlarni suiiste’mol qilish	0,6	0,36	0,7 (1,2)
	TC03	Huquqlar yoki ruxsatlarni soxtalashtirish	0,5	0,42	0,6 (1)
	TC04	Harakatlarni rad etish	0,7	0,6	1,3 (2,1)
Tashkiliy tahdidlar	TO01	Xodimlarning etishmasligi	0,5	0,3	0,4 (0,7)
	TO02	Resurslarning etishmasligi	0,6	0,41	0,7 (1,2)
	TO03	Xizmat ko‘rsatuvchining to‘lovga layoqatsizligi	0,4	0,52	0,6 (1)
	TO04	Qonunchilik yoki normativ-huquqiy hujjatlarning buzilishi	0,6	0,37	0,7 (1,2)
Saqlash tizimlari va infratuzilmasiga tahdidlar	TD01	Ruxsat etilmagan foydalanish	0,6	0,33	0,5 (0,9)
	TD02	Ruxsatsiz kirish	0,4	0,22	0,2 (0,4)
	TD03	Qonunlar va me’yoriy hujjatlarga rioya qilmaslik uchun yuridik javobgarlik	0,6	0,37	0,7 (1,2)
	TD04	Saqlash tizimlariga DoS va DDoS hujumlar	0.4	-	-
	TD05	Ma’lumotlarga zarar etkazish, o‘zgartirish va yo‘q qilish	0,6	0,4	0.7 (1.2)
	TD06	Ma’lumotlar sizib chiqishi	0,6	0,5	0,9 (1,5)
	TD07	Axborot tashuvchi yoki saqlovchi vositani o‘g‘irlash yoki tasodifiy yo‘qotish	0,4	0,61	0,7 (1,2)
	TD08	Zararli dastur hujumi yoki inyeksiyasi	0,6	0,42	0,7 (1,2)
	TD09	Noto‘g‘ri ishlov berish yoki foydalanish tugagandan keyin utilizatsiya qilish	0,4	0,6	0,7 (1,2)
Server uskunalari 8 (axborotning qiymati – 8)					
Jismoniy tahdidlar	TP01	Yong‘in	0,2	0,15	0,2 (0,2)
	TP02	Suv toshishi	0,2	0,15	0,2 (0,2)
	TP03	Ifloslanish, zararli radiatsiya	0,3	0,15	0,4 (0,4)
	TP04	Katta baxtsiz hodisa	0,3	0,15	0,4 (0,4)
	TP05	Portlash, halokat	0,2	0,13	0,2 (0,2)
	TP06	Chang, korroziya, muzlash	0,1	0,2	0,2 (0,2)
Tabiiy tahdidlar	TN01	Iqlim hodisasi	0,4	0,15	0,5 (0,5)
	TN02	Seysmik hodisa	0,4	0,2	0,7 (0,7)
	TN03	Vulqon hodisasi	0	0,2	0 (0)
	TN04	Meteorologik hodisa	0,3	0,15	0,4 (0,4)
	TN05	Suv toshqini	0,4	0,1	0,3 (0,3)
	TN06	Pandemiya/epidemiya hodisasi	0,4	0,2	0,6 (0,6)

Tahdid turlari	Tahdid turlari	Tahdidning nomlanishi	Tahdidning sodir bo‘lish ehtimolligi	Tashkiliy-texnik tadbirlarning bajarilganlik holati	Salbiy oqibat yuzaga kelish riski
Infratuzilmaning ishlamay qolishi	TI01	Ta’minot tizimining ishdan chiqishi	0,6	0,2	1 (1)
	TI02	Sovutish yoki shamollatish tizimining ishlamay qolishi	0,7	0,5	2,8 (2,8)
	TI03	Energiya ta’minotining buzilishi	0,7	0,4	2,2 (2,2)
	TI04	Telekommunikatsiya tarmog‘ining ishdan chiqishi	0,8	0,27	1,7 (1,7)
	TI05	Telekommunikatsiya uskunalari ishlamay qolishi	0,8	0,3	1,9 (1,9)
	TI06	Elektromagnit nurlanish	0,4	-	-
	TI07	Termal nurlanish	0,4	-	-
	TI08	Elektromagnit impulslar	0,4	-	-
Texnik muvaffaqiyatsizliklar	TT01	Qurilma yoki tizimning ishdan chiqishi	0,7	0,32	1,8 (1,8)
	TT02	Axborot tizimining to‘yinganligi	0,5	-	-
	TT03	Axborot tizimini ta’mirlash qobiliyatini buzilishi	0,4	0,3	0,9 (0,9)
Xodimlar harakati	TH01	Terrorizm, hujumlar, sabotaj	0,2	0,3	0,5 (0,5)
	TH02	Ijtimoiy muhandislik	0,2	0,27	0,4 (0,4)
	TH03	Qurilmaning nurlanishini ushlab turish	0,4	0,4	1,3 (1,3)
	TH04	Masofaviy monitoring	0,2	0,43	0,7 (0,7)
	TH05	Tinglash	0,6	0,17	0,8 (0,8)
	TH06	Ma’lumotlarni tashuvchi vositalarni yoki hujjatlarni o‘g‘irlash	0,6	0,3	1,4 (1,4)
	TH07	Uskunani o‘g‘irlash	0,4	0,3	1 (1)
	TH08	Raqamli identifikatorni yoki identifikatsiya ma’lumotlarini o‘g‘irlash	0,5	0,25	1 (1)
	TH09	Tashlab yuborilgan yoki takror ishlatilayotgan ma’lumot tashuvchi qurilmalardan ma’lumot olish	0,4	0,5	1,6 (1,6)
	TH10	Axborotni oshkor qilish	0,6	0,47	2,3 (2,3)
	TH11	Ishonchsiz manbalardan ma’lumotlarni kiritish	0,5	0,37	1,7 (1,7)
	TH12	Uskunani buzish	0,4	0,34	1,1 (1,1)
	TH13	Dasturiy ta’minotni buzish	0,4	0,24	0,8 (0,8)
	TH14	Veb-aloqa orqali Drive-by ekspluatatsiyasidan foydalanish	0,6	0,3	1,4 (1,4)
	TH15	Takroriy hujum, o‘rtadagi odam hujumi	0,5	0,1	0,4 (0,4)
	TH16	Shaxsiy ma’lumotlarni ruxsatsiz qayta ishlash	0,6	0,33	1,6 (1,6)
	TH17	Obyektlarga ruxsatsiz kirish	0,4	0,2	0,6 (0,6)
	TH18	Qurilmalardan ruxsatsiz foydalanish	0,4	0,27	0,8 (0,8)
	TH19	Qurilmalardan noto‘g‘ri foydalanish	0,6	-	-
	TH20	Qurilmalar yoki ma’lumot tashuvchilarni shikastlash	0,4	-	-
	TH21	Soxta dasturiy ta’minotni nusxalash	0,5	0,17	0,7 (0,7)
	TH22	Qalbaki yoki nusxalangan dasturiy ta’minotdan foydalanish	0,4	0,1	0,3 (0,3)
	TH23	Ma’lumotlarga shikast yetkazish	0,5	0,28	1,1 (1,1)
	TH24	Noqonuniy ma’lumotlarni qayta ishlash	0,4	0,48	1,5 (1,5)

Tahdid turlari	Tahdid turlari	Tahdidning nomlanishi	Tahdidning sodir bo‘lish ehtimolligi	Tashkiliy-texnik tadbirlarning bajarilganlik holati	Salbiy oqibat yuzaga kelish riski
	TH25	Zararli dasturlarni yuborish yoki tarqatish	0,6	-	-
	TH26	Joylashuvni aniqlash	0,2	0,3	0,5 (0,5)
Xizmatlar yoki funksiyalarni buzish	TC01	Foydalanishda xatoliklar	0,5	0,2	0,8 (0,8)
	TC02	Huquqlar yoki ruxsatlarni suiiste’mol qilish	0,6	0,15	0,7 (0,7)
	TC03	Huquqlar yoki ruxsatlarni soxtalashtirish	0,5	0,24	1 (1)
	TC04	Harakatlarni rad etish	0,7	0,3	1,7 (1,7)
Tashkiliy tahdidlar	TO01	Xodimlarning etishmasligi	0,5	0,2	0,8 (0,8)
	TO02	Resurslarning etishmasligi	0,6	0,4	1,9 (1,9)
	TO03	Xizmat ko‘rsatuvchining to‘lovga layoqatsizligi	0,4	0,2	0,6 (0,6)
	TO04	Qonunchilik yoki normativ-huquqiy hujjatlarning buzilishi	0,6	0,24	1,2 (1,2)
Saqlash tizimlari va infratuzilmasiga tahdidlar	TD01	Ruxsat etilmagan foydalanish	0,6	0,33	1,6 (1,6)
	TD02	Ruxsatsiz kirish	0,4	0,2	0,6 (0,6)
	TD03	Qonunlar va me’yoriy hujjatlarga rioya qilmaslik uchun yuridik javobgarlik	0,6	0,24	1,2 (1,2)
	TD04	Saqlash tizimlariga DoS va DDoS hujumlar	-	-	-
	TD05	Ma’lumotlarga zarar etkazish, o‘zgartirish va yo‘q qilish	0,6	0,3	1,4 (1,4)
	TD06	Ma’lumotlar sizib chiqishi	0,6	0,47	2,3 (2,3)
	TD07	Axborot tashuvchi yoki saqlovchi vositani o‘g‘irlash yoki tasodifiy yo‘qotish	0,4	-	-
	TD08	Zararli dastur hujumi yoki inyeksiyasi	0,6	-	-
	TD09	Noto‘g‘ri ishlov berish yoki foydalanish tugagandan keyin utilizatsiya qilish	0,4	0,5	1,6 (1,6)
Kirish chiqishni nazorat qilish tizimi 3 (axborotning qiymati – 5)					
Jismoniy tahdidlar	TP01	Yong‘in	0,2	0,26	0,1 (0,3)
	TP02	Suv toshishi	0,2	0,3	0,1 (0,3)
	TP03	Ifloslanish, zararli radiatsiya	0,3	0,31	0,3 (0,4)
	TP04	Katta baxtsiz hodisa	0,3	0,33	0,3 (0,4)
	TP05	Portlash, halokat	0,2	0,19	0,1 (0,2)
	TP06	Chang, korroziya, muzlash	0,1	0,37	0,1 (0,2)
Tabiiy tahdidlar	TN01	Iqlim hodisasi	0,4	0,19	0,2 (0,4)
	TN02	Seysmik hodisa	0,4	0,3	0,3 (0,6)
	TN03	Vulqon hodisasi	0	0,2	0 (0)
	TN04	Meteorologik hodisa	0,3	0,22	0,1 (0,3)
	TN05	Suv toshqini	0,4	0,18	0,2 (0,4)
	TN06	Pandemiya/epidemiya hodisasi	0,4	0,31	0,3 (0,6)
Infratuzilmaning ishlamay qolishi	TI01	Ta’minot tizimining ishdan chiqishi	0,6	0,5	0,9 (1,5)
	TI02	Sovutish yoki shamollatish tizimining ishlamay qolishi	0,7	0,48	1,1 (1,7)

