ELEKTRON HUJJAT AYLANISHIDA AXBOROT XAVFSIZLIGINI TA’MINLASHNING HUQUQIY VA TEXNOLOGIK ASOSLARI

Davlat boshqaruvi huquqi (70420106)
magistratura yo‘nalishi talabasi

Xalilov Saidakbar Muratovich

Annotatsiya. Mazkur maqolada O’zbekiston Respublikasida elektron hujjat aylanishi tizimlarida axborot xavfsizligini ta’minlashning huquqiy va texnologik mexanizmlari tahlil qilinadi. Milliy qonunchilikdagi asosiy me’yoriy-huquqiy hujjatlar — “Elektron hujjat aylanishi to’g’risida”, “Elektron raqamli imzo to’g’risida”, “Kiberxavfsizlik to’g’risida” hamda “Shaxsga doir ma’lumotlar to’g’risida”gi qonunlar, shuningdek 2026-2030-yillarga mo’ljallangan Kiberxavfsizlik strategiyasini tasdiqlagan Prezident farmonini chuqur o’rganildi. Maqolada xavfsizlik tahdidlari, kriptografik himoya, elektron raqamli imzo infratuzilmasi, shaxsiy ma’lumotlarning himoyasi va muhim axborot infratuzilmasini muhofaza qilish masalalari yoritilgan hamda tizimga amaliy tavsiyalar berilgan.

Kalit so’zlar: elektron hujjat aylanishi, axborot xavfsizligi, elektron raqamli imzo, kiberxavfsizlik, shaxsga doir ma’lumotlar, muhim axborot infratuzilmasi, kriptografik himoya.

Kirish

Raqamli iqtisodiyotning rivojlanishi, "Raqamli O‘zbekiston — 2030" strategiyasining amalga oshirilishi hamda davlat boshqaruvini elektronlashtirish O’zbekiston Respublikasida elektron hujjat aylanishining keng joriy etilishiga olib kelmoqda. Bugungi kunda davlat organlari, xo’jalik yurituvchi subyektlar, bank-moliya sektori va fuqarolar o’rtasidagi rasmiy hujjat almashinuvi asosan elektron kanallar orqali amalga oshirilmoqda. Ushbu o’tish iqtisodiy samaradorlikni oshirish, byurokratiyani qisqartirish va xizmatlarni qulaylashtirish imkonini beradi, biroq ayni paytda yangi, murakkab xavfsizlik tahdidlarini yuzaga keltiradi.

Elektron hujjatning qog’oz hujjatdan tub farqi shundaki, u moddiy tashuvchisi bilan ajralmas emas: elektron hujjat nusxasi asl nusxaga mutlaqo mos keladi, uni oson tahrirlash, nusxalash, ko’chirish mumkin. Shu sabab elektron hujjatning huquqiy kuchini, yaxlitligini va haqqoniyligini ta’minlash uchun kriptografik himoya, elektron raqamli imzo va tashkiliy-texnik choralar majmui zarur bo’ladi. Axborot xavfsizligining uchta asosiy xususiyati — konfidensiallik (maxfiylik), yaxlitlik (integrity) va undan erkin foydalanilishi (availability) — elektron hujjat aylanishining har bir bosqichida qo’llab-quvvatlanishi lozim.

Ushbu maqolaning maqsadi O’zbekiston Respublikasi qonunchiligi doirasida elektron hujjat aylanishida axborot xavfsizligini ta’minlashning huquqiy asoslari va texnologik mexanizmlarini yaxlit tizim sifatida tahlil qilish hamda sohada mavjud muammolarga yechimlar taklif etishdan iborat. Tadqiqot davomida milliy qonunlar, Prezident farmonlari, Vazirlar Mahkamasi qarorlari va vakolatli organlarning me’yoriy hujjatlari o’rganildi.

1. Elektron hujjat aylanishi tizimlariga tahdidlar va xavfsizlik talablari

Elektron hujjat aylanishi qonunchilikda "elektron hujjatlarni yaratish, ularga ishlov berish, jo’natish, qabul qilish, saqlash, ulardan foydalanish va ularni yo’q qilish bilan bog’liq jarayonlar yig’indisi" sifatida ta’riflangan[1]. Bu jarayonning har bir bosqichida elektron hujjatning yaxlitligi hamda unga ruxsatsiz kirishning oldi olinishi ta’minlanishi lozim. Qonunda elektron hujjat deb "elektron shaklda qayd etilgan, uni identifikatsiya qilish imkonini beruvchi rekvizitlarga ega axborot" tushuniladi[2].

