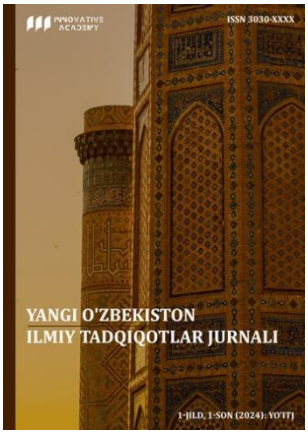

HUQUQIY TEXNOLOGIYALARDA KIBER XAVFSIZLIK: O‘ZBEKISTONNING "KIBER XAVFSIZLIK TO‘G‘RISIDA"GI QONUNNING TAHLILI VA JANUBIY KOREYA STANDARTLARI

Hakimov Azizbek Aminboy Ugli
Toshkent davlat yuridik Universiteti Xalqaro huquq va qiyosiy huquqshunoslik fakulteti 1- bosqich talabasi
https://doi.org/10.5281/zenodo.17532780

ARTICLE INFO

Qabul qilindi: 1-noyabr 2025 yil
Ma’qullandi: 3-noyabr 2025 yil
Nashr qilindi: 4-noyabr 2025 yil

KEY WORDS

kiberxavfsizlik, huquqiy texnologiyalar, elektron hujjat, smart-kontrakt, O‘zbekiston, Janubiy Koreya.

ABSTRACT

Ushbu maqola O‘zbekistonning “Kiber xavfsizlik to‘g‘risida”gi qonuni va Janubiy Koreyaning kiberxavfsizlik standartlarini qiyosiy tahlil qiladi. Maqolada kiberxavfsizlikning huquqiy texnologiyalardagi roli, davlat va xususiy sektorning majburiyatlari, shuningdek, elektron ma’lumotlarni himoya qilish mexanizmlari ko‘rib chiqilgan. Qiyosiy tahlil orqali O‘zbekistonning qonunchiligi va Janubiy Koreya tajribasi o‘rtasidagi o‘xshashliklar va farqlar aniqlanadi. Maqola kiberxavfsizlikni mustahkamlash va milliy qonunchilikni xalqaro standartlar bilan uyg‘unlashtirish bo‘yicha tavsiyalar beradi.

Kirish

Dunyo bo'ylab raqamli o’zgarishlar tezlashib borayotgan bir paytda, kiberxavfsizlik endi faqat texnik muammo emas, balki huquqiy, tashkiliy va siyosiy qiyinchilik hamdir. O'zbekiston kabi kengroq ulanish va raqamli xizmatlarni taqdim etishga kirishayotgan davlatlar uchun axborot tizimlarini himoya qilish, fuqarolarning ma'lumotlarini himoya qilish va kiber-tahdidlarni boshqarish zarurati juda muhim ahamiyat kasb etadi. 2022-yil 15-aprelda O'zbekiston Respublikasi 2022-yil 17-iyulda kuchga kirgan "Kiberxavfsizlik to'g'risida"gi Qonunni qabul qildi. Ammo, Koreya Respublikasi (Janubiy Koreya) Koreya Internet va xavfsizlik agentligi (KISA) tomonidan boshqariladigan ISMS-P (Axborot xavfsizligini boshqarish tizimi) sertifikati kabi yetuk standartlarga ega bo'lgan uzoq vaqtdan beri mavjud bo'lgan kiberxavfsizlik va axborotni himoya qilish rejimiga ega. Shuning uchun O‘zbekiston qonunchiligi va Koreya amaliyotining qiyosiy tahlili orqali O’zbekiston qonunchiligiga foydali tushunchalarni berishi mumkin: O‘zbekiston qanday huquqiy asoslarni joriy etgan, tahdid tendentsiyalari mahalliy miqyosda qanday ko‘rinishga ega, Koreya standartlari amalda qanday ishlaydi va O‘zbekiston kiberxavfsizlik boshqaruvini mustahkamlash uchun qanday saboqlar olishi mumkin.