Tahdid turlari	Tahdid turlari	Tahdidning nomlanishi	Tahdidning sodir bo‘lish ehtimolligi	Tashkiliy-texnik tadbirlarning bajarilganlik holati	Salbiy oqibat yuzaga kelish riski
	TI03	Energiya ta’minotining buzilishi	0,7	0,4	0,8 (1,4)
	TI04	Telekommunikatsiya tarmog‘ining ishdan chiqishi	0,8	0,42	0,9 (1,6)
	TI05	Telekommunikatsiya uskunalari ishlamay qolishi	0,8	0,41	0,9 (1,6)
	TI06	Elektromagnit nurlanish	0,4	0,3	0,4 (0,6)
	TI07	Termal nurlanish	0,4	0,5	0,6 (1)
	TI08	Elektromagnit impulslar	0,4	0,33	0,3 (0,6)
Texnik muvaffaqiyatsizliklar	TT01	Qurilma yoki tizimning ishdan chiqishi	0,7	0,61	1,3 (2,1)
	TT02	Axborot tizimining to‘yinganligi	0,5	0,41	0,6 (1)
	TT03	Axborot tizimini ta’mirlash qobiliyatini buzilishi	0,4	0,38	0,5 (0,8)
Xodimlar harakati	TH01	Terrorizm, hujumlar, sabotaj	0,2	0,39	0,2 (0,4)
	TH02	Ijtimoiy muhandislik	0,2	0,4	0,2 (0,4)
	TH03	Qurilmaning nurlanishini ushlab turish	0,4	0,6	0,7 (1,2)
	TH04	Masofaviy monitoring	0,2	0.42	0.2 (0.4)
	TH05	Tinglash	0,6	0.31	0.5 (0.9)
	TH06	Ma’lumotlarni tashuvchi vositalarni yoki hujjatlarni o‘g‘irlash	0,6	0,4	0.7 (1.2)
	TH07	Uskunani o‘g‘irlash	0,4	0,4	0.4 (0.8)
	TH08	Raqamli identifikatorni yoki identifikatsiya ma’lumotlarini o‘g‘irlash	0,5	0.42	0.6 (1)
	TH09	Tashlab yuborilgan yoki takror ishlatilayotgan ma’lumot tashuvchi qurilmalardan ma’lumot olish	0,4	0.6	0.7 (1.2)
	TH10	Axborotni oshkor qilish	0,6	0.5	0,9 (1,5)
	TH11	Ishonchsiz manbalardan ma’lumotlarni kiritish	0,5	0	0 (0)
	TH12	Uskunani buzish	0,4	0.28	0,3 (0,6)
	TH13	Dasturiy ta’minotni buzish	0,4	0,39	0,4 (0,8)
	TH14	Veb-aloqa orqali Drive-by ekspluatatsiyasidan foydalanish	0,6	0,4	0,7 (1,2)
	TH15	Takroriy hujum, o‘rtadagi odam hujumi	0,5	0,42	0,6 (1)
	TH16	Shaxsiy ma’lumotlarni ruxsatsiz qayta ishlash	0,6	0,33	0,5 (0,9)
	TH17	Obyektlarga ruxsatsiz kirish	0,4	0,22	0,2 (0,4)
	TH18	Qurilmalardan ruxsatsiz foydalanish	0,4	0,29	0,3 (0,6)
	TH19	Qurilmalardan noto‘g‘ri foydalanish	0,6	0,18	0,3 (0,6)
	TH20	Qurilmalar yoki ma’lumot tashuvchilarni shikastlash	0,4	0,61	0,7 (1,2)
	TH21	Soxta dasturiy ta’minotni nusxalash	0,5	0,4	0,6 (1)
	TH22	Qalbaki yoki nusxalangan dasturiy ta’minotdan foydalanish	0,4	0,51	0,6 (1)
	TH23	Ma’lumotlarga shikast yetkazish	0,5	0,42	0,6 (1)
	TH24	Noqonuniy ma’lumotlarni qayta ishlash	0,4	0,5	0,6 (1)
	TH25	Zararli dasturlarni yuborish yoki tarqatish	0,6	0,42	0,7 (1,2)
	TH26	Joylashuvni aniqlash	0,2	0,27	0,1 (0,3)

Tahdid turlari	Tahdid turlari	Tahdidning nomlanishi	Tahdidning sodir bo‘lish ehtimolligi	Tashkiliy-texnik tadbirlarning bajarilganlik holati	Salbiy oqibat yuzaga kelish riski
Xizmatlar yoki funksiyalarni buzish	TC01	Foydalanishda xatoliklar	0,5	0,55	0,9 (1,5)
	TC02	Huquqlar yoki ruxsatlarni suiiste’mol qilish	0,6	0,36	0,7 (1,2)
	TC03	Huquqlar yoki ruxsatlarni soxtalashtirish	0,5	0,42	0,6 (1)
	TC04	Harakatlarni rad etish	0,7	0,6	1,3 (2,1)
Tashkiliy tahdidlar	TO01	Xodimlarning etishmasligi	0,5	0,3	0,4 (0,7)
	TO02	Resurslarning etishmasligi	0,6	0,41	0,7 (1,2)
	TO03	Xizmat ko‘rsatuvchining to‘lovga layoqatsizligi	0,4	0,52	0,6 (1)
	TO04	Qonunchilik yoki normativ-huquqiy hujjatlarning buzilishi	0,6	0,37	0,7 (1,2)
Saqlash tizimlari va infratuzilmasiga tahdidlar	TD01	Ruxsat etilmagan foydalanish	0,6	0,33	0,5 (0,9)
	TD02	Ruxsatsiz kirish	0,4	0,22	0,2 (0,4)
	TD03	Qonunlar va me’yoriy hujjatlarga rioya qilmaslik uchun yuridik javobgarlik	0,6	0,37	0,7 (1,2)
	TD04	Saqlash tizimlariga DoS va DDoS hujumlar	0.4	-	-
	TD05	Ma’lumotlarga zarar etkazish, o‘zgartirish va yo‘q qilish	0,6	0,4	0.7 (1.2)
	TD06	Ma’lumotlar sizib chiqishi	0,6	0,5	0,9 (1,5)
	TD07	Axborot tashuvchi yoki saqlovchi vositani o‘g‘irlash yoki tasodifiy yo‘qotish	0,4	0,61	0,7 (1,2)
	TD08	Zararli dastur hujumi yoki inyeksiyasi	0,6	0,42	0,7 (1,2)
	TD09	Noto‘g‘ri ishlov berish yoki foydalanish tugagandan keyin utilizatsiya qilish	0,4	0,6	0,7 (1,2)
Videokuzatuv tizimi 3 (axborotning qiymati – 5)					
Jismoniy tahdidlar	TP01	Yong‘in	0,2	0,26	0,1 (0,3)
	TP02	Suv toshishi	0,2	0,3	0,1 (0,3)
	TP03	Ifloslanish, zararli radiatsiya	0,3	0,31	0,3 (0,4)
	TP04	Katta baxtsiz hodisa	0,3	0,33	0,3 (0,4)
	TP05	Portlash, halokat	0,2	0,19	0,1 (0,2)
	TP06	Chang, korroziya, muzlash	0,1	0,37	0,1 (0,2)
Tabiiy tahdidlar	TN01	Iqlim hodisasi	0,4	0,19	0,2 (0,4)
	TN02	Seysmik hodisa	0,4	0,3	0,3 (0,6)
	TN03	Vulqon hodisasi	0	0,2	0 (0)
	TN04	Meteorologik hodisa	0,3	0,22	0,1 (0,3)
	TN05	Suv toshqini	0,4	0,18	0,2 (0,4)
	TN06	Pandemiya/epidemiya hodisasi	0,4	0,31	0,3 (0,6)
Infratuzilmaning ishlamay qolishi	TI01	Ta’minot tizimining ishdan chiqishi	0,6	0,5	0,9 (1,5)
	TI02	Sovutish yoki shamollatish tizimining ishlamay qolishi	0,7	0,48	1,1 (1,7)
	TI03	Energiya ta’minotining buzilishi	0,7	0,4	0,8 (1,4)
	TI04	Telekommunikatsiya tarmog‘ining ishdan chiqishi	0,8	0,42	0,9 (1,6)