Elektron hujjat aylanishi tizimlariga nisbatan tahdidlarni shartli ravishda quyidagi guruhlarga bo’lish mumkin: (1) texnik tahdidlar — zararli dasturlar

[1]O'zbekiston Respublikasining 2004-yil 29-apreldagi 611-II-sonli "Elektron hujjat aylanishi to'g'risida"gi Qonuni (2021-yil 21-apreldagi O'RQ-683-sonli Qonun tahririda). Qonunchilik ma'lumotlari milliy bazasi. URL: https://lex.uz/acts/-165079

[2]O'zbekiston Respublikasining "Elektron hujjat aylanishi to'g'risida"gi Qonunining 5-moddasi. Ushbu moddada elektron hujjatning majburiy rekvizitlari — uni identifikatsiya qilish imkonini beradigan axborot va elektron raqamli imzo belgilangan.

(viruslar, troyanlar, ransomware), DDoS-hujumlar, SQL-injeksiyalar, tarmoq trafigini tutib qolish (man-in-the-middle); (2) tashkiliy tahdidlar — foydalanuvchilarning beparvoligi, ijtimoiy injeneriya, fishing, ruxsat boshqaruvidagi kamchiliklar; (3) ichki tahdidlar — xodimlarning yomon niyatli harakatlari yoki sovuqqonligi natijasida ma’lumotlar sizib chiqishi; (4) huquqiy tahdidlar — elektron hujjatning sud jarayonida isbot sifatida tan olinmasligi xavfi, elektron raqamli imzo kalitlarining noqonuniy ishlatilishi.

Elektron hujjat aylanishini muhofaza qilish chora-tadbirlari ishtirokchilarga yoki boshqa yuridik va jismoniy shaxslarga zarar yetkazilishining oldini olish maqsadida qonunchilikda belgilangan tartibda amalga oshiriladi[3]. Bu norma umumiy xususiyatga ega bo’lib, aniq texnik talablar alohida me’yoriy hujjatlar bilan belgilanadi.

"Axborotlashtirish to’g’risida"gi Qonun[4] axborot resurslari va axborot tizimlarining egalari, mulkdorlari hamda operatorlari zimmasiga ularni muhofaza qilish majburiyatini yuklaydi. Qonunning 19-moddasiga ko’ra, axborot tizimlarining xavfsizligini ta’minlash bo’yicha chora-tadbirlar ularni loyihalash bosqichidan boshlab amalga oshirilishi lozim[5].

Xalqaro tajriba va ISO/IEC 27001 standartiga muvofiq, elektron hujjat aylanishida axborot xavfsizligining quyidagi talablari ajratiladi: konfidensiallik — hujjat faqat vakolatli shaxslar uchun mavjud bo’lishi; yaxlitlik — hujjat mazmuni ruxsatsiz o’zgartirilmasligi; avtentiklik — hujjat manbai va muallifi ishonchli aniqlanishi; inkor etib bo’lmaslik (non-repudiation) — imzolovchi keyinchalik o’z imzosini inkor eta olmasligi; mavjudlik — hujjatdan zarur vaqtda foydalanish

[3]O'zbekiston Respublikasining "Elektron hujjat aylanishi to'g'risida"gi Qonunining 17-moddasi.

[4]O'zbekiston Respublikasining 2003-yil 11-dekabrdagi 560-II-sonli "Axborotlashtirish to'g'risida"gi Qonuni. URL: https://lex.uz/docs/-83472

[5]O'zbekiston Respublikasining "Axborotlashtirish to'g'risida"gi Qonunining 19-moddasi axborot resurslari va axborot tizimlarini himoyalash tartibini belgilaydi.

imkoniyatining saqlanishi; auditlash mumkinligi — barcha harakatlarning izi qolishi va tekshirilishi imkoniyati.

