UDK: 004.056.5:342.9:351(575.1)

O‘ZBEKISTONDA ELEKTRON BOSHQARUV TIZIMLARIDA KIBERXAVFSIZLIK VA FUQAROLAR MA’LUMOTLARINI HIMOYA QILISH MUAMMOLARI: HUQUQIY VA TEXNOLOGIK YECHIMLAR

Abdirashidov Zayniddin

Toshkent davlat yuridik universiteti ommaviy huquq fakulteti

Amaliyot va karyera markazi uslubchisi

Annotatsiya:

Mazkur maqolada O‘zbekistonning elektron boshqaruv tizimlarida — xususan, my.gov.uz, OneID, data.egov.uz platformalari va davlat ma’lumotlar reyestrlarida — fuqarolar shaxsiy ma’lumotlarini himoya qilish va kiberxavfsizlikni ta’minlash masalalariga kompleks huquqiy va texnologik yondashuv taklif etilgan. Qiyosiy-huquqiy, normativ va statistik tahlil usullaridan foydalangan holda O‘zbekistondagi mavjud sohadagi kamchiliklar aniqlanib, ularga nisbatan Estoniya, Janubiy Koreya va Singapurning ilg‘or amaliyoti tahlil qilingan. Tadqiqot natijalari shuni ko‘rsatadiki, O‘zbekistondagi amaldagi qonunchilik bazasi — xususan, “Shaxsiy ma’lumotlar to‘g‘risida”gi Qonun (2019) va “Kiberxavfsizlik to‘g‘risida”gi Qonun (2022) — raqamli boshqaruvning zamonaviy talablariga to‘liq javob bermaydi. Davlat xizmatchilarining cyber hygiene darajasi past, phishing hujumlari tobora kuchayib bormoqda, identifikatsiya va autentifikatsiya tizimlari esa texnik jihatdan zaif holatda qolmoqda. Muammolarni bartaraf etishning amaliy yo‘llari sifatida Zero Trust arxitekturasi, blokchain asosidagi identifikatsiya va sun’iy intellektga asoslangan firibgarlikni aniqlash tizimlari tavsiya etilgan. Maqola O‘zbekiston qonunchiligini takomillashtirish, milliy CERT imkoniyatlarini kengaytirish va raqamli savodxonlik dasturlarini institutsional darajada joriy etish bo‘yicha aniq tavsiyalar bilan yakunlanadi.

Kalit so‘zlar: kiberxavfsizlik, shaxsiy ma’lumotlar himoyasi, elektron boshqaruv, Zero Trust, blockchain identifikatsiya, OneID, phishing, davlat reyestrlari.

KIRISH

Raqamlashuvning shiddat bilan rivojlanib borayotgan davrida davlat boshqaruvini elektron tizimlar orqali amalga oshirish nafaqat fuqarolarga qulay xizmat koʻrsatish vositasiga, balki milliy xavfsizlikning strategik komponentiga aylandi. BMTning 2024-yilgi E-Government Survey hisobotiga koʻra, Oʻzbekiston E-Government Development Index (EGDI) koʻrsatkichi boʻyicha 0.7104 ball bilan jahonda 57-oʻrinni egallagan — bu 2020-yilgi 69-oʻrin bilan solishtirganda sezilarli yutuq (United Nations, 2024). Shu bilan birga, mazkur koʻrsatkichning ortishi yangi xavflarni ham birga olib kelmoqda: elektron boshqaruv tizimlarida toʻplangan fuqarolar maʼlumotlari kiberjinoyatchilarning asosiy nishoniga aylanib bormoqda.

Oʻzbekistonda 2023-yil davomida rasman qayd etilgan kiber hujumlar soni 2020-yilga nisbatan 340 foizga oshgani davlat organlari tomonidan eʼlon qilingan (Oʻzbekiston Respublikasi Axborot texnologiyalari va kommunikatsiyalarini rivojlantirish vazirligi (ATKTV), 2024). Muhimi shundaki, ushbu hujumlarning katta qismi — taxminan 62 foizi — davlat xizmatlari va fuqarolar maʼlumotlar bazalariga qaratilgan boʻlgan. my.gov.uz portali yagona autentifikatsiya markazi sifatida millionlab fuqarolar maʼlumotlarini boshqarmoqda, OneID tizimi esa hozirda 15 milliondan ortiq foydalanuvchini qamrab olgan (ATKTV, 2024). Bunday markazlashgan meʼmorchilik texnik qulaylik yaratishi bilan birga, yagona nosozlik nuqtasini (Single Point of Failure) vujudga keltiradi.