Tahdid turlari	Tahdid turlari	Tahdidning nomlanishi	Tahdidning sodir bo‘lish ehtimolligi	Tashkiliy-texnik tadbirlarning bajarilganlik holati	Salbiy oqibat yuzaga kelish riski
	TI05	Telekommunikatsiya uskunalari ishlamay qolishi	0,8	0,41	0,9 (1,6)
	TI06	Elektromagnit nurlanish	0,4	0,3	0,4 (0,6)
	TI07	Termal nurlanish	0,4	0,5	0,6 (1)
	TI08	Elektromagnit impulslar	0,4	0,33	0,3 (0,6)
Texnik muvaffaqiyatsizliklar	TT01	Qurilma yoki tizimning ishdan chiqishi	0,7	0,61	1,3 (2,1)
	TT02	Axborot tizimining to‘yinganligi	0,5	0,41	0,6 (1)
	TT03	Axborot tizimini ta’mirlash qobiliyatini buzilishi	0,4	0,38	0,5 (0,8)
Xodimlar harakati	TH01	Terrorizm, hujumlar, sabotaj	0,2	0,39	0,2 (0,4)
	TH02	Ijtimoiy muhandislik	0,2	0,4	0,2 (0,4)
	TH03	Qurilmaning nurlanishini ushlab turish	0,4	0,6	0,7 (1,2)
	TH04	Masofaviy monitoring	0,2	0.42	0.2 (0.4)
	TH05	Tinglash	0,6	0.31	0.5 (0.9)
	TH06	Ma’lumotlarni tashuvchi vositalarni yoki hujjatlarni o‘g‘irlash	0,6	0,4	0.7 (1.2)
	TH07	Uskunani o‘g‘irlash	0,4	0,4	0.4 (0.8)
	TH08	Raqamli identifikatorni yoki identifikatsiya ma’lumotlarini o‘g‘irlash	0,5	0.42	0.6 (1)
	TH09	Tashlab yuborilgan yoki takror ishlatilayotgan ma’lumot tashuvchi qurilmalardan ma’lumot olish	0,4	0.6	0.7 (1.2)
	TH10	Axborotni oshkor qilish	0,6	0.5	0,9 (1,5)
	TH11	Ishonchsiz manbalardan ma’lumotlarni kiritish	0,5	0	0 (0)
	TH12	Uskunani buzish	0,4	0.28	0,3 (0,6)
	TH13	Dasturiy ta’minotni buzish	0,4	0,39	0,4 (0,8)
	TH14	Veb-aloqa orqali Drive-by ekspluatatsiyasidan foydalanish	0,6	0,4	0,7 (1,2)
	TH15	Takroriy hujum, o‘rtadagi odam hujumi	0,5	0,42	0,6 (1)
	TH16	Shaxsiy ma’lumotlarni ruxsatsiz qayta ishlash	0,6	0,33	0,5 (0,9)
	TH17	Obyektlarga ruxsatsiz kirish	0,4	0,22	0,2 (0,4)
	TH18	Qurilmalardan ruxsatsiz foydalanish	0,4	0,29	0,3 (0,6)
	TH19	Qurilmalardan noto‘g‘ri foydalanish	0,6	0,18	0,3 (0,6)
	TH20	Qurilmalar yoki ma’lumot tashuvchilarni shikastlash	0,4	0,61	0,7 (1,2)
	TH21	Soxta dasturiy ta’minotni nusxalash	0,5	0,4	0,6 (1)
	TH22	Qalbaki yoki nusxalangan dasturiy ta’minotdan foydalanish	0,4	0,51	0,6 (1)
	TH23	Ma’lumotlarga shikast yetkazish	0,5	0,42	0,6 (1)
	TH24	Noqonuniy ma’lumotlarni qayta ishlash	0,4	0,5	0,6 (1)
	TH25	Zararli dasturlarni yuborish yoki tarqatish	0,6	0,42	0,7 (1,2)
	TH26	Joylashuvni aniqlash	0,2	0,27	0,1 (0,3)
Xizmatlar yoki funksiyalarni buzish	TC01	Foydalanishda xatoliklar	0,5	0,55	0,9 (1,5)
	TC02	Huquqlar yoki ruxsatlarni suiiste’mol qilish	0,6	0,36	0,7 (1,2)

Tahdid turlari	Tahdid turlari	Tahdidning nomlanishi	Tahdidning sodir bo‘lish ehtimolligi	Tashkiliy-texnik tadbirlarning bajarilganlik holati	Salbiy oqibat yuzaga kelish riski
	TC03	Huquqlar yoki ruxsatlarni soxtalashtirish	0,5	0,42	0,6 (1)
	TC04	Harakatlarni rad etish	0,7	0,6	1,3 (2,1)
Tashkiliy tahdidlar	TO01	Xodimlarning etishmasligi	0,5	0,3	0,4 (0,7)
	TO02	Resurslarning etishmasligi	0,6	0,41	0,7 (1,2)
	TO03	Xizmat ko‘rsatuvchining to‘lovga layoqatsizligi	0,4	0,52	0,6 (1)
	TO04	Qonunchilik yoki normativ-huquqiy hujjatlarning buzilishi	0,6	0,37	0,7 (1,2)
Saqlash tizimlari va infratuzilmasiga tahdidlar	TD01	Ruxsat etilmagan foydalanish	0,6	0,33	0,5 (0,9)
	TD02	Ruxsatsiz kirish	0,4	0,22	0,2 (0,4)
	TD03	Qonunlar va me’yoriy hujjatlarga rioya qilmaslik uchun yuridik javobgarlik	0,6	0,37	0,7 (1,2)
	TD04	Saqlash tizimlariga DoS va DDoS hujumlar	0.4	-	-
	TD05	Ma’lumotlarga zarar etkazish, o‘zgartirish va yo‘q qilish	0,6	0,4	0.7 (1.2)
	TD06	Ma’lumotlar sizib chiqishi	0,6	0,5	0,9 (1,5)
	TD07	Axborot tashuvchi yoki saqlovchi vositani o‘g‘irlash yoki tasodifiy yo‘qotish	0,4	0,61	0,7 (1,2)
	TD08	Zararli dastur hujumi yoki inyeksiyasi	0,6	0,42	0,7 (1,2)
	TD09	Noto‘g‘ri ishlov berish yoki foydalanish tugagandan keyin utilizatsiya qilish	0,4	0,6	0,7 (1,2)
citrus.buxdu.uz 3 (axborotning qiymati – 5)					
Jismoniy tahdidlar	TP01	Yong‘in	0,2	0,26	0,1 (0,3)
	TP02	Suv toshishi	0,2	0,3	0,1 (0,3)
	TP03	Ifloslanish, zararli radiatsiya	0,3	0,31	0,3 (0,4)
	TP04	Katta baxtsiz hodisa	0,3	0,33	0,3 (0,4)
	TP05	Portlash, halokat	0,2	0,19	0,1 (0,2)
	TP06	Chang, korroziya, muzlash	0,1	0,37	0,1 (0,2)
Tabiiy tahdidlar	TN01	Iqlim hodisasi	0,4	0,19	0,2 (0,4)
	TN02	Seysmik hodisa	0,4	0,3	0,3 (0,6)
	TN03	Vulqon hodisasi	0	0,2	0 (0)
	TN04	Meteorologik hodisa	0,3	0,22	0,1 (0,3)
	TN05	Suv toshqini	0,4	0,18	0,2 (0,4)
	TN06	Pandemiya/epidemiya hodisasi	0,4	0,31	0,3 (0,6)
Infratuzilmaning ishlamay qolishi	TI01	Ta’minot tizimining ishdan chiqishi	0,6	0,5	0,9 (1,5)
	TI02	Sovutish yoki shamollatish tizimining ishlamay qolishi	0,7	0,48	1,1 (1,7)
	TI03	Energiya ta’minotining buzilishi	0,7	0,4	0,8 (1,4)
	TI04	Telekommunikatsiya tarmog‘ining ishdan chiqishi	0,8	0,42	0,9 (1,6)
	TI05	Telekommunikatsiya uskunalari ishlamay qolishi	0,8	0,41	0,9 (1,6)
	TI06	Elektromagnit nurlanish	0,4	0,3	0,4 (0,6)

Tahdid turlari	Tahdid turlari	Tahdidning nomlanishi	Tahdidning sodir bo‘lish ehtimolligi	Tashkiliy-texnik tadbirlarning bajarilganlik holati	Salbiy oqibat yuzaga kelish riski
	TI07	Termal nurlanish	0,4	0,5	0,6 (1)
	TI08	Elektromagnit impulslar	0,4	0,33	0,3 (0,6)
Texnik muvaffaqiyatsizliklar	TT01	Qurilma yoki tizimning ishdan chiqishi	0,7	0,61	1,3 (2,1)
	TT02	Axborot tizimining to‘yinganligi	0,5	0,41	0,6 (1)
	TT03	Axborot tizimini ta’mirlash qobiliyatini buzilishi	0,4	0,38	0,5 (0,8)
Xodimlar harakati	TH01	Terrorizm, hujumlar, sabotaj	0,2	0,39	0,2 (0,4)
	TH02	Ijtimoiy muhandislik	0,2	0,4	0,2 (0,4)
	TH03	Qurilmaning nurlanishini ushlab turish	0,4	0,6	0,7 (1,2)
	TH04	Masofaviy monitoring	0,2	0.42	0.2 (0.4)
	TH05	Tinglash	0,6	0.31	0.5 (0.9)
	TH06	Ma’lumotlarni tashuvchi vositalarni yoki hujjatlarni o‘g‘irlash	0,6	0,4	0.7 (1.2)
	TH07	Uskunani o‘g‘irlash	0,4	0,4	0.4 (0.8)
	TH08	Raqamli identifikatorni yoki identifikatsiya ma’lumotlarini o‘g‘irlash	0,5	0.42	0.6 (1)
	TH09	Tashlab yuborilgan yoki takror ishlatilayotgan ma’lumot tashuvchi qurilmalardan ma’lumot olish	0,4	0.6	0.7 (1.2)
	TH10	Axborotni oshkor qilish	0,6	0.5	0,9 (1,5)
	TH11	Ishonchsiz manbalardan ma’lumotlarni kiritish	0,5	0	0 (0)
	TH12	Uskunani buzish	0,4	0.28	0,3 (0,6)
	TH13	Dasturiy ta’minotni buzish	0,4	0,39	0,4 (0,8)
	TH14	Veb-aloqa orqali Drive-by ekspluatatsiyasidan foydalanish	0,6	0,4	0,7 (1,2)
	TH15	Takroriy hujum, o‘rtadagi odam hujumi	0,5	0,42	0,6 (1)
	TH16	Shaxsiy ma’lumotlarni ruxsatsiz qayta ishlash	0,6	0,33	0,5 (0,9)
	TH17	Obyektlarga ruxsatsiz kirish	0,4	0,22	0,2 (0,4)
	TH18	Qurilmalardan ruxsatsiz foydalanish	0,4	0,29	0,3 (0,6)
	TH19	Qurilmalardan noto‘g‘ri foydalanish	0,6	0,18	0,3 (0,6)
	TH20	Qurilmalar yoki ma’lumot tashuvchilarni shikastlash	0,4	0,61	0,7 (1,2)
	TH21	Soxta dasturiy ta’minotni nusxalash	0,5	0,4	0,6 (1)
	TH22	Qalbaki yoki nusxalangan dasturiy ta’minotdan foydalanish	0,4	0,51	0,6 (1)
	TH23	Ma’lumotlarga shikast yetkazish	0,5	0,42	0,6 (1)
	TH24	Noqonuniy ma’lumotlarni qayta ishlash	0,4	0,5	0,6 (1)
	TH25	Zararli dasturlarni yuborish yoki tarqatish	0,6	0,42	0,7 (1,2)
	TH26	Joylashuvni aniqlash	0,2	0,27	0,1 (0,3)
Xizmatlar yoki funksiyalarni buzish	TC01	Foydalanishda xatoliklar	0,5	0,55	0,9 (1,5)
	TC02	Huquqlar yoki ruxsatlarni suiiste’mol qilish	0,6	0,36	0,7 (1,2)
	TC03	Huquqlar yoki ruxsatlarni soxtalashtirish	0,5	0,42	0,6 (1)
	TC04	Harakatlarni rad etish	0,7	0,6	1,3 (2,1)