2. Elektron hujjat aylanishida axborot xavfsizligining huquqiy asoslari

O’zbekiston Respublikasida elektron hujjat aylanishi va axborot xavfsizligi sohasidagi qonunchilik bazasi oxirgi yillarda sezilarli darajada kengaytirildi va zamonaviylashtirildi. Bu sohadagi munosabatlar bir necha darajadagi me’yoriy hujjatlar bilan tartibga solinadi: qonunlar, Prezident farmonlari va qarorlari, Vazirlar Mahkamasi qarorlari hamda vakolatli organlarning idoraviy hujjatlari.

Ushbu sohadagi asosiy hujjat — 2004-yil 29-apreldagi 611-II-sonli "Elektron hujjat aylanishi to’g’risida"gi Qonun[6] elektron hujjat tushunchasi, uning huquqiy maqomi, rekvizitlari, aylanish tartibi, saqlash va muhofaza qilish masalalarini belgilaydi. Qonun 2021-yil 21-apreldagi O’RQ-683-sonli Qonun bilan jiddiy tahrirdan o’tkazilgan bo’lib, uning amaldagi tahririda zamonaviy talablar o’z aksini topgan. Qonunning 16-moddasi elektron hujjatlarni qonunchilikda belgilangan tartibda saqlash majburiyatini, 17-moddasi esa ularni muhofaza qilish rejimini nazarda tutadi.

2022-yil 12-oktabrdagi O’RQ-793-sonli "Elektron raqamli imzo to’g’risida"gi Qonun — sohadagi eng muhim hujjatlardan biri. Ushbu Qonun oldingi 2003-yildagi qonunni almashtirgan bo’lib, elektron raqamli imzo (ERI) bilan bog’liq barcha munosabatlarni zamonaviy talablar darajasida qayta tartibga soladi. Qonunga muvofiq, elektron raqamli imzo — elektron hujjatdagi axborotni ERI yopiq kalitidan foydalangan holda maxsus o’zgartirish natijasida hosil qilingan, ochiq kalit yordamida hujjatdagi xatolikning yo’qligini aniqlash va imzo egasini identifikatsiya qilish imkonini beradigan imzodir.

Qonunning muhim xususiyati shundaki, to’g’ri qo’yilgan va haqiqiy sertifikat bilan tasdiqlangan ERI bilan imzolangan elektron hujjat qog’oz hujjatdagi qo’l

qo’yilgan va muhr bosilgan hujjatga teng huquqiy kuchga ega bo’ladi. ERI kalit sertifikatlari faoliyat ko’rsatuvchi ro’yxatga olish markazlari tomonidan beriladi[7], bu esa Public Key Infrastructure (PKI) tamoyillariga asoslanadi.

2022-yil 15-apreldagi O’RQ-764-sonli "Kiberxavfsizlik to’g’risida"gi Qonun— mamlakatda kiberxavfsizlik sohasidagi munosabatlarni tartibga soluvchi birinchi maxsus qonundir. Qonun 8 bob va 40 moddadan iborat bo’lib, asosiy tushunchalar, tamoyillar, davlat siyosati yo’nalishlari, subyektlarning huquq va majburiyatlari hamda mas’ul organlarning vakolatlarini belgilaydi. Qonunga ko’ra, O’zbekiston Respublikasi Davlat xavfsizlik xizmati kiberxavfsizlik sohasidagi vakolatli davlat organi hisoblanadi.

Qonunning 14-moddasi davlat organlari va tashkilotlariga kiberxavfsizlikni ta’minlash majburiyatini yuklaydi: ular vakolatli davlat organidan kibertahdidlar va zaifliklar to’g’risida axborot olish, kiberhujumlar haqida xabar berish, sertifikatlangan dasturiy ta’minotdan foydalanish va sohaga doir hujjatlarni vakolatli organ bilan kelishish majburiyatlariga ega. 15-modda ma’lumotlarning zaxira nusxalarini ko’chirish majburiyatini belgilab, ularning saqlanish muddati oxirgi 3 oydan kam bo’lmasligi shartini ilgari suradi.

19-moddaga muvofiq, axborot tizimlari va resurslarining kiberxavfsizligini ta’minlash uchun qo’llaniladigan apparat, apparat-dasturiy hamda dasturiy vositalar majburiy sertifikatlashtirishdan o’tkaziladi[8]. Bu tartib muhim axborot infratuzilmasini tashqaridan keltirilgan, tasdiqlanmagan vositalar orqali buzg’unchilik qilinishining oldini olishga qaratilgan.