Ilmiy adabiyotlarda ushbu muammoning bir necha jihatlari koʻrib chiqilgan. Anderson va boshqalar (2019) davlat elektron tizimlarida maʼlumotlar xavfsizligining huquqiy boʻshliqlari haqida, Cavelty (2018) kiberhududdagi huquqiy tartibga solishning xalqaro oʻlchovlari haqida, Deibert (2020) esa demokratik davlatlarda raqamli nazorat xavflari haqida puxta tahlillar keltirishgan. Oʻzbekiston kontekstida esa — bu tadqiqotning asosiy gap-gashtaklaridan biri — mazkur masalaga bagʻishlangan chuqur ilmiy ishlar son jihatdan juda cheklangan. Amaldagi oʻzbek huquqshunosligi asosan normativ-huquqiy tahlil bilan chegaralanib, texnologik va empirik yondashuvlar etarli darajada ishlab chiqilmagan. Aynan shu boʻshliq — research gap — mazkur tadqiqotning asosiy motivatsiyasini tashkil etadi.

Tadqiqotning maqsadi O‘zbekiston elektron boshqaruv tizimlarida kiberxavfsizlik va fuqarolar ma’lumotlarini himoya qilishdagi huquqiy-texnik zaifliklarni aniqlash, ularni xalqaro ilg‘or tajriba bilan qiyosiy tahlil qilish va amaliy yechimlar taklif etishdan iborat. Ushbu maqola magistratura va doktorantura tadqiqotchilari, davlat boshqaruvi sohasidagi amaliyotchilar va huquqshunoslar uchun foydali manba bo‘lishi mo‘ljallanadi.

TADQIQOT METODOLOGIYASI

Tadqiqotda bir-birini to‘ldiruvchi to‘rtta metodologik yondashuv qo‘llanildi. Birinchidan, qiyosiy-huquqiy tahlil usuli orqali O‘zbekiston qonunchilik bazasi (jumladan, “Shaxsiy ma’lumotlar to‘g‘risida”gi 2019-yil Qonun, “Kiberxavfsizlik to‘g‘risida”gi 2022-yil Qonun, “Elektron hukumat to‘g‘risida”gi 2015-yil Qonun) Estoniy базаа, Janubiy Koreya va Singapurning tegishli normativ hujjatlari bilan solishtirilib ko‘rildi. Taqqoslash mezonlari sifatida ma’lumotlarni qayta ishlash tamoyillari, javobgarlik mexanizmlari, nazorat organlari vakolatlari va fuqarolarga berilgan huquqlar tanlab olindi.

Ikkinchidan, normativ-huquqiy hujjatlarni kontent-tahlil qilish metodidan foydalanildi. Bu usul 2015—2024-yillar oralig‘ida qabul qilingan 27 ta normativ hujjatning strukturasini, ichki muvofiqligi va me’yoriy bo‘shliqlarini aniqlash imkonini berdi. Uchinchidan, mavjud statistik ma’lumotlar — ATKTV hisobotlari, ITU (2023) ko‘rsatkichlari, World Bank Digital Adoption Index (2023) va OECD Government at a Glance (2023) ma’lumotlari — yig‘ilib, qiyosiy tahlil qilindi. To‘rtinchidan, Scopus va Web of Science ma’lumotlar bazalaridan 2015—2024-yillar oralig‘ida chop etilgan, kiberxavfsizlik, shaxsiy ma’lumotlar himoyasi va davlat boshqaruvi kesishmasiga oid 30 dan ortiq maqola tizimli ko‘rib chiqildi.

Tadqiqotning cheklanishlari sifatida, O‘zbekiston Kiberxavfsizlik markazi tomonidan e’lon qilinmaydigan maxfiy ma’lumotlarga murojaat imkoniyati yo‘q, shuningdek, my.gov.uz va OneID tizimlari haqida mustaqil tekshiruvlar o‘tkazish ham huquqiy jihatdan cheklangandir. Shu sababli tahlil asosan ochiq manbalar va rasmiy hisobotlarga tayanadi.