Tahdid turlari	Tahdid turlari	Tahdidning nomlanishi	Tahdidning sodir bo‘lish ehtimolligi	Tashkiliy-texnik tadbirlarning bajarilganlik holati	Salbiy oqibat yuzaga kelish riski
Tashkiliy tahdidlar	TO01	Xodimlarning etishmasligi	0,5	0,3	0,4 (0,7)
	TO02	Resurslarning etishmasligi	0,6	0,41	0,7 (1,2)
	TO03	Xizmat ko‘rsatuvchining to‘lovga layoqatsizligi	0,4	0,52	0,6 (1)
	TO04	Qonunchilik yoki normativ-huquqiy hujjatlarning buzilishi	0,6	0,37	0,7 (1,2)
Saqlash tizimlari va infratuzilmasiga tahdidlar	TD01	Ruxsat etilmagan foydalanish	0,6	0,33	0,5 (0,9)
	TD02	Ruxsatsiz kirish	0,4	0,22	0,2 (0,4)
	TD03	Qonunlar va me’yoriy hujjatlarga rioya qilmaslik uchun yuridik javobgarlik	0,6	0,37	0,7 (1,2)
	TD04	Saqlash tizimlariga DoS va DDoS hujumlar	0.4	-	-
	TD05	Ma’lumotlarga zarar etkazish, o‘zgartirish va yo‘q qilish	0,6	0,4	0.7 (1.2)
	TD06	Ma’lumotlar sizib chiqishi	0,6	0,5	0,9 (1,5)
	TD07	Axborot tashuvchi yoki saqlovchi vositani o‘g‘irlash yoki tasodifiy yo‘qotish	0,4	0,61	0,7 (1,2)
	TD08	Zararli dastur hujumi yoki inyeksiyasi	0,6	0,42	0,7 (1,2)
	TD09	Noto‘g‘ri ishlov berish yoki foydalanish tugagandan keyin utilizatsiya qilish	0,4	0,6	0,7 (1,2)
srep.buxdu.uz (axborotning qiymati – 5)					
Jismoniy tahdidlar	TP01	Yong‘in	0,2	0,26	0,1 (0,3)
	TP02	Suv toshishi	0,2	0,3	0,1 (0,3)
	TP03	Ifloslanish, zararli radiatsiya	0,3	0,31	0,3 (0,4)
	TP04	Katta baxtsiz hodisa	0,3	0,33	0,3 (0,4)
	TP05	Portlash, halokat	0,2	0,19	0,1 (0,2)
	TP06	Chang, korroziya, muzlash	0,1	0,37	0,1 (0,2)
Tabiiy tahdidlar	TN01	Iqlim hodisasi	0,4	0,19	0,2 (0,4)
	TN02	Seysmik hodisa	0,4	0,3	0,3 (0,6)
	TN03	Vulqon hodisasi	0	0,2	0 (0)
	TN04	Meteorologik hodisa	0,3	0,22	0,1 (0,3)
	TN05	Suv toshqini	0,4	0,18	0,2 (0,4)
	TN06	Pandemiya/epidemiya hodisasi	0,4	0,31	0,3 (0,6)
Infratuzilmaning ishlamay qolishi	TI01	Ta’minot tizimining ishdan chiqishi	0,6	0,5	0,9 (1,5)
	TI02	Sovutish yoki shamollatish tizimining ishlamay qolishi	0,7	0,48	1,1 (1,7)
	TI03	Energiya ta’minotining buzilishi	0,7	0,4	0,8 (1,4)
	TI04	Telekommunikatsiya tarmog‘ining ishdan chiqishi	0,8	0,42	0,9 (1,6)
	TI05	Telekommunikatsiya uskunalari ishlamay qolishi	0,8	0,41	0,9 (1,6)
	TI06	Elektromagnit nurlanish	0,4	0,3	0,4 (0,6)
	TI07	Termal nurlanish	0,4	0,5	0,6 (1)
	TI08	Elektromagnit impulslar	0,4	0,33	0,3 (0,6)

Tahdid turlari	Tahdid turlari	Tahdidning nomlanishi	Tahdidning sodir bo‘lish ehtimolligi	Tashkiliy-texnik tadbirlarning bajarilganlik holati	Salbiy oqibat yuzaga kelish riski
Texnik muvaffaqiyatsizliklar	TT01	Qurilma yoki tizimning ishdan chiqishi	0,7	0,61	1,3 (2,1)
	TT02	Axborot tizimining to‘yinganligi	0,5	0,41	0,6 (1)
	TT03	Axborot tizimini ta’mirlash qobiliyatini buzilishi	0,4	0,38	0,5 (0,8)
Xodimlar harakati	TH01	Terrorizm, hujumlar, sabotaj	0,2	0,39	0,2 (0,4)
	TH02	Ijtimoiy muhandislik	0,2	0,4	0,2 (0,4)
	TH03	Qurilmaning nurlanishini ushlab turish	0,4	0,6	0,7 (1,2)
	TH04	Masofaviy monitoring	0,2	0.42	0.2 (0.4)
	TH05	Tinglash	0,6	0.31	0.5 (0.9)
	TH06	Ma’lumotlarni tashuvchi vositalarni yoki hujjatlarni o‘g‘irlash	0,6	0,4	0.7 (1.2)
	TH07	Uskunani o‘g‘irlash	0,4	0,4	0.4 (0.8)
	TH08	Raqamli identifikatorni yoki identifikatsiya ma’lumotlarini o‘g‘irlash	0,5	0.42	0.6 (1)
	TH09	Tashlab yuborilgan yoki takror ishlatilayotgan ma’lumot tashuvchi qurilmalardan ma’lumot olish	0,4	0.6	0.7 (1.2)
	TH10	Axborotni oshkor qilish	0,6	0.5	0,9 (1,5)
	TH11	Ishonchsiz manbalardan ma’lumotlarni kiritish	0,5	0	0 (0)
	TH12	Uskunani buzish	0,4	0.28	0,3 (0,6)
	TH13	Dasturiy ta’minotni buzish	0,4	0,39	0,4 (0,8)
	TH14	Veb-aloqa orqali Drive-by ekspluatatsiyasidan foydalanish	0,6	0,4	0,7 (1,2)
	TH15	Takroriy hujum, o‘rtadagi odam hujumi	0,5	0,42	0,6 (1)
	TH16	Shaxsiy ma’lumotlarni ruxsatsiz qayta ishlash	0,6	0,33	0,5 (0,9)
	TH17	Obyektlarga ruxsatsiz kirish	0,4	0,22	0,2 (0,4)
	TH18	Qurilmalardan ruxsatsiz foydalanish	0,4	0,29	0,3 (0,6)
	TH19	Qurilmalardan noto‘g‘ri foydalanish	0,6	0,18	0,3 (0,6)
	TH20	Qurilmalar yoki ma’lumot tashuvchilarni shikastlash	0,4	0,61	0,7 (1,2)
	TH21	Soxta dasturiy ta’minotni nusxalash	0,5	0,4	0,6 (1)
	TH22	Qalbaki yoki nusxalangan dasturiy ta’minotdan foydalanish	0,4	0,51	0,6 (1)
	TH23	Ma’lumotlarga shikast yetkazish	0,5	0,42	0,6 (1)
	TH24	Noqonuniy ma’lumotlarni qayta ishlash	0,4	0,5	0,6 (1)
	TH25	Zararli dasturlarni yuborish yoki tarqatish	0,6	0,42	0,7 (1,2)
	TH26	Joylashuvni aniqlash	0,2	0,27	0,1 (0,3)
Xizmatlar yoki funksiyalarni buzish	TC01	Foydalanishda xatoliklar	0,5	0,55	0,9 (1,5)
	TC02	Huquqlar yoki ruxsatlarni suiiste’mol qilish	0,6	0,36	0,7 (1,2)
	TC03	Huquqlar yoki ruxsatlarni soxtalashtirish	0,5	0,42	0,6 (1)
	TC04	Harakatlarni rad etish	0,7	0,6	1,3 (2,1)
Tashkiliy tahdidlar	TO01	Xodimlarning etishmasligi	0,5	0,3	0,4 (0,7)
	TO02	Resurslarning etishmasligi	0,6	0,41	0,7 (1,2)

Tahdid turlari	Tahdid turlari	Tahdidning nomlanishi	Tahdidning sodir bo‘lish ehtimolligi	Tashkiliy-texnik tadbirlarning bajarilganlik holati	Salbiy oqibat yuzaga kelish riski
	TO03	Xizmat ko‘rsatuvchining to‘lovga layoqatsizligi	0,4	0,52	0,6 (1)
	TO04	Qonunchilik yoki normativ-huquqiy hujjatlarning buzilishi	0,6	0,37	0,7 (1,2)
Saqlash tizimlari va infratuzilmasiga tahdidlar	TD01	Ruxsat etilmagan foydalanish	0,6	0,33	0,5 (0,9)
	TD02	Ruxsatsiz kirish	0,4	0,22	0,2 (0,4)
	TD03	Qonunlar va me’yoriy hujjatlarga rioya qilmaslik uchun yuridik javobgarlik	0,6	0,37	0,7 (1,2)
	TD04	Saqlash tizimlariga DoS va DDoS hujumlar	0.4	-	-
	TD05	Ma’lumotlarga zarar etkazish, o‘zgartirish va yo‘q qilish	0,6	0,4	0.7 (1.2)
	TD06	Ma’lumotlar sizib chiqishi	0,6	0,5	0,9 (1,5)
	TD07	Axborot tashuvchi yoki saqlovchi vositani o‘g‘irlash yoki tasodifiy yo‘qotish	0,4	0,61	0,7 (1,2)
	TD08	Zararli dastur hujumi yoki inyeksiyasi	0,6	0,42	0,7 (1,2)
	TD09	Noto‘g‘ri ishlov berish yoki foydalanish tugagandan keyin utilizatsiya qilish	0,4	0,6	0,7 (1,2)
pedskills.buxdu.uz (axborotning qiymati – 5)					
Jismoniy tahdidlar	TP01	Yong‘in	0,2	0,26	0,1 (0,3)
	TP02	Suv toshishi	0,2	0,3	0,1 (0,3)
	TP03	Ifloslanish, zararli radiatsiya	0,3	0,31	0,3 (0,4)
	TP04	Katta baxtsiz hodisa	0,3	0,33	0,3 (0,4)
	TP05	Portlash, halokat	0,2	0,19	0,1 (0,2)
	TP06	Chang, korroziya, muzlash	0,1	0,37	0,1 (0,2)
Tabiiy tahdidlar	TN01	Iqlim hodisasi	0,4	0,19	0,2 (0,4)
	TN02	Seysmik hodisa	0,4	0,3	0,3 (0,6)
	TN03	Vulqon hodisasi	0	0,2	0 (0)
	TN04	Meteorologik hodisa	0,3	0,22	0,1 (0,3)
	TN05	Suv toshqini	0,4	0,18	0,2 (0,4)
	TN06	Pandemiya/epidemiya hodisasi	0,4	0,31	0,3 (0,6)
Infratuzilmaning ishlamay qolishi	TI01	Ta’minot tizimining ishdan chiqishi	0,6	0,5	0,9 (1,5)
	TI02	Sovutish yoki shamollatish tizimining ishlamay qolishi	0,7	0,48	1,1 (1,7)
	TI03	Energiya ta’minotining buzilishi	0,7	0,4	0,8 (1,4)
	TI04	Telekommunikatsiya tarmog‘ining ishdan chiqishi	0,8	0,42	0,9 (1,6)
	TI05	Telekommunikatsiya uskunalari ishlamay qolishi	0,8	0,41	0,9 (1,6)
	TI06	Elektromagnit nurlanish	0,4	0,3	0,4 (0,6)
	TI07	Termal nurlanish	0,4	0,5	0,6 (1)
	TI08	Elektromagnit impulslar	0,4	0,33	0,3 (0,6)
Texnik muvaffaqiyatsizliklar	TT01	Qurilma yoki tizimning ishdan chiqishi	0,7	0,61	1,3 (2,1)
	TT02	Axborot tizimining to‘yinganligi	0,5	0,41	0,6 (1)