2026-yil 10-martda O’zbekiston Respublikasi Prezidenti tomonidan imzolangan PF-38-sonli Farmon mamlakatning 2026-2030-yillarga mo’ljallangan Kiberxavfsizlik strategiyasini tasdiqladi. Strategiyaning asosiy yo’nalishlari: milliy

[7]"Elektron raqamli imzo to'g'risida"gi Qonunning ro'yxatga olish markazlari faoliyatiga oid moddalari. Ro'yxatga olish markazlari kalit sertifikatlarini beradi va ularning haqiqiyligini ta'minlaydi.

[8]"Kiberxavfsizlik to'g'risida"gi Qonunning 19-moddasi axborot tizimlari va resurslarining kiberxavfsizligini ta'minlash uchun qo'llaniladigan dasturiy va apparat vositalarni sertifikatlashtirish talablarini belgilaydi.

kiberbarqarorlikni mustahkamlash va muhim axborot hamda davlat raqamli infratuzilmasini himoya qilish; kiberxavflarni tizimli ravishda kamaytirish; raqamli innovatsiyalar va sun’iy intellekt texnologiyalari sohasida kiberxavfsizlikni ta’minlash; texnologik mustaqillikka erishish; xalqaro hamkorlikni rivojlantirishdan iboratdir.

Farmonga muvofiq, 2026-yil 1-apreldan Adliya vazirligi, Energetika vazirligi va Soliq qo’mitasida Kiberxavfsizlikni ta’minlash bo’limlari tashkil etildi, shuningdek Prezident huzuridagi Xavfsizlik kengashi kotibi raisligida milliy muvofiqlashtiruvchi kengash tuzildi. Bu institutsional yangiliklar elektron hujjat aylanishi tizimlari himoyasini ham bevosita ta’sir qilib, idoralararo muvofiqlashtirishni kuchaytirishga xizmat qiladi.

3. Axborot xavfsizligini ta’minlashning texnik va tashkiliy mexanizmlari

Huquqiy asoslar belgilab bergan talablar amaliyotda texnik va tashkiliy mexanizmlar yordamida ro’yobga chiqariladi. Elektron hujjat aylanishida axborot xavfsizligini ta’minlashning asosiy vositalarini quyidagicha tasniflash mumkin.

ERI elektron hujjatning yaxlitligi va avtentikligini ta’minlovchi asosiy vosita hisoblanadi. Amaliyotda asimmetrik kriptografiya (RSA, ECDSA va GOST-algoritmlari) qo’llaniladi: imzolovchi hujjatning xesh-qiymatini o’zining yopiq kaliti bilan shifrlaydi, qabul qiluvchi esa imzolovchi ochiq kaliti yordamida uni tekshiradi. Agar hujjat mazmuni o’zgartirilsa, xesh-qiymat ham o’zgaradi va imzo haqiqiyligi buziladi. Shu bois ERI bir vaqtning o’zida uchta vazifani — identifikatsiya, avtentifikatsiya va yaxlitlikni nazorat qilish vazifalarini bajaradi.

Kalit va sertifikatlarni boshqarish — alohida jiddiy vazifadir. Yopiq kalitlar foydalanuvchining shaxsiy qurilmasi (kriptoprovayder, smart-karta, USB-token) yoki ishonchli bulutli muhitda saqlanadi. Kalitning yo’qolishi yoki bo’shashishi darhol sertifikatning bekor qilinishiga olib kelishi kerak, aks holda noqonuniy imzolangan hujjatlar paydo bo’lishi mumkin. Shu sababli ro’yxatga olish markazlari bekor qilingan sertifikatlar ro’yxatini (CRL) yoki Online Certificate Status Protocol (OCSP) xizmatini real vaqt rejimida yuritadilar.

Elektron hujjatlarni saqlashda va uzatishda ma’lumotlar shifrlanadi. Saqlashda odatda simmetrik shifrlash (AES-256) qo’llaniladi, uzatishda esa TLS 1.3 protokoli keng tarqalgan. Davlat organlarining yopiq tarmoqlarida mamlakatda sertifikatlangan kriptografik vositalardan foydalanish talabi amal qiladi. Bu "Kiberxavfsizlik to’g’risida"gi Qonunning 19-moddasida belgilangan sertifikatlash talabi bilan bog’liqdir.