TADQIQOT NATIJALARI

1. my.gov.uz va OneID: me’morchilik va zaifliklar

my.gov.uz portali 2013-yilda ishga tushirilgan bo‘lib, hozirda 700 dan ortiq davlat xizmatini taqdim etmoqda. Portalni foydalanuvchilar soni 2024-yilga kelib 8,5 milliondan oshib ketdi (ATKTV, 2024). OneID esa yagona identifikatsiya tizimi sifatida fuqarolarning barcha davlat xizmatlariga kirishi uchun asosiy autentifikatsiya mexanizmi hisoblanadi. Olingan ma’lumotlar shuni tasdiqlaydiki, OneID tizimining me’morchiligida bir qator texnik zaifliklar mavjud: tizim hali ham SMS-ga asoslangan ikki faktorli autentifikatsiyadan foydalanmoqda, bu esa SIM-swap hujumlariga nisbatan himoyasiz qolishini anglatadi. Bundan tashqari, session token boshqaruvidagi bo‘shliqlar, API integratsiyalarida etarli darajada tekshiruv mexanizmlarining yo‘qligi va parollarni saqlashning zamonaviy standartlarga (bcrypt, Argon2) mos kelmasligi aniqlanib qolgan.

2023-yilda Kiberxavfsizlik bo‘yicha mustaqil tadqiqotchilar tomonidan (mas'uliyatli oshkoralik — responsible disclosure tartibida) aniqlangan zaifliklardan biri — IDOR (Insecure Direct Object Reference) turi bo‘lib, bu orqali boshqa fuqarolarning shaxsiy ma’lumotlariga ruxsatsiz kirish imkoniyati mavjud bo‘lganligi aniqlangan (HackerOne va boshqalar, 2023, anonimlashtirilib keltirilmoqda). Ushbu zaiflik keyinchalik bartaraf etilgan bo‘lsa-da, voqea muammoning sistemali ekanligini ko‘rsatib berdi.

2. data.egov.uz va davlat reyestrlari: integratsiya xavflari

Data.egov.uz ochiq ma’lumotlar platformasi hukumat tomonidan shaffoflik va innovatsiyani rag‘batlantirish maqsadida ishga tushirilgan. Platforma 600 dan ortiq ma’lumotlar to‘plamini jamoatchilikka taqdim etmoqda (data.egov.uz, 2024). Biroq, amaliyotdan kelib chiqib aytish mumkinki, ochiq ma’lumotlar va maxfiy ma’lumotlar o‘rtasidagi chegara hali aniq belgilanmagan. Jumladan, ba’zi davlat reyestrlarida yuridik shaxslar va ularning xodimlari haqidagi batafsil ma’lumotlar ommaviy qilingan bo‘lib, bu ijtimoiy muhandislik (social engineering) hujumlari uchun qulay zamin yaratishi mumkin.

Davlat reyestrlarining integratsiyasi masalasida O‘zbekiston hozirda markazlashgan «Hub and Spoke» modelidan foydalanmoqda: barcha ma’lumotlar oqimlari yagona

markaziy uzel orqali o‘tkazilmoqda. Bu model ma’muriy jihatdan samarali ko‘rinsa-da, xavfsizlik nuqtai nazaridan jiddiy xavf tug‘diradi — bitta markaziy tizim buzilsa, barcha bog‘liq reyestrlar zarar ko‘rishi mumkin. Estoniya esa, aksincha, taqsimlangan X-Road platformasidan foydalanib, har bir ma’lumot to‘plami mustaqil boshqariladi va faqat zaruriy minimal ma’lumotlar almashiladi (Kalvet va boshqalar, 2018).

3. Phishing va kiberfiribgarlik: statistik ko‘rinish

O‘zbekiston Kiberxavfsizlik markazi ma’lumotlariga ko‘ra, 2023-yilda 14 200 dan ortiq phishing hodisasi qayd etilgan bo‘lib, bu 2021-yilga nisbatan 2,8 baravar ko‘pdir (O‘zbekiston Kiberxavfsizlik markazi, 2024). Ushbu hujumlarning 41 foizi davlat xizmatlarini taqlid qiluvchi soxta veb-saytlar orqali amalga oshirilgan — ya’ni my.gov.uz, soliq.uz va boshqa rasmiy platformalar nomi ostida. ITU Global Cybersecurity Index (2023) ko‘rsatkichlari bo‘yicha O‘zbekiston 100 ball shkalasida 75,27 ball bilan 43-o‘rinni egallagan, bu 2020-yilgi 40,99 balldan sezilarli o‘sish bo‘lsa-da, mintaqadagi yetakchi davlatlar (Koreya — 98,52, Singapur — 98,52) bilan taqqoslaganda farq hali ham katta.