Tahdid turlari	Tahdid turlari	Tahdidning nomlanishi	Tahdidning sodir bo‘lish ehtimolligi	Tashkiliy-texnik tadbirlarning bajarilganlik holati	Salbiy oqibat yuzaga kelish riski
	TT03	Axborot tizimini ta’mirlash qobiliyatini buzilishi	0,4	0,38	0,5 (0,8)
Xodimlar harakati	TH01	Terrorizm, hujumlar, sabotaj	0,2	0,39	0,2 (0,4)
	TH02	Ijtimoiy muhandislik	0,2	0,4	0,2 (0,4)
	TH03	Qurilmaning nurlanishini ushlab turish	0,4	0,6	0,7 (1,2)
	TH04	Masofaviy monitoring	0,2	0.42	0.2 (0.4)
	TH05	Tinglash	0,6	0.31	0.5 (0.9)
	TH06	Ma’lumotlarni tashuvchi vositalarni yoki hujjatlarni o‘g‘irlash	0,6	0,4	0.7 (1.2)
	TH07	Uskunani o‘g‘irlash	0,4	0,4	0.4 (0.8)
	TH08	Raqamli identifikatorni yoki identifikatsiya ma’lumotlarini o‘g‘irlash	0,5	0.42	0.6 (1)
	TH09	Tashlab yuborilgan yoki takror ishlatilayotgan ma’lumot tashuvchi qurilmalardan ma’lumot olish	0,4	0.6	0.7 (1.2)
	TH10	Axborotni oshkor qilish	0,6	0.5	0,9 (1,5)
	TH11	Ishonchsiz manbalardan ma’lumotlarni kiritish	0,5	0	0 (0)
	TH12	Uskunani buzish	0,4	0.28	0,3 (0,6)
	TH13	Dasturiy ta’minotni buzish	0,4	0,39	0,4 (0,8)
	TH14	Veb-aloqa orqali Drive-by ekspluatatsiyasidan foydalanish	0,6	0,4	0,7 (1,2)
	TH15	Takroriy hujum, o‘rtadagi odam hujumi	0,5	0,42	0,6 (1)
	TH16	Shaxsiy ma’lumotlarni ruxsatsiz qayta ishlash	0,6	0,33	0,5 (0,9)
	TH17	Obyektlarga ruxsatsiz kirish	0,4	0,22	0,2 (0,4)
	TH18	Qurilmalardan ruxsatsiz foydalanish	0,4	0,29	0,3 (0,6)
	TH19	Qurilmalardan noto‘g‘ri foydalanish	0,6	0,18	0,3 (0,6)
	TH20	Qurilmalar yoki ma’lumot tashuvchilarni shikastlash	0,4	0,61	0,7 (1,2)
	TH21	Soxta dasturiy ta’minotni nusxalash	0,5	0,4	0,6 (1)
	TH22	Qalbaki yoki nusxalangan dasturiy ta’minotdan foydalanish	0,4	0,51	0,6 (1)
	TH23	Ma’lumotlarga shikast yetkazish	0,5	0,42	0,6 (1)
	TH24	Noqonuniy ma’lumotlarni qayta ishlash	0,4	0,5	0,6 (1)
	TH25	Zararli dasturlarni yuborish yoki tarqatish	0,6	0,42	0,7 (1,2)
	TH26	Joylashuvni aniqlash	0,2	0,27	0,1 (0,3)
Xizmatlar yoki funksiyalarni buzish	TC01	Foydalanishda xatoliklar	0,5	0,55	0,9 (1,5)
	TC02	Huquqlar yoki ruxsatlarni suiiste’mol qilish	0,6	0,36	0,7 (1,2)
	TC03	Huquqlar yoki ruxsatlarni soxtalashtirish	0,5	0,42	0,6 (1)
	TC04	Harakatlarni rad etish	0,7	0,6	1,3 (2,1)
Tashkiliy tahdidlar	TO01	Xodimlarning etishmasligi	0,5	0,3	0,4 (0,7)
	TO02	Resurslarning etishmasligi	0,6	0,41	0,7 (1,2)
	TO03	Xizmat ko‘rsatuvchining to‘lovga layoqatsizligi	0,4	0,52	0,6 (1)
	TO04	Qonunchilik yoki normativ-huquqiy hujjatlarning buzilishi	0,6	0,37	0,7 (1,2)

Tahdid turlari	Tahdid turlari	Tahdidning nomlanishi	Tahdidning sodir bo‘lish ehtimolligi	Tashkiliy-texnik tadbirlarning bajarilganlik holati	Salbiy oqibat yuzaga kelish riski
Saqlash tizimlari va infratuzilmasiga tahdidlar	TD01	Ruxsat etilmagan foydalanish	0,6	0,33	0,5 (0,9)
	TD02	Ruxsatsiz kirish	0,4	0,22	0,2 (0,4)
	TD03	Qonunlar va me’yoriy hujjatlarga rioya qilmaslik uchun yuridik javobgarlik	0,6	0,37	0,7 (1,2)
	TD04	Saqlash tizimlariga DoS va DDoS hujumlar	0.4	-	-
	TD05	Ma’lumotlarga zarar etkazish, o‘zgartirish va yo‘q qilish	0,6	0,4	0.7 (1.2)
	TD06	Ma’lumotlar sizib chiqishi	0,6	0,5	0,9 (1,5)
	TD07	Axborot tashuvchi yoki saqlovchi vositani o‘g‘irlash yoki tasodifiy yo‘qotish	0,4	0,61	0,7 (1,2)
	TD08	Zararli dastur hujumi yoki inyeksiyasi	0,6	0,42	0,7 (1,2)
	TD09	Noto‘g‘ri ishlov berish yoki foydalanish tugagandan keyin utilizatsiya qilish	0,4	0,6	0,7 (1,2)

6-jadval. Axborot aktivlariga nisbatan salbiy oqibat yuzaga kelish riski tahlili

Tahdid turlari	Tahdidning nomlanishi	hemis.buxdu.uz	masofaviy.buxdu.uz	uniwork.buxdu.uz	moodle.buxdu.uz	student.buxdu.uz	buxdu.uz	Korporativ elektron pochta	Journal.buxdu.uz	Universitet fayl serveri	IP telefoniya	Ishchi stansiyalar	Server uskunalari	Kirish chiqishni nazorat qilish tizimi	Videokuzatuv tizimi
Jismoniy tahdidlar	Yong‘in	0,2 (0,3)	0,2 (0,3)	0,2 (0,3)	0,2 (0,3)	0,3 (0,3)	0,1 (0,1)	0,2 (0,3)	0,1 (0,1)	0,2 (0,2)	0,3 (0,3)	0,1 (0,3)	0,2 (0,2)	0,1 (0,3)	0,1 (0,3)
	Suv toshishi	0,2 (0,3)	0,2 (0,3)	0,2 (0,3)	0,2 (0,3)	0,3 (0,3)	0,1 (0,1)	0,2 (0,3)	0,1 (0,1)	0,4 (0,4)	0,4 (0,4)	0,1 (0,3)	0,2 (0,2)	0,1 (0,3)	0,1 (0,3)
	Ifloslanish, zararli radiatsiya	0,3 (0,4)	0,3 (0,4)	0,3 (0,4)	0,3 (0,4)	0,6 (0,6)	0,1 (0,2)	0,4 (0,5)	0,1 (0,2)	0,3 (0,3)	1,8 (1,8)	0,3 (0,4)	0,4 (0,4)	0,3 (0,4)	0,3 (0,4)
	Katta baxtsiz hodisa	0,3 (0,4)	0,3 (0,4)	0,3 (0,4)	0,4 (0,5)	0,4 (0,4)	0,1 (0,2)	0,4 (0,5)	0,1 (0,2)	0,5 (0,5)	0,4 (0,4)	0,3 (0,4)	0,4 (0,4)	0,3 (0,4)	0,3 (0,4)
	Portlash, halokat	0,2 (0,2)	0,2 (0,2)	0,2 (0,2)	0,2 (0,2)	0,3 (0,3)	0,1 (0,1)	0,1 (0,2)	0,1 (0,1)	0,2 (0,2)	0,3 (0,3)	0,1 (0,2)	0,2 (0,2)	0,1 (0,2)	0,1 (0,2)
	Chang, korroziya, muzlash	0,1 (0,1)	0,1 (0,1)	0,1 (0,1)	0,1 (0,2)	0,1 (0,1)	0 (0,1)	0,1 (0,2)	0 (0,1)	0,1 (0,1)	0,14 (0,14)	0,1 (0,2)	0,2 (0,2)	0,1 (0,2)	0,1 (0,2)
Tabiiy	Iqlim hodisasi	0,3	0,3	0,3	0,4	0,3	0,1	0,2	0,1	0,4	0,6	0,2	0,5	0,2	0,2