Muhim axborot tizimlari, shu jumladan elektron hujjat aylanishi platformalari foydalanishga topshirilgunga qadar kiberxavfsizlik talablariga muvofiqlik yuzasidan majburiy ekspertizadan o’tkaziladi. Bu jarayonda zaiflikka qarshi test (penetration testing), loyiha hujjatlarini tahlil qilish, xavfsizlik siyosati va tashkiliy choralarni baholash amalga oshiriladi. Ekspertiza natijalari asosida tizimga xavfsizlik sinfi (daraja) beriladi va u xizmatga qo’yilishiga ruxsat olinadi.

Statistik ma’lumotlarga ko’ra, axborot xavfsizligi hodisalarining asosiy qismi texnik emas, balki tashkiliy va inson omili bilan bog’liq. Shu bois tashkilotda quyidagi mexanizmlar joriy etilishi zarur: ichki axborot xavfsizligi siyosati va tartib-qoidalari; foydalanuvchilarga ruxsatlarni minimal zarurat tamoyili asosida berish (least privilege); ikki omilli autentifikatsiya (MFA); muntazam audit va nazorat; xodimlarni ijtimoiy injeneriya va fishingga qarshi o’qitish; hodisalarga javob qaytarish rejasi (Incident Response Plan). Xodimlarning bu sohadagi savodxonligi nafaqat tashkilotning ichki xavfsizligini, balki butun milliy raqamli ekotizimning barqarorligini ta’minlaydi.

4. Shaxsiy ma’lumotlarning himoyasi va muhim axborot infratuzilmasi

Elektron hujjatlar ko’pincha fuqarolarning shaxsga doir ma’lumotlarini o’z ichiga oladi: pasport ma’lumotlari, JSHSHIR, tibbiy va moliyaviy ma’lumotlar va boshqalar. Bunday ma’lumotlarga ishlov berish 2019-yil 2-iyuldagi O’RQ-547-sonli "Shaxsga doir ma’lumotlar to’g’risida"gi Qonun[9] bilan tartibga solinadi. Qonun GDPR ruhiga yaqin bo’lib, subyektning roziligi, maqsadga muvofiqlik,

[9]O'zbekiston Respublikasining 2019-yil 2-iyuldagi O'RQ-547-sonli "Shaxsga doir ma'lumotlar to'g'risida"gi Qonuni. Kuchga kirish sanasi: 2019-yil 1-oktabr. Oxirgi tahrir: 2023-yil 29-noyabr. URL: https://lex.uz/docs/-4396419

ma’lumotlarning minimalligi, aniqlik, saqlash muddati cheklanishi kabi asosiy tamoyillarni o’rnatadi. Subyekt o’z ma’lumotlariga kirish, ularni tuzatish, o’chirish va ishlov berishni cheklash huquqlariga ega.

Qonunning muhim xususiyati — 2021-yil 14-yanvardagi tahrir bilan kiritilgan lokalizatsiya talabi[10]. Unga ko’ra, O’zbekiston Respublikasi fuqarolarining shaxsga doir ma’lumotlari O’zbekiston hududida joylashgan texnik vositalar yordamida jamlanishi, tizimlashtirilishi va saqlanishi lozim. Bu me’yor elektron hujjat aylanishi tizimlarini loyihalashda serverlar va ma’lumotlar bazalarining geografik joylashuvi masalasini birinchi o’ringa qo’yadi. Vazirlar Mahkamasining 2022-yil 5-oktabrdagi 570-sonli qarori va Adliya vazirining 2023-yil 15-noyabrdagi 3477-sonli buyrug’i[11] bu sohada amaliy tartib-qoidalarni belgilab berdi. Xususan, ma’lumotlar bazasining mulkdori yoki operatori zimmasiga ma’lumotlarni himoya qilish uchun mas’ul bo’lgan maxsus tuzilmaviy bo’linma yoki vakolatli shaxs tayinlash (ya’ni Data Protection Officer — DPO — ga teng) majburiyati yuklangan.