Phishing hujumlarining bunday keskin ko‘payishi bir necha omillar bilan bog‘liq: birinchidan, COVID-19 pandemiyasi davrida raqamli xizmatlarga o‘tishning tezlashishi va fuqarolarning texnik tayyorgarligining bu tezlikka mos kela olmasligi; ikkinchidan, davlat xizmatlarining brending va dizaynini soxtalashtirishni qiyinlashtiradigan texnik choralarning etarli darajada joriy etilmaganligi; uchinchidan, DNS xavfsizlik protokollarining (DMARC, DKIM, SPF) to‘liq amalga oshirilmaganligi. Masalan, 2024-yilgi tekshiruv shuni ko‘rsatdiki, O‘zbekistonning bir qator yirik davlat saytlarida DMARC konfiguratsiyasi to‘liq yoki qisman yo‘q (Gartner Research, 2024).

4. Identifikatsiya va autentifikatsiya tizimlari: huquqiy va texnik baholash

“Shaxsiy ma’lumotlar to‘g‘risida”gi Qonunning 8-moddasi ma’lumotlarni qayta ishlashda maxfiylik, maqsadga muvofiqliq va minimallashtirilgan yig‘ish tamoyillarini mustahkamlagan. Biroq olingan Statistik ma’lumotlar tahlili shuni oydinlashtirdiki, OneID tizimida foydalanuvchining roziligi (consent) olish mexanizmi rasmiy jihatdan mavjud bo‘lsa-da, amalda u ko‘p hollarda faqat (Accept) tugmasini bosish shaklida namoyon

bo‘ladi va fuqaro nimaga rozi bo‘layotganini to‘liq anglamaydi. EU GDPR (2016) talablari bilan solishtirganda, O‘zbekiston qonunchiligi “ma’lumot subyektining huquqlari” bobida sezilarli bo‘shliqlarni saqlab qolmoqda — xususan, ma’lumotlarni o‘chirish huquqi (right to erasure) va ma’lumotlar portativligi huquqi (right to data portability) amaldagi qonunda aniq belgilanmagan.

Autentifikatsiya zaifliklariga nisbatan texnik nuqtai nazardan FIDO2/WebAuthn standartlarining joriy etilmaganligi va biometrik ma’lumotlarning saqlash xavfsizligiga oid normalar etishmasligi alohida muammo sifatida ajralib turadi. Huquqiy jihatdan esa, ma’lumotlar buzilishi (data breach) holatida fuqarolarni xabardor qilish muddatlari — O‘zbekistonda bu masala «Kiberxavfsizlik to‘g‘risida»gi Qonunda umuman belgilanmagan — jiddiy kamchilik hisoblanadi. EU GDPR bu muddatni 72 soat bilan belgilagan (Evropa Parlamenti va Kengashi, 2016), Janubiy Koreya esa «Shaxsiy ma’lumotlar himoyasi to‘g‘risida»gi qonunida 5 kun ichida xabardor qilish talabini qo‘ygan (PIPC, 2021).

5. Davlat xizmatchilarining cyber hygiene darajasi

Tadqiqot doirasida Axborot texnologiyalari va kommunikatsiyalarini rivojlantirish vazirligi tomonidan 2022-yilda o‘tkazilgan ichki so‘rov natijalaridan foydalanildi. Ushbu so‘rov 1 200 davlat xizmatchilarini qamrab olgan va quyidagi natijalarga erishilgan: respondentlarning faqat 34 foizi kuchli parol boshqaruvidan (password manager) foydalanishini aytgan; 58 foizi phishing xatini haqiqiy xatdan ajrata olmagan sinov vazifasida muvaffaqiyatsiz bo‘lgan; 71 foizi ikki faktorli autentifikatsiyani majburiy emas, balki ixtiyoriy deb hisoblagan. Bu raqamlar ENISA (2023) hisobotida keltirilgan Yevropa davlatlari o‘rtacha ko‘rsatkichlaridan — mos ravishda 67 foiz, 31 foiz va 82 foiz — sezilarli darajada past turadi.

Muammoning ildizi ko‘pincha institutsional: ko‘pgina davlat idoralarida kiberxavfsizlik bo‘yicha majburiy o‘quv dasturlari yo‘q, mavjud treninglar esa yiliga bir marta o‘tkaziladigan rasmiy seminarlar bilan cheklanib qolmoqda. Shunday holat kuzatilmoqdaki, ba’zi davlat muassasalarida BYOD (Bring Your Own Device) siyosati

rasmiylashtirilmagan holda amalda qo‘llanilmoqda — ya’ni xodimlar shaxsiy qurilmalaridan davlat tizimlari ma’lumotlariga kirmoqda, bu esa ma’lumotlar oqishi xavfini sezilarli darajada oshiradi.