Tahdid turlari	Tahdidning nomlanishi	hemis.buxdu.uz	masofaviy.buxdu.uz	uniwork.buxdu.uz	moodle.buxdu.uz	student.buxdu.uz	buxdu.uz	Korporativ elektron pochta	Journal.buxdu.uz	Universitet fayl serveri	IP telefoniya	Ishchi stansiyalar	Server uskunalari	Kirish chiqishni nazorat qilish tizimi	Videokuzatuv tizimi
tahdidlar		(0,4)	(0,4)	(0,4)	(0,5)	(0,3)	(0,2)	(0,3)	(0,2)	(0,4)	(0,6)	(0,4)	(0,5)	(0,4)	(0,4)
	Seysmik hodisa	0,4 (0,5)	0,4 (0,5)	0,4 (0,5)	0,4 (0,5)	2,3 (2,3)	0,2 (0,3)	0,5 (0,6)	0,2 (0,3)	0,4 (0,4)	0,6 (0,6)	0,3 (0,6)	0,7 (0,7)	0,3 (0,6)	0,3 (0,6)
	Vulqon hodisasi	0 (0)	0 (0)	0 (0)	0 (0)	0	0 (0)	0 (0)	0 (0)	0 (0)	0	0 (0)	0 (0)	0 (0)	0 (0)
	Meteorologik hodisa	0,3 (0,4)	0,3 (0,4)	0,3 (0,4)	0,3 (0,4)	0,2 (0,2)	0,1 (0,2)	0,4 (0,5)	0,1 (0,2)	0,3 (0,3)	0,21 (0,21)	0,1 (0,3)	0,4 (0,4)	0,1 (0,3)	0,1 (0,3)
	Suv toshqini	0,4 (0,5)	0,4 (0,5)	0,4 (0,5)	0,4 (0,5)	0,2 (0,2)	0,1 (0,2)	0,2 (0,3)	0,1 (0,2)	0,3 (0,3)	0,28 (0,28)	0,2 (0,4)	0,3 (0,3)	0,2 (0,4)	0,2 (0,4)
	Pandemiya/epidemiya hodisasi	0,4 (0,5)	0,4 (0,5)	0,4 (0,5)	1 (1,3)	0,2 (0,2)	0,2 (0,3)	0,5 (0,6)	0,2 (0,3)	0,4 (0,4)	0,28 (0,28)	0,3 (0,6)	0,6 (0,6)	0,3 (0,6)	0,3 (0,6)
Infratuzil maning ishlamay qolishi	Ta’minot tizimining ishdan chiqishi	1,1 (1,4)	1,1 (1,4)	1,1 (1,4)	1,2 (1,5)	0,8 (0,8)	0,5 (1,1)	1,5 (1.8)	0,5 (1,1)	1,5 (1,5)	1,3 (1,3)	0,9 (1,5)	1 (1)	0,9 (1,5)	0,9 (1,5)
	Sovutish yoki shamollatish tizimining ishlamay qolishi	0,9 (1,3)	0,9 (1,3)	0,9 (1,3)	1,5 (1,9)	1,5 (1,5)	0,6 (1,1)	1,5 (1,7)	0,6 (1,1)	1,1 (1,1)	1,5 (1,5)	1,1 (1,7)	2,8 (2,8)	1,1 (1,7)	1,1 (1,7)
	Energiya ta’minotining buzilishi	1,1 (1,5)	1,1 (1,5)	1,1 (1,5)	1,3 (1,7)	1,9 (1,9)	0,7 (1,2)	1,9 (2,2)	0,7 (1,2)	1,8 (1,8)	1,5 (1,5)	0,8 (1,4)	2,2 (2,2)	0,8 (1,4)	0,8 (1,4)
	Telekommunikatsiya tarmog‘ining ishdan chiqishi	1,8 (2,4)	1,8 (2,4)	1,8 (2,4)	2,6 (3,3)	2,3 (2,3)	0,8 (1,5)	2,2 (2,5)	0,8 (1,5)	2,6 (2,6)	1,7 (1,7)	0,9 (1,6)	1,7 (1,7)	0,9 (1,6)	0,9 (1,6)
	Telekommunikatsiya uskunalari ishlamay qolishi	1,6 (2,1)	1,6 (2,1)	1,6 (2,1)	1,5 (2)	1,7 (1,7)	1 (1,6)	2,2 (2,5)	1 (1,6)	1,7 (1,7)	1,7 (1,7)	0,9 (1,6)	1,9 (1,9)	0,9 (1,6)	0,9 (1,6)
	Elektromagnit nurlanish	0,2 (0,3)	0,2 (0,3)	0,2 (0,3)	0,3 (0,4)	0,3 (0,3)	0,1 (0,2)	0,2 (0,3)	0,1 (0,2)	0,3 (0,3)	0,8 (0,8)	0,4 (0,6)	-	0,4 (0,6)	0,4 (0,6)
	Termal nurlanish	0,2 (0,3)	0,2 (0,3)	0,2 (0,3)	0,3 (0,4)	0,3 (0,3)	0,1 (0,2)	0,2 (0,3)	0,1 (0,2)	0,3 (0,3)	0,3(0, 3)	0,6 (1)	-	0,6 (1)	0,6 (1)
	Elektromagnit impulslar	0,2 (0,3)	0,2 (0,3)	0,2 (0,3)	0,3 (0,4)	0,3 (0,3)	0,1 (0,2)	0,2 (0,3)	0,1 (0,2)	0,3 (0,3)	0,8 (0,8)	0,3 (0,6)	-	0,3 (0,6)	0,3 (0,6)
Texnik muvaffaqi yatsizlik	Qurilma yoki tizimning ishdan chiqishi	1,7 (2,2)	1,7 (2,2)	1,7 (2,2)	1,7 (2,2)	1,9 (1,9)	0,9 (1,5)	2,4 (2,8)	0,9 (1,5)	2.2 (2,2)	2,1 (2,1)	1,3 (2,1)	1,8 (1,8)	1,3 (2,1)	1,3 (2,1)
	Axborot tizimining to‘yinganligi	0,8 (1,1)	0,8 (1,1)	0,8 (1,1)	1 (1,2)	1,4 (1,4)	0,5 (0,8)	1,4 (1,6)	0,5 (0,8)	1,5 (1,5)	1,4 (1,4)	0,6 (1)	-	0,6 (1)	0,6 (1)

Tahdid turlari	Tahdidning nomlanishi	hemis.buxdu.uz	masofaviy.buxdu.uz	uniwork.buxdu.uz	moodle.buxdu.uz	student.buxdu.uz	buxdu.uz	Korporativ elektron pochta	Journal.buxdu.uz	Universitet fayl serveri	IP telefoniya	Ishchi stansiyalar	Server uskunalari	Kirish chiqishni nazorat qilish tizimi	Videokuzatuv tizimi
	Axborot tizimini ta’mirlash qobiliyatini buzilishi	0,9 (1,2)	0,9 (1,2)	0,9 (1,2)	0,9 (1,2)	1,1 (1,1)	0,4 (0,7)	1,1 (1,3)	0,4 (0,7)	1,1 (1,1)	1,2 (1,2)	0,5 (0,8)	0,9 (0,9)	0,5 (0,8)	0,5 (0,8)
Xodimlar harakati	Terrorizm, hujumlar, sabotaj	0,4 (0,5)	0,4 (0,5)	0,4 (0,5)	0,5 (0,6)	0,6 (0,6)	0,3 (0,5)	0,5 (0,6)	0,3 (0,5)	0,3 (0,3)	0,7 (0,7)	0,2 (0,4)	0,5 (0,5)	0,2 (0,4)	0,2 (0,4)
	Ijtimoiy muhandislik	0,4 (0,5)	0,4 (0,5)	0,4 (0,5)	0,3 (0,4)	0,5 (0,5)	0,3 (0,4)	0,4 (0,6)	0,3 (0,4)	0,3 (0,3)	0,4 (0,4)	0,2 (0,4)	0,4 (0,4)	0,2 (0,4)	0,2 (0,4)
	Qurilmaning nurlanishini ushlab turish	1,2 (1,6)	1,2 (1,6)	1,2 (1,6)	1,4 (1,8)	1,4 (1,4)	0,8 (1,3)	1,4 (1,6)	0,8 (1,3)	1,1 (1,1)	1,4 (1,4)	0,7 (1,2)	1,3 (1,3)	0,7 (1,2)	0,7 (1,2)
	Masofaviy monitoring	0,5 (0,7)	0,5 (0,7)	0,5 (0,7)	0,6 (0,7)	0,6 (0,6)	0,2 (0,4)	0,5 (0,6)	0,2 (0,4)	0,6 (0,6)	0,6 (0,6)	0.2 (0.4)	0,7 (0,7)	0.2 (0.4)	0.2 (0.4)
	Tinglash	1 (1,3)	1 (1,3)	1 (1,3)	1,1 (1,4)	1,3 (1,3)	0,5 (0,8)	1,2 (1,4)	0,5 (0,8)	1,1 (1,1)	1,3 (1,3)	0.5 (0.9)	0,8 (0,8)	0.5 (0.9)	0.5 (0.9)
	Ma’lumotlarni tashuvchi vositalarni yoki hujjatlarni o‘g‘irlash	1,1 (1,4)	1,1 (1,4)	1,1 (1,4)	1,4 (1,8)	1,3 (1,3)	0,5 (0,9)	1,6 (1,9)	0,5 (0,9)	1,3 (1,3)	1,3 (1,3)	0.7 (1.2)	1,4 (1,4)	0.7 (1.2)	0.7 (1.2)
	Uskunani o‘g‘irlash	0,8 (1,1)	0,8 (1,1)	0,8 (1,1)	0,8 (1,1)	0,8 (0,8)	0,8 (1,1)	1,1 (1,2)	0,8 (1,1)	0,9 (0,9)	0,8 (0,8)	0.4 (0.8)	1 (1)	0.4 (0.8)	0.4 (0.8)
	Raqamli identifikatorni yoki identifikatsiya ma’lumotlarini o‘g‘irlash	0,8 (1,1)	0,8 (1,1)	0,8 (1,1)	1,3 (1,6)	1,1 (1,1)	0,4 (0,7)	1,4 (1,6)	0,4 (0,7)	1,1 (1,1)	1,1 (1,1)	0.6 (1)	1 (1)	0.6 (1)	0.6 (1)
	Tashlab yuborilgan yoki takror ishlatilayotgan ma’lumot tashuvchi qurilmalardan ma’lumot olish	1 (1.4)	1 (1.4)	1 (1.4)	1,2 (1,6)	1,2 (1,2)	0,5 (1)	1,1 (1,2)	0,5 (1)	1,2 (1,2)	1,2 (1,2)	0.7 (1.2)	1,6 (1,6)	0.7 (1.2)	0.7 (1.2)
	Axborotni oshkor qilish	1,6 (2,2)	1,6 (2,2)	1,6 (2,2)	2 (2,5)	2,1 (2,1)	0,9 (1,5)	2,5 (2,8)	0,9 (1,5)	1,9 (1,9)	1,7 (1,7)	0,9 (1,5)	2,3 (2,3)	0,9 (1,5)	0,9 (1,5)
	Ishonchsiz manbalardan ma’lumotlarni kiritish	1,6 (2,1)	1,6 (2,1)	1,6 (2,1)	1,8 (2,3)	1,6 (1,6)	0,7 (1,2	1,7 (2)	0,7 (1,2	1,6 (1,6)	1,8 (1,8)	0 (0	1,7 (1,7)	0 (0	0 (0
	Uskunani buzish	0,7 (0,9)	0,7 (0,9)	0,7 (0,9)	0,8 (1)	0,9 (0,9)	0,4 (0,6)	0,8 (0,9)	0,4 (0,6)	0,9 (0,9)	1,1 (1,1)	0,3 (0,6)	1,1 (1,1)	0,3 (0,6)	0,3 (0,6)
	Dasturiy ta’minotni buzish	0,8 (1)	0,8 (1)	0,8 (1)	1,1 (1,4)	1,2 (1,2)	0,4 (0,8)	1,1 (1,2)	0,4 (0,8)	1 (1)	1,1 (1,1)	0,4 (0,8)	0,8 (0,8)	0,4 (0,8)	0,4 (0,8)
	Veb-aloqa orqali Drive-by ekspluatatsiyasidan foydalanish	1,1 (1,5)	1,1 (1,5)	1,1 (1,5)	1,1 (1,5)	1,3 (1,3)	0,7 (1,2)	1,6 (1,9)	0,7 (1,2)	1,6 (1,6)	1,7 (1,7)	0,7 (1,2)	1,4 (1,4)	0,7 (1,2)	0,7 (1,2)