Davlat idoralari, bank-moliya tizimi, energetika va transport sohalarining elektron hujjat aylanishi platformalari muhim axborot infratuzilmasi obyektlari qatoriga kiradi. Ular "Kiberxavfsizlik to’g’risida"gi Qonun hamda Kiberxavfsizlik strategiyasida nazarda tutilgan maxsus himoya rejimiga muvofiq ta’minlanadi: zaiflikni aniqlashning uzluksiz monitoringi, SOC (Security Operations Center) orqali 24/7 kuzatish, davriy penetratsion testlar va mustaqil ekspertlar ishtirokida xavfsizlikni baholash. Bunday yondashuv natijasida kibertahdidlarga qarshi tizim proaktiv holatda ishlaydi.

[10]"Shaxsga doir ma'lumotlar to'g'risida"gi Qonunning 27-moddasi (2021-yil 14-yanvardagi O'RQ-666-sonli Qonun bilan kiritilgan 27-1-modda) — shaxsga doir ma'lumotlarni O'zbekiston Respublikasi hududida joylashgan serverlar va ma'lumotlar bazalarida jamlash, tizimlashtirish va saqlash talabi.

[11]O'zbekiston Respublikasi Adliya vazirining 2023-yil 15-noyabrdagi 3477-sonli "Shaxsga doir ma'lumotlar bazasining mulkdori va (yoki) operatorining shaxsga doir ma'lumotlarga ishlov berilishini hamda ularning himoya qilinishini ta'minlovchi tuzilmaviy bo'linmasi yoki vakolatli shaxsi faoliyatini tashkil etishning namunaviy tartibini tasdiqlash haqida"gi buyrug'i. URL: https://lex.uz/docs/-6663969

Elektron hujjat aylanishining huquqiy asoslari shuningdek "Elektron hukumat to'g'risida"gi 2020-yil 15-yanvardagi O'RQ-599-sonli Qonun[12] bilan ham bog'liq, chunki davlat xizmatlari ko'rsatish jarayonida hujjatlar almashinuvi elektron hukumat infratuzilmasi doirasida amalga oshiriladi. ISO/IEC 27001 kabi xalqaro standartlarga moslashtirilgan menejment tizimlari mamlakatda ham tobora keng joriy etilmoqda.

Xulosa

O'tkazilgan tahlil shuni ko'rsatadiki, O'zbekiston Respublikasida elektron hujjat aylanishida axborot xavfsizligini ta'minlashning yetarli darajada mustahkam huquqiy bazasi shakllantirilgan. "Elektron hujjat aylanishi to'g'risida", "Elektron raqamli imzo to'g'risida", "Kiberxavfsizlik to'g'risida" va "Shaxsga doir ma'lumotlar to'g'risida"gi qonunlar yaxlit tizim tashkil qilib, elektron hujjatning yaratilishidan boshlab yo'q qilishgacha bo'lgan barcha bosqichlarini qamrab oladi. 2026-yilda qabul qilingan Kiberxavfsizlik strategiyasi ushbu bazani keyingi besh yilga mo'ljallangan aniq yo'nalish va ustuvorliklar bilan to'ldirdi.

Shu bilan birga, bir qator amaliy muammolar hamon mavjud: soha mutaxassislari yetishmasligi, ba'zi tashkilotlarda xavfsizlik madaniyati yetarli darajada rivojlanmaganligi, ERI infratuzilmasining birlashtirilmaganligi, xalqaro standartlarga moslashtirilish jarayonining yakunlanmaganligi. Bu muammolarni bartaraf etish uchun quyidagi chora-tadbirlarni tavsiya etish mumkin:

birinchidan, tashkilotlarda ma'lumotlarni himoya qilish bo'yicha vakolatli shaxs (DPO) lavozimini yanada kengroq joriy etish va ularning malakasini oshirish dasturlarini ishlab chiqish;

ikkinchidan, elektron hujjat aylanishi platformalarini ISO/IEC 27001 va ISO/IEC 27701 standartlari talablariga muvofiq sertifikatlashtirishni majburiy qilish;

[12]O'zbekiston Respublikasining 2020-yil 15-yanvardagi O'RQ-599-sonli "Elektron hukumat to'g'risida"gi Qonuni. URL: https://lex.uz/docs/-4691520

uchinchidan, barcha davlat organlari uchun yagona, sertifikatlangan elektron hujjat aylanishi platformasini joriy etishni jadallashtirish va mahalliy ishlab chiqaruvchilarni qo’llab-quvvatlash;

to’rtinchidan, foydalanuvchilar uchun kiberxavfsizlik savodxonligi bo’yicha muntazam o’quv dasturlarini amalga oshirish va aholi o’rtasida ogohlik madaniyatini shakllantirish;

beshinchidan, tahdidlar haqidagi axborotni ishonchli almashinuvi uchun milliy CERT (Computer Emergency Response Team) hamda sektoral ISAC (Information Sharing and Analysis Center) tuzilmalarini yanada rivojlantirish.