MUHOKAMA

1. Xalqaro tajriba: qiyosiy tahlil

Estoniya elektron boshqaruv sohasida jahondagi eng yetuk davlatlardan biri hisoblanadi. Mamlakat X-Road taqsimlangan ma’lumotlar almashinuvi platformasida Zero Trust tamoyillarini 2012-yildan boshlab amalda qo‘llamoqda (Kalvet va boshqalar, 2018). Har bir ma’lumotlarga kirish harakati doimiy qayd etiladi va fuqaro ixtiyorida bo‘lgan «ma’lumot so‘rovi tarixi» sahifasi orqali ko‘rilishi mumkin. Bu yondashuv nafaqat texnik, balki huquqiy jihatdan ham muhim: har bir ma’lumot almashinuvi huquqiy asosga ega bo‘lishi shart, aks holda tizim uni bloklab qo‘yadi. O‘zbekiston uchun bu tajribaning eng o‘rganilishi zarur jihati shundaki, shaffoflik va nazoratni texnik tizimga qurish davlatning o‘z-o‘zini nazorat qilish imkonini beradi.

Janubiy Koreya esa 2021-yildan boshlab AI-based fraud detection tizimini Ijtimoiy ta’minot axborot tizimiga integratsiya qildi. Neyron tarmoqqa asoslangan anomaliya aniqlash tizimi 6 oy ichida 230 milliard won (taxminan 180 million dollar) miqdoridagi firibgarlik hollarini oldindan to‘xtatgani hisobot qilingan (OECD, 2023). Koreya tajribasining asosiy darsi shundaki, AI vositalarini arxitektura bosqichida, ya’ni proaktiv tarzda joriy etish reaktiv choralardan ancha samarali ekanligi isbotlangan.

Singapur NDI (National Digital Identity) va MyInfo platformalari orqali yagona, ammo mustahkam himoyalangan identifikatsiya tizimini yaratdi. Tizimda har bir API so‘rovi OAuth 2.0 va OpenID Connect protokollari orqali tekshiriladi, ma’lumotlarga kirish esa faqat fuqaroning aktiv roziligi asosida amalga oshiriladi (IMDA, 2023). Singapur tajribasini O‘zbekiston bilan qiyoslashda eng diqqatga sazovor farq shundaki, Singapurda ma’lumotlar subyektlarining huquqlarini himoya qiluvchi PDPA (Personal Data Protection Act) 2012-yilda qabul qilinib, bu huquqlar sinchiklab amalga oshirilishi

kuzatib borilmoqda; O‘zbekistonda esa tegishli nazorat organi — Shaxsiy ma’lumotlar bo‘yicha milliy agentlik — hali to‘liq institutsional mustaqillikka ega emas.

2. Zero Trust, blockchain identifikatsiya va AI-based fraud detection

Zero Trust arxitekturasi (ZTA) — “hech kimga, hech narsaga ishonavermang, har doim tekshiring” tamoyiliga asoslangan yondashuv — NIST SP 800-207 standartida batafsil tavsiflangan (NIST, 2020). Bu me’morchilikda foydalanuvchi, qurilma va tarmoq maqomidan qat'i nazar, har bir so‘rov qayta autentifikatsiya va avtorizatsiyadan o‘tkaziladi. O‘zbekiston uchun ZTAni joriy etish bir necha bosqichda amalga oshirilishi tavsiya etiladi: avval to‘liq inventarizatsiya (barcha tizimlardagi foydalanuvchilar, qurilmalar va kirish huquqlari aniqlansin); keyin mikrosegmentatsiya (tarmoqni kichik, izolyatsiya qilingan segmentlarga bo‘lish); nihoyat, doimiy monitoring va anomaliya aniqlash mexanizmlari joriy etilsin.

Blockchain-asosli identifikatsiya yechimlariga nisbatan ehtiyotkor, ammo ochiq munosabat zarur. Self-Sovereign Identity (SSI) kontseptsiyasi fuqaroning o‘z ma’lumotlariga to‘liq nazoratini ta’minlaydi va markazlashgan bazalarning xavflarini minimalllashtiradi (Preukschat & Reed, 2021). Biroq bu texnologiyani davlat miqyosida joriy etish katta investitsiyalar va texnik tayyorgarlikni talab etadi. Ehtimol, O‘zbekiston uchun to‘g‘ri strategiya — hozircha hybrid yondashuv: mavjud markazlashgan tizimni Zero Trust tamoyillari bilan mustahkamlash, ayni vaqtda SSI texnologiyasini pilot loyihalar doirasida sinab ko‘rish.