Tahdid turlari	Tahdidning nomlanishi	hemis.buxdu.uz	masofaviy.buxdu.uz	uniwork.buxdu.uz	moodle.buxdu.uz	student.buxdu.uz	buxdu.uz	Korporativ elektron pochta	Journal.buxdu.uz	Universitet fayl serveri	IP telefoniya	Ishchi stansiyalar	Server uskunalari	Kirish chiqishni nazorat qilish tizimi	Videokuzatuv tizimi
	Takroriy hujum, o‘rtadagi odam hujumi	1 (1,3)	1 (1,3)	1 (1,3)	1,1 (1,4)	1,4 (1,4)	0,5 (0,8)	1,4 (1,6)	0,5 (0,8)	1,2 (1,2)	1,4 (1,4)	0,6 (1)	0,4 (0,4)	0,6 (1)	0,6 (1)
	Shaxsiy ma’lumotlarni ruxsatsiz qayta ishlash	1,1 (1,5)	1,1 (1,5)	1,1 (1,5)	1,3 (1,6)	1,3 (1,3)	0,8 (1,3)	1,6 (1,9)	0,8 (1,3)	1,8 (1,8)	1,3(1, 3)	0,5 (0,9)	1,6 (1,6)	0,5 (0,9)	0,5 (0,9)
	Obyektlarga ruxsatsiz kirish	0,6 (0,7)	0,6 (0,7)	0,6 (0,7)	0,4 (0,5)	0,6 (0,6)	0,2 (0,4)	0,5 (0,6)	0,2 (0,4)	0,5 (0,5)	0,6 (0,6)	0,2 (0,4)	0,6 (0,6)	0,2 (0,4)	0,2 (0,4)
	Qurilmalardan ruxsatsiz foydalanish	0,6 (0,8)	0,6 (0,8)	0,6 (0,8)	0,7 (0,9)	0,8 (0,8)	0,3 (0,5)	0,8 (0,9)	0,3 (0,5)	0,7 (0,7)	0,8 (0,8)	0,3 (0,6)	0,8 (0,8)	0,3 (0,6)	0,3 (0,6)
	Qurilmalardan noto‘g‘ri foydalanish	0,7 (1)	0,7 (1)	0,7 (1)	0,8 (1,1)	0,8 (0,8)	0,8 (1,3)	0,8 (0,9)	0,8 (1,3)	1,7 (1,7)	0,8 (0,8)	0,3 (0,6)	-	0,3 (0,6)	0,3 (0,6)
	Qurilmalar yoki ma’lumot tashuvchilarni shikastlash	1 (1,4)	1 (1,4)	1 (1,4)	1,2 (1,5)	1.2 (1,2)	0,6 (1,1)	1,6 (1,9)	0,6 (1,1)	1,4 (1,4)	1,7 (1,7)	0,7 (1,2)	-	0,7 (1,2)	0,7 (1,2)
	Soxta dasturiy ta’minotni nusxalash	1,2 (1,6)	1,2 (1,6)	1,2 (1,6)	1,3 (1,6)	1,4 (1,4)	0,5 (0,8)	1,6 (1,9)	0,5 (0,8)	1 (1)	1,4 (1,4)	0,6 (1)	0,7 (0,7)	0,6 (1)	0,6 (1)
	Qalbaki yoki nusxalangan dasturiy ta’minotdan foydalanish	0,9 (1,2)	0,9 (1,2)	0,9 (1,2)	1,2 (1,5)	0,3 (0,3)	0,6 (1)	1,4 (1,6)	0,6 (1)	1,5 (1,5)	1,1 (1,1)	0,6 (1)	0,3 (0,3)	0,6 (1)	0,6 (1)
	Ma’lumotlarga shikast yetkazish	1 (1,3)	1 (1,3)	1 (1,3)	1,1 (1,4)	0,3 (0,3)	1 (1,3)	1,4 (1,6)	1 (1,3)	1,1 (1,1)	1,4 (1,4)	0,6 (1)	1,1 (1,1)	0,6 (1)	0,6 (1)
	Noqonuniy ma’lumotlarni qayta ishlash	1,1 (1,4)	1,1 (1,4)	1,1 (1,4)	1,2 (1,6)	0,6 (0,6)	0.6 (1)	1,1 (1,3)	0.6 (1)	1,2 (1,2)	1,1 (1,1)	0,6 (1)	1,5 (1,5)	0,6 (1)	0,6 (1)
	Zararli dasturlarni yuborish yoki tarqatish	1,1 (1,5)	1,1 (1,5)	2 (2,3)	2,4 (2,8)	0,4 (0,4)	0.7 (1,2)	1,9 (1,9)	0.7 (1,2)	1,7 (1,7)	0,7 (1,2)	1,9 (2,1)	-	0,7 (1,2)	0,7 (1,2)
	Joylashuvni aniqlash	0,3 (0,4)	0,3 (0,4)	0,3 (0,4)	0,3 (0,4)	0,3 (0,3)	0,1 (0,2)	0,4 (0,5)	0,1 (0,2)	0,4 (0,4)	0,7 (0,7)	0,1 (0,3)	0,5 (0,5)	0,1 (0,3)	0,1 (0,3)
Xizmatlar yoki funksiyal arni buzish	Foydalanishda xatoliklar	1,2 (1,6)	1,2 (1,6)	1,2 (1,6)	1,4 (1,8)	0,1 (0,1)	1,2 (1,6)	1,6 (1,9)	1,2 (1,6)	1,6 (1,6)	1,4 (1,4)	0,9 (1,5)	0,8 (0,8)	0,9 (1,5)	0,9 (1,5)
	Huquqlar yoki ruxsatlarni suiiste’mol qilish	0,9 (1,2)	0,9 (1,2)	0,9 (1,2)	1,4 (1,8)	0,3 (0,3)	0,6 (1)	1,2 (1,4)	0,6 (1)	1,8 (1,8)	1,3 (1,3)	0,7 (1,2)	0,7 (0,7)	0,7 (1,2)	0,7 (1,2)
	Huquqlar yoki ruxsatlarni soxtalashtirish	0,8 (1,1)	0,8 (1,1)	0,8 (1,1)	1,3 (1,7)	2,3 (2,3)	0,6 (0.9)	1,6 (1,9)	0,6 (0.9)	1,1 (1,1)	1,1 (1,1)	0,6 (1)	1 (1)	0,6 (1)	0,6 (1)
	Harakatlarni rad etish	1,6	1,6	1,6	1,6	0	0,7	2	0,7	2 (2)	1,9	1,3	1,7	1,3	1,3