Zamonaviy tahdidlar — jumladan, sun’iy intellekt asosidagi hujumlar, dipfeyklar va ransomware-epidemiyalar — elektron hujjat aylanishi tizimlarining himoyasini doimiy takomillashtirishni talab etadi. Huquqiy bazaning sohadagi tez o’zgarishlarga moslashuvchan bo’lishi, texnik choralar bilan muvofiqlashtirilishi va xalqaro tajribaga asoslanishi O’zbekiston raqamli iqtisodiyotining ishonchli va barqaror rivojlanishi garovi bo’ladi.

FOYDALANILGAN ADABIYOTLAR RO’YXATI

1. O’zbekiston Respublikasining 2004-yil 29-apreldagi 611-II-sonli "Elektron hujjat aylanishi to’g’risida"gi Qonuni (O’zbekiston Respublikasining 2021-yil 21-apreldagi O’RQ-683-sonli Qonuni tahririda). — URL: https://lex.uz/acts/-165079

2. O’zbekiston Respublikasining 2022-yil 12-oktabrdagi O’RQ-793-sonli "Elektron raqamli imzo to’g’risida"gi Qonuni. — URL: https://lex.uz/docs/-6234904

3. O’zbekiston Respublikasining 2022-yil 15-apreldagi O’RQ-764-sonli "Kiberxavfsizlik to’g’risida"gi Qonuni. — URL: https://lex.uz/docs/-5960604

4. O’zbekiston Respublikasining 2019-yil 2-iyuldagi O’RQ-547-sonli "Shaxsga doir ma’lumotlar to’g’risida"gi Qonuni. — URL: https://lex.uz/docs/-4396419

5. O’zbekiston Respublikasining 2003-yil 11-dekabrdagi 560-II-sonli "Axborotlashtirish to’g’risida"gi Qonuni. — URL: https://lex.uz/docs/-83472

6. O’zbekiston Respublikasining 2020-yil 15-yanvardagi O’RQ-599-sonli "Elektron hukumat to’g’risida"gi Qonuni. — URL: https://lex.uz/docs/-4691520

7. O’zbekiston Respublikasi Prezidentining 2026-yil 10-martdagi PF-38-sonli "O’zbekiston Respublikasining Kiberxavfsizlik strategiyasini belgilash va kiberjinoyatchilikning oldini olish tizimini takomillashtirish to’g’risida"gi Farmoni.

8. O’zbekiston Respublikasi Prezidentining 2022-yil 28-yanvardagi PF-60-sonli "2022-2026-yillarga mo’ljallangan Yangi O’zbekistonning taraqqiyot strategiyasi to’g’risida"gi Farmoni. — URL: https://lex.uz/docs/-5841063

9. O’zbekiston Respublikasi Vazirlar Mahkamasining 2022-yil 5-oktabrdagi 570-sonli "Shaxsga doir ma’lumotlarga ishlov berish sohasidagi ayrim normativ-huquqiy hujjatlarni tasdiqlash to’g’risida"gi qarori.

10. ISO/IEC 27701:2019. Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines. — Geneva: ISO, 2019.

11. Rustambekov I. Elektron hujjat aylanishi tizimlarini joriy etishning huquqiy masalalari // Yuridik fanlar axborotnomasi. — Toshkent, 2020. — 2-son. — B. 45-52.

12. Azizov A. Axborot xavfsizligi va kriptografiya asoslari. — Toshkent: TATU, 2022. — 312 b.

13. Eshonqulov J., Ummatova I. Legal status of electronic signatures in the Republic of Uzbekistan // Central Asian Journal of Multidisciplinary Research and Management Studies. — 2025. — Vol. 6, No. 3. — P. 120-128.