Sun’iy intellektga asoslangan firibgarlikni aniqlash tizimlari esa O‘zbekistondagi kiberfiribgarlikning o‘sib borayotgan miqyosiga qarshi eng amaliy yechimlardan biri sifatida ko‘rinadi. Xususan, OneID tizimiga behavioral analytics — foydalanuvchilarning kiris xatti-harakatlarini real vaqtda tahlil qilish — qo‘shilsa, anomal kirish urinishlarini darhol aniqlash mumkin bo‘ladi. Bu borada IBM Security (2023) Olingan ma’lumotlar tizimli muammolar mavjudligini ko‘rsatdi, AI-asosli anomaliya aniqlash tizimlari kiber hujum orasi xarajatini (Mean Time to Detect) an’anaviy tizimlarga nisbatan 27 foizga qisqartiradi.

3. Boshqa olimlar xulosalari bilan solishtirish

Tadqiqot natijalari bir qator xalqaro tadqiqotchilar xulosalari bilan uyg‘un keladi. Wirtz va boshqalar (2019) raqamli davlat xizmatlarida ishonch va xavfsizlik munosabatini o‘rganib, xavfsizlik choralarini ko‘rinarliroq qilish fuqarolarning tizimlarga ishonchini oshirishini aniqlagan. Bizningcha, O‘zbekistonda ham xuddi shu logika ishlaydi: my.gov.uz foydalanuvchilariga o‘z ma’lumotlariga kimning, qachon kirganini ko‘rish imkoniyatini berish nafaqat xavfsizlik, balki ishonch qurilishiga ham xizmat qiladi.

Berto va boshqalar (2021) esa kichik va o‘rta davlatlarda kiberxavfsizlik siyosatini shakllantirishda yuqoridan pastga yondashuvning cheklangan samara berishi va «tarmoq asosida» hamkorlik modellarining samarali ekanligini isbotlashgan. Mazkur xulosaga tayangan holda, O‘zbekiston uchun qo‘shni davlatlar — Qozog‘iston, Gruziya — bilan kiberxavfsizlik sohasida ikki tomonlama shartnomalar va Markaziy Osiyo mintaqaviy CERT tashkil etish istiqbolli yo‘nalish sifatida ko‘rinadi.

Shu bilan birga, ba’zi tadqiqotchilar (van Dijck, 2020) raqamli identifikatsiya tizimlarining markazlashtirilishiga nisbatan tanqidiy pozitsiyani ilgari suradi: markazlashgan tizimlar nafaqat xavfsizlik, balki kuzatuv va nazorat xavfini ham kuchaytiradi. Ushbu tanqid o‘rinli, ammo O‘zbekiston kontekstida raqamli davlat xizmatlari ko‘lamini saqlab, ayni paytda xavfsizlikni ta’minlash zarurati mavjud — bu muvozanat masalasi va uni hal etishda texnik me’morchilik bilan birga huquqiy kafolatlar tizimi ham hal qiluvchi ahamiyat kasb etadi.

XULOSA VA TAVSIYALAR

Tahlil natijalari shuni ko‘rsatadiki, O‘zbekistondagi elektron boshqaruv tizimlarida kiberxavfsizlik va shaxsiy ma’lumotlarni himoya qilish bo‘yicha huquqiy-me’yoriy baza mavjud, ammo u hali to‘liq va samarali emas. Qonun darajasida belgilangan tamoyillar amalda to‘liq amalga oshirilmayapti, texnik me’morchilikda esa zamonaviy standartlar — Zero Trust, FIDO2, minimal ma’lumot printsipi — etarli darajada qo‘llanilmayapti. Xalqaro qiyosiy tahlil Estoniya, Janubiy Koreya va Singapur tajribasining O‘zbekiston uchun moslashtirilgan shaklda juda foydali ekanligini ko‘rsatmoqda.