Tahdid turlari	Tahdidning nomlanishi	hemis.buxdu.uz	masofaviy.buxdu.uz	uniwork.buxdu.uz	moodle.buxdu.uz	student.buxdu.uz	buxdu.uz	Korporativ elektron pochta	Journal.buxdu.uz	Universitet fayl serveri	IP telefoniya	Ishchi stansiyalar	Server uskunalari	Kirish chiqishni nazorat qilish tizimi	Videokuzatuv tizimi
		(2,1)	(2,1)	(2,1)	(2)		(1,1)	(2,3)	(1,1)		(1,9)	(2,1)	(1,7)	(2,1)	(2,1)
Tashkiliy tahdidlar	Xodimlarning etishmasligi	1,1 (1,5)	1,1 (1,5)	1,1 (1,5)	1,3 (1,7)	0,2 (0,2)	0,4 (0,7)	1,6 (1,9)	0,4 (0,7)	1,2 (1,2)	1,1(1, 1)	0,4 (0,7)	0,8 (0,8)	0,4 (0,7)	0,4 (0,7)
	Resurslarning etishmasligi	1,3 (1,6)	1,3 (1,6)	1,3 (1,6)	1,4 (118)	0,2 (0,2)	0,6 (1)	1,2 (1,4)	0,6 (1)	1,4 (1,4)	1,7(1, 7)	0,7 (1,2)	1,9 (1,9)	0,7 (1,2)	0,7 (1,2)
	Xizmat ko‘rsatuvchining to‘lovga layoqatsizligi	0,9 (1,2)	0,9 (1,2)	0,9 (1,2)	1 (1,3)	0,2 (0,2)	0,4 (0,7)	0,8 (0,9)	0,4 (0,7)	1 (1)	1,1 (1,1)	0,6 (1)	0,6 (0,6)	0,6 (1)	0,6 (1)
	Qonunchilik yoki normativ-huquqiy hujjatlarning buzilishi	1,4 (1,9)	1,4 (1,9)	1,4 (1,9)	1,7 (2,2)	0,8 (0,8)	0,7 (1,2)	1,6 (1,9)	0,7 (1,2)	1,7 (1,7)	1,7 (1,7)	0,7 (1,2)	1,2 (1,2)	0,7 (1,2)	0,7 (1,2)
Saqlash tizimlari va infratuzil-masiga tahdidlar	Ruxsat etilmagan foydalanish	1,1 (1,5)	0,8 (1,3)	1,8 (1,8)	1,3 (1,3)	1,5 (1,5)	1,6 (1,9)	1,3 (1,6)	1,6 (1,9)	1,3 (1,4)	0,5 (0,9)	1,1 (1,5)	2 (2)	1,1 (1,5)	1,1 (1,5)
	Ruxsatsiz kirish	0,6 (0,7)	0,2 (0,4)	0,5 (0,5)	0,6 (0,6)	1,9 (1,9)	0,5 (0,6)	0,4 (0,5)	0,5 (0,6)	0,4 (0,4)	0,2 (0,4)	0,6 (0,7)	0,2 (0,4)	0,6 (0,7)	0,6 (0,7)
	Qonunlar va me’yoriy hujjatlarga rioya qilmaslik uchun yuridik javobgarlik	1,4 (1,9)	0,7 (1,2)	1,7 (1,7)	1,7 (1,7)	2,3 (2,3)	1,6 (1,9)	1,7 (2,2)	1,6 (1,9)	1,7 (1,9)	0,7 (1,2)	1,4 (1,9)	0,7 (1,2)	1,4 (1,9)	1,4 (1,9)
	Saqlash tizimlariga DoS va DDoS hujumlar	-	1,26 (2,1)	-	-	1,7 (1,7)	1,5 (1,7)	-	1,5 (1,7)	-	-	-	1,26 (2,1)	-	-
	Ma’lumotlarga zarar etkazish, o‘zgartirish va yo‘q qilish	1,1 (1,4)	0,5 (0,9)	1,3 (1,3)	1,3 (1,3)	0,3 (0,3)	1,6 (1,9)	1,4 (1,8)	1,6 (1,9)	1,4 (1,6)	0.7 (1.2)	1,1 (1,4)	0,5 (0,9)	1,1 (1,4)	1,1 (1,4)
	Ma’lumotlar sizib chiqishi	1,6 (2,2)	0,9 (1,5)	2,5 (2,8)	-	0,3 (0,3)	1,9 (1,9)	2 (2,5)	1,9 (1,9)	2 (2,3)	0,9 (1,5)	1,6 (2,2)	0,9 (1,5)	1,6 (2,2)	1,6 (2,2)
	Axborot tashuvchi yoki saqlovchi vositani o‘g‘irlash yoki tasodifiy yo‘qotish	1 (1,4)	0,6 (1,1)	1,4 (1,4)	1.2 (1,2)	0,3 (0,3)	1,6 (1,9)	1,2 (1,5)	1,6 (1,9)	1,2 (1,3)	0,7 (1,2)	1 (1,4)	0,6 (1,1)	1 (1,4)	1 (1,4)
	Zararli dastur hujumi yoki inyeksiyasi	1,1 (1,5)	0.7 (1,2)	1,7 (1,7)	1,4 (1,4)	1,9 (1,9)	1,6 (1,9)	1,4 (1,8)	1,6 (1,9)	1,4 (1,6)	0,7 (1,2)	1,1 (1,5)	0.7 (1,2)	1,1 (1,5)	1,1 (1,5)
	Noto‘g‘ri ishlov berish yoki foydalanish tugagandan keyin utilizatsiya qilish	1 (1.4)	0,5 (1)	1,2 (1,2)	1,2 (1,2)	1,4 (1,4)	1,1 (1,2)	1,2 (1,6)	1,1 (1,2)	1,2 (1,4)	0,7 (1,2)	1 (1.4)	0,5 (1)	1 (1.4)	1 (1.4)

7-jadval: Axborot xavfsizligi riskini baholash natijalari

Tahdidning nomlanishi	Riskning bahosi	Himoya obyektlari	Rejalashtirilgan chora-tadbirlar	Qolgan risk
Sovutish yoki shamollatish tizimining ishlamay qolishi	2,8 (2,8)	Server uskunalari	1. Server xonasida zaxira sovutish tizimi 2.Server xonasida ventilyatsiya tizimini tashkil qilish	0,8(0,8)
Energiya ta’minotining buzilishi	2,2 (2,2)	Server uskunalari	1.Binoga zaxira quvvat liniyasini yetkazib berish 2. Dizel generatorini tashkil etish 3.Server uskunalari uchun zaxira UPSni tashkil qilish	0,6(0,7)
Telekommunikatsiya tarmog‘ining ishdan chiqishi	2,6 (2,6)	moodle.buxdu.uz	1.Kabel ulanishlarining sifatini tekshirish 2.Asosiy telekommunikatsiya uskunalarini bron qilish 3.Tarmoq boshqaruvini yaxshilash 4.Tashqi tarmoqqa zaxiraviy ulanishni tashkil etish 5. Telekommunikatsiya uskunalari va aloqa liniyalarining ishlashi monitoringini ta’minlash 6.Rejani joriy etish va telekommunikatsiya vositalarining oldini olishni ta’minlash	0,6 (0,6)
	2,2 (2,5)	student.buxdu.uz		0,6 (0,7)
	2,3 (2,3)	Korporativ elektron pochta		0,6 (0,8)
	2,6 (3,3)	Fayl server		0,6 (0,8)
Telekommunikatsiya uskunalari ishlamay qolishi	2,2 (2,5)	Korporativ elektron pochta	1.Rejani joriy etish va telekommunikatsiya vositalarining oldini olishni ta’minlash 2. Telekommunikatsiya uskunalarini vaqti-vaqti bilan almashtirish uchun yetarli bo‘lmagan jadvalni ta’minlash 3.Tashqi tarmoqqa zaxiraviy ulanishni tashkil qilish 4.Asosiy telekommunikatsiya uskunalarini bron qilish	0,9 (0,9)
Qurilma yoki tizimning ishdan chiqishi	2.2 (2,2)	fayl server	1. Telekommunikatsiya uskunalari zaxirasi 2.Serverlarni zaxiralash	0,5 (0,5)
	2,4 (2,8)	Korporativ elektron pochta		0,9 (0,9)
	2,1 (2,1)	IP telefoniya		0,8 (0,8)
Axborotni oshkor qilish	2,5 (2,8)	moodle.buxdu.uz	1. Matritsa bo‘yicha foydalanuvchining tizimga kirishini nazorat qilish 2.Xodimlarning xabardorligini oshirish 3. Tizimlarda foydalanuvchi faolligini kuzatish 4. Hujjatlarni nazorat qilish 5. Xodimlarning talablarga muvofiqligini nazorat qilish 6. Xodimlarning konfidensial ma’lumotlar bilan ishlash tartib-qoidalariga rioya qilishini nazorat qilish	1 (1)
	2 (2,5)	student.buxdu.uz		1 (1,2)
	2.3	Korporativ elektron pochta		0,8 (0,8)
	2,5 (2,8)	Server uskunalari		0,8 (0,9)

Tahdidning nomlanishi	Riskning bahosi	Himoya obyektlari	Rejalashtirilgan chora-tadbirlar	Qolgan risk
			7.Kadrlar bilan tuzilgan shartnomalarda javobgarlik darajasini oshirish 8. Voqea sodir bo‘lgan taqdirda intizomiy jazo choralarini joriy etish axborot xavfsizligi	
Zararli dasturlarni yuborish yoki tarqatish	2 (2,3)	uniwork.buxdu.uz	1. Litsenziyalangan dasturiy ta’minotdan foydalanish 2. Dasturiy ta’minotga kiritilgan o‘zgarishlarni nazorat qilish 3.Zararli trafikni aniqlash 4.IDPSning samarali qo‘llanilishi 5. Xodimlarning elektron pochta va messenjerlardan foydalanish qoidalariga rioya qilish	1,2 (1,2)
	2,4 (2,8)	moodle.buxdu.uz		1 (1)
	1,9 (1,9)	buxdu.uz		0,5 (0.6)
	1,9 (2,1)	Ishchi stansiyalar		1,1 (1,2)
Harakatlarni rad etish	2 (2)	Fayl server	1.fayl serveriga kirishda foydalanuvchi harakatlarini kiritish monitoring 2. Elektron pochtaga kirishda foydalanuvchi harakatlarining monitoringini kiritish	1 (1)
	2 (2,3)	Korporativ elektron pochta		1,2 (1,4)
Ruxsat etilmagan foydalanish	2 (2)	Server uskunalari	Server xonasiga kirishda signalizatsiya tizimini o‘rnatish	0,8 (1,1)
	1,1 (1,5)	Kirish chiqish nazorat qilish tizimi	Kirish chiqishni nazorat tizimidan foydalanish tartibini buzuvchilar uchun qat’iy tartib o‘rnatish	0,5 (0.6)
	1,1 (1,5)	Videokuzatuv tizimi	Videokuzatuv tizimini faoliyatiga inson omilini aralashishini kamaytirish choralarini ko‘rish	0,5 (0.6)
Ma’lumot sizib chiqishi	2,5 (2,8)	uniwork.buxdu.uz	1. Saqlash tizimlari joylashgan server xonasiga kirishni boshqarishni kuchaytirish 2. Tizim xotiralarida administratorlarni autentifikatsiya qilish darajasini oshirish (parollarni murakkablikni oshirish va o‘zgartirish muddatini qisqartirish) 3. Tizim omborlariga mantiqiy kirish vaqtida xodimlar va administratorlar harakatlarini hisobga olish (log). 4. Administratorlarning axborot tizimlari va serverlariga kirishini boshqarish va nazorat qilish uchun PAM tizimini joriy etish	1,1 (1,2)
	2 (2,5)	buxdu.uz		1 (1,2)
	2,3 (2,3)	Korporativ elektron pochta		0,5 (0.6)
	2 (2,5)	Journal.buxdu.uz		1,1 (1,2)
	2 (2,3)	Fayl server		0,9 (1,2)