Metodologiya

Kuchli markaziy texnik agentlik va professional milliy CERT yaratish g’oyasi bu Koreyadan olishimiz mumkin bo’lgan istiqbolli loyihalardan biridir. Bu orqali, siyosatni muvofiqlashtirish, operatsion CERT/CSIRT funksiyalari, zaifliklarni boshqarish, jamoatchilikni xabardor qilish va sanoat uchun texnik yordamni birlashtirgan (Koreyadagi KISAga o'xshash) yagona, yaxshi resurslarga ega milliy kiberxavfsizlik agentligini yaratish yoki mustahkamlash bu kiberxavsizlik tizimimiz uchun sezilarli darajadagi keng islohotdir. Bundan tashqari, “Kiberxavfsilik to’g’risidagi qonun” va shuningdek boshqa qiyosiy qonunchiliklardagi tahlilim asosida shuni ayta olamanki O’zbekistonning banklar va banklararo aylanmalar sohasi ancha xavfsizlik va e’tiborga muhtoj. Bunday xulosaga kelishimga asosiy sabab bu Janubiy

Koreyaning Moliyaviy sohadagi kiberxavfsizligi bilan taqqoslov bo’ldi chunki u Janubiy Koreyada bank servislari KISA (Korea Internet & Security Agency) tizimiga amal qilgan holda to’lov tizimini tashkillashtirgan hisoblanadi. KISAning ustunligi shundaki bu orqali banklar o’zaro hujumlar haqidagi ma’lumotni avtomatik almashadi. O‘zbekistonda bunday yagona axborot almashish platformasi hali to‘liq yo‘lga qo‘yilmagan, monitoring asosan so‘rov va hisobot shaklida amalga oshiriladi. Shuningdek ularda Majburiy xavfsizlik sertifikatsiyasi **“Security Grade System”** mavjud, ya’ni KISA tashkiloti har bir bankning xavfsizlik va ITga oid bo’limini yillik auditdan o’tkazadi. Masalan, **Shinhan Ban**k, **Kookmin Bank** va **Hana Banklar** 2024-yilda “**A** daraja” bilan tasdiqlangan. Agar biror tizim “**C**” yoki “**D**” darajada bo‘lsa, unga onlayn xizmatlar ko‘rsatishga ruxsat berilmaydi. Bularning faktik farqi, O‘zbekistonda “sertifikatlashtirilgan tizim” talabi mavjud, ammo balli yoki darajali baholash tizimi mavjud emas. Auditlar muntazam emas, balki normativ talabga asosan o‘tkaziladi. Bunday ma’sulyatli tizimni tashkillashtirish uchun ular Shaxsiy javobgarlik va rahbarlar uchun qat’iy jazolarni ham qo’llashdan tap tortishmagan. 2021-yilda **KakaoBank**da ma’lumotlar sizib chiqishi uchun CEO 1 yilga diskvalifikatsiya qilingan. **PIPA (Personal Information Protection Act)** ga ko‘ra, bank mijoz ma’lumotlarini himoya qilmasa, jarima bank aylanmasining 3% gacha yetishi mumkin. O‘zbekistonda hozircha rahbarlar uchun shaxsiy javobgarlik mexanizmi sust, jarimalar asosan tashkilot miqyosida belgilanadi.

Muhokama

Bu loyihani amalga oshirish uchun avvalambor bizga qonuniy vakolatlarga ega bo’lgan shuningdek aniq majburiyat belgilab bera oldigan organlarning ruxsati kerak bo’ladi. Misol uchun, shu sohaga doir Prezident farmoni yoki Vazirlar mahkamasi Qarori orqali bu loyihani keng miqyosda shuningdek tez muddatda bajarish imkoni vujudga keladi. Bundan tashqari, bu loyihaning yetarli darajada kuchli va zarur bo’lgan potensialini namoyon etishi uchun mudofaa, ichki ishlar, moliya vazirliklaridan yangi agentlik uchun ishchi guruhlar tuzishga yordam berish va ularning ushbu vazirlik tizimidan qisman yoki to’liq foydalanish uchun cheklovlar olib tashlanishi maqsadga muvofiq bo’lardi. Chunki ular yordami orqali smenali, 24/7 hodisalarni boshqarish, sud-tibbiy laboratoriyalar va xavfsiz SOC (xavfsizlik operatsiyalari markazi) bilan to'liq ishlaydigan milliy CERT/CSIRTni tizimlashtirish osonlashardi.

Yuqorida aytilgan talabdagi kuchli tizimlashgan holda tashkil etilgan CERT orqali 24 soat ichida tahdid yuzasidan xabar berish tizimini tashkillashtirish talabi qo’yilsa foydadan xoli bo’lmas edi. Chunki bu orqali milliy CERT virus yoki yetkazilgan zararning manbaiini aniqlab unga zarba berish orqali boshqa tizimlarni hakerlar hujumidan saqlab qolishadi va shuningdek ularning API manzillari orqali taxminiy joylashuv va shuningdek ularning qurilmalari haqida ko’p malumot olish imkoni bo’ladi. Lekin, bu 24 soatdan o’ta u yerdagi ko’plab qimmatli ma’lumotlar allaqachon yo’qolgan bo’ladi, Misol uchun, bu yondashuv Janubiy Koreyada qonun asosida mustahkamlab qo’yilgan va bu jabrlanuvchilarni ogohlikka chaqirishga yordam beradi.

Natija

O’zbekiston Respublikasining kiberxavfsizlik to’g’risidagi qonuni 2022 yilda ishlab chiqilgan bo’lib hozirgi kunda ko’proq qo’llanma vazifasini bajara olyapti xolos yani undagi malumotlar yetarlicha faktik emas va ushubu jihati ham uning yangi tuzilgani va uning qayta ishlashga muhtojligini bildirib turadi.
Chunki kiberxavsizlik sohasi shunchalik kattaki bizning qonunda u haqida malumotlarning Caselarning hattoki 5% ham kiritilmagan. Ammo buning sababi ushbu haligacha kiritlmagan sohalarga nisbatan talab bo’lmayotgani va uni chuqurroq rivojlantirish uchun bizga ko’proq vaqt va tajriba kerak ekanligini takidlab o’tishimiz maqsadga muvofiq bo’ladi.

Shuningdek raqamli texnologiyalarning rivojlanish tezligi tobora ortib bormoqda ayniqsa su'niy intelekt va blokcheyn. Lekin bizning qonunchilik tizimimiz bu ikki gigant sohani to'laligicha qoplay olgani yo'q, ammo buning uchun sabablar ham yetarlicha. Qonun nimaga yaratiladi ? Buning birdan bir sababi ushbu sohada jamiyatimizda talab mavjud va u yerda ma'lum bir huquqiy muammolar bor, va ko'rib turibsizki u muammolarni yechish uchun qonunlar ishlab chiqila boshlanadi. Demak biz bu sohadagi qonunchilikni to'liq bo'lishini talab qilishdan oldin O"beksitonda yetarlicha keng tendensiyadagi foydalanuvchilar soni shuningdek bunga muvofiq muammolar soniga ega bo'lishimiz darkor.
Keling kiber sohaning yondosh bir bo'gini bo'lmish Blokcheyn va smart kontraktlar haqida mushohada qilsak. O'zbekiston Respublikasining Blokcheyn va Smartkontraktlar Qonunchiligida ma'lum bir muammolar kuzatiladi. Men bu muammoni aynan "SmartKontrakt" so'ziga ta'rif izlaganimda sezgandim.

SMART KONTRAKT so'ziga ta'rif:
https://lex.uz/docs/-6299481?query=smart%20kontrakt#sr-1

ELEKTRON HUJJAT so'ziga ta'rif:
https://lex.uz/ru/docs/-165079

Smart-kontraktning ta'rifining oxirgi qismiga e'tibor berilsa, unda "elektron shakldagi shartnoma" deb aytilgan. Lex.uz portalida esa aynan "elektron shartnoma"ga aniq ta'rif berilmagan, biroq u elektron hujjat ekanligini bilamiz. Endi "elektron hujjat" ta'rifiga qarasak, unda elektron raqamli imzo (E-imzo) bo'lishi shartligi ko'rsatilgan. Bu holatni qonunchilikdagi nomuvofiqlik yoki xato deb atash mumkin. Chunki blokcheyn texnologiyasi asosidagi smart-kontraktga E-imzo qo'yishning imkoni yo'q. Demak, smart-kontraktning amaldagi qonunlardagi ta'rifi uning asl texnologik mohiyatiga zid keladi. Masalani tushuntirish biroz murakkab bo'lishi mumkin, chunki blokcheynning o'zi ham murakkab tizimdir. Raqamli imzo ba'zan sertifikatlangan raqamli kod deb ham ataladi. E-imzoning aniq texnik va huquqiy talablari mavjud. Ammo blokcheynda ishlatiladigan kriptoimzolar — masalan, **ECDSA** yoki **Ed25519** algoritmlariga asoslangan imzolar — ko'pincha milliy sertifikatlangan elektron raqamli imzo (EDS) bilan teng deb tan olinmaydi. Natijada, davlat tomonidan talab qilinadigan turdagi E-imzoni smart-kontraktga qo'yishning iloji bo'lmaydi. Shu sababli, amaldagi qonunchilikdagi smart-kontrakt ta'rifi bilan texnologiyaning o'zi o'rtasida huquqiy-