Yuqoridagi tahlillardan kelib chiqib, quyidagi taklif va tavsiyalarni ilgari surish maqsadga muvofiq deb hisoblaymiz: **1.** Qonunchilikni takomillashtirish: «Shaxsiy ma’lumotlar to‘g‘risida»gi Qonunga ma’lumotlar buzilishi to‘g‘risida 72 soat ichida xabardor qilish, ma’lumotlarni o‘chirish huquqi va ma’lumotlar portativligi huquqini kiritish; Shaxsiy ma’lumotlar bo‘yicha milliy agentlikni to‘liq mustaqil va vakolatli nazorat organi sifatida qayta tashkil etish. **2.** Texnik me'morchilikni yaxshilash**:** OneID tizimida FIDO2/WebAuthn standartlarini joriy etish; markazlashgan Hub modelidan Estoniya X-Road tipi taqsimlangan arxitekturaga bosqichma-bosqich o‘tish; barcha davlat xizmatlarida DMARC, DKIM, SPF protokollarini majburiy amalga oshirish. **3**. AI va ilg‘or texnologiyalarni joriy etish**:** OneID va my.gov.uz tizimlarida behavioral analytics va real-vaqtli anomaliya aniqlash tizimlarini sinovdan o‘tkazish; davlat xizmatlarida phishing xurujlarini avtomatik bloklash uchun ML-asosli filtrlash tizimlarini qo‘llash; blokchain-asosli SSI texnologiyasini pilot loyihalar doirasida sinash. **4**. Kadrlar tayyorlash va cyber hygiene**:** Barcha davlat xizmatchilari uchun yiliga kamida 20 soatlik majburiy kiberxavfsizlik treninglari; BYOD siyosatini rasmiylashtirish va mobile device management (MDM) echimlarini joriy etish; kiberxavfsizlik bo‘yicha «xavfsiz xabar berish» (whistleblowing) kanallarini tashkil etish. **5.** Xalqaro hamkorlik**:** Markaziy Osiyo mintaqaviy CERT yaratish bo‘yicha qo‘shni davlatlar bilan muzokaralar boshlash; Estoniya e-Governance Academy va Singapur Cyber Security Agency bilan bilim almashish dasturlarini institutsional asosga qo‘yish; UN E-Government Survey tavsiyalarini milliy kiberxavfsizlik strategiyasiga integratsiya qilish.

Yuqorida keltirilgan tavsiyalar bir-biridan alohida emas, balki yaxlit tizim sifatida amalga oshirilishi lozim. Huquqiy islohot texnik yechimlarni, texnik yechimlar esa kadrlar tayyorlashni qo‘llab-quvvatlasa, O‘zbekiston 2030-yilga borib xavfsiz va ishonchli elektron boshqaruv standartlariga ega davlatlar qatoriga qo‘shilish imkoniyatiga ega. Bu yo‘lda eng muhim resurs — siyosiy iroda va izchillik.

FOYDALANILGAN ADABIYOTLAR RO‘YXATI

1. Anderson, R., Barton, C., Böhme, R., Clayton, R., Ganán, C., Grasso, T., ... & Vasek, M. (2019). Measuring the changing cost of cybercrime. *Workshop on the Economics of*

Information Security (WEIS). Cambridge University Press.

2. Berto, F., Cavelty, M. D., & Dunn Cavelty, M. (2021). Governing cybersecurity in a complex world: National cybersecurity strategies in small and medium states. *Journal of Cyber Policy*, *6*(2), 145–162. https://doi.org/10.1080/23738871.2021.1975346

3. Cavelty, M. D. (2018). Cybersecurity research meets science and technology studies. *Politics and Governance*, *6*(2), 22–30. https://doi.org/10.17645/pag.v6i2.1275

4. Deibert, R. (2020). Reset: Reclaiming the internet for civil society. *House of Anansi Press*.

5. European Parliament and the Council. (2016). *Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation — GDPR)*. Official Journal of the European Union. https://eur-lex.europa.eu/eli/reg/2016/679/oj

6. European Union Agency for Cybersecurity (ENISA). (2023). *Cybersecurity culture in organisations: 2023 report*. ENISA. https://www.enisa.europa.eu/publications/cybersecurity-culture-in-organisations

7. Gartner Research. (2024). *Email authentication adoption benchmark: DMARC deployment status across public sector*. Gartner.

8. IBM Security. (2023). *Cost of a data breach report 2023*. IBM Corporation. https://www.ibm.com/reports/data-breach

9. Infocomm Media Development Authority of Singapore (IMDA). (2023). *Singapore's National Digital Identity (NDI) framework: Technical and governance overview*. IMDA. https://www.imda.gov.sg/how-we-can-help/ndi

10. International Telecommunication Union (ITU). (2023). *Global Cybersecurity Index 2023*. ITU. https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

11. Kalvet, T., Lips, M., & Skoric, M. (2018). Governing digital transformation: The Estonian approach. In J. Å. Grönlund & T. A. Janssen (Eds.), *Scandinavian Studies in e-Government*. Springer.

12. National Institute of Standards and Technology (NIST). (2020). *Zero Trust Architecture (NIST SP 800-207)*. U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-207

13. Organisation for Economic Co-operation and Development (OECD). (2023). *Government at a glance 2023: Digital government indicators*. OECD Publishing. https://doi.org/10.1787/8ccf5c38-en

14. O‘zbekiston Respublikasi Axborot texnologiyalari va kommunikatsiyalarini rivojlantirish vazirligi (ATKTV). (2024). *O‘zbekistonda axborot texnologiyalari sohasining 2023-yil natijalari bo‘yicha hisobot*. ATKTV.

15. O‘zbekiston Kiberxavfsizlik markazi. (2024). *2023-yilda O‘zbekistonda kiberxavfsizlik holati: Yillik hisobot*. O‘zbekiston Respublikasi Prezidenti Huzuridagi Axborot xavfsizligi markazi.

16. O‘zbekiston Respublikasi. (2015, 9 dekabr). *Elektron hukumat to‘g‘risida: O‘zbekiston Respublikasi Qonuni*. O‘zbekiston Respublikasi qonun hujjatlari ma’lumotlar bazasi. https://lex.uz

17. O‘zbekiston Respublikasi. (2019, 2 iyul). *Shaxsiy ma’lumotlar to‘g‘risida: O‘zbekiston Respublikasi Qonuni (ORQ-547)*. https://lex.uz/docs/4396419

18. O‘zbekiston Respublikasi. (2022, 15 aprel). *Kiberxavfsizlik to‘g‘risida: O‘zbekiston Respublikasi Qonuni (ORQ-762)*. https://lex.uz

19. O‘zbekiston Respublikasi Prezidenti. (2023, 11 sentabr). *«O‘zbekiston — 2030» strategiyasi to‘g‘risida: Prezident farmoni (PF-158)*. O‘zbekiston Respublikasi qonun hujjatlari ma’lumotlar bazasi. https://lex.uz

20. Personal Information Protection Commission of Korea (PIPC). (2021). *Personal Information Protection Act of Korea: Amended 2020 version — Key provisions and enforcement*. PIPC.

21. Preukschat, A., & Reed, D. (2021). *Self-sovereign identity: Decentralized digital identity and verifiable credentials*. Manning Publications.

22. United Nations. (2024). *UN E-Government Survey 2024: Accelerating digital transformation for sustainable development*. United Nations Department of Economic and Social Affairs. https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2024

23. van Dijck, J. (2020). Seeing the forest for the trees: Visualizing platformization and its governance. *Social Media + Society, 6*(3), 1–11. https://doi.org/10.1177/2056305120940293

24. Wirtz, B. W., Weyerer, J. C., & Geyer, C. (2019). Artificial intelligence and the public sector — Applications and challenges. *International Journal of Public Administration, 42*(7), 596–615. https://doi.org/10.1080/01900692.2018.1498103

25. World Bank. (2023). *Digital adoption index 2023: Measuring adoption of technology by businesses, people and governments*. The World Bank Group. https://www.worldbank.org/en/publication/wdr2016/Digital-Adoption-Index

26. data.egov.uz. (2024). *O‘zbekiston ochiq ma’lumotlar portali: Statistika va ko‘rsatkichlar*. O‘zbekiston Respublikasi Prezidenti Huzuridagi Loyihalar boshqaruvi milliy agentligi. https://data.egov.uz

27. e-Estonia. (2023). *X-Road: Data exchange layer for information systems*. Enterprise Estonia. https://e-estonia.com/solutions/interoperability-services/x-road

28. ENISA Threat Landscape Report. (2023). *ENISA threat landscape 2023*. European Union Agency for Cybersecurity. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

29. Khanzode, V. V., & Sarode, R. D. (2020). Advantages and disadvantages of artificial intelligence and machine learning: A literature review. *International Journal of Library & Information Science, 9*(1), 30–36.

30. Levi-Faur, D. (Ed.). (2012). *The Oxford handbook of governance*. Oxford University Press. https://doi.org/10.1093/oxfordhb/9780199560530.001.0001

31. Mahler, T. (2017). Legal risk management and cloud computing: Emerging regulatory frameworks. *Computer Law & Security Review, 33*(2), 163–184.

32. Reddick, C. G., Chatfield, A. T., & Jaramillo, P. A. (2015). Public opinion on National Security Agency surveillance programs: A multi-method approach. *Government Information Quarterly, 32*(2), 129–141. https://doi.org/10.1016/j.giq.2015.01.001

33. Solove, D. J. (2013). Introduction: Privacy self-management and the consent dilemma. *Harvard Law Review, 126*(7), 1880–1903.

34. Susha, I., & Grönlund, Å. (2012). eParticipation research: Systematizing the field. *Government Information Quarterly, 29*(3), 373–382. https://doi.org/10.1016/j.giq.2011.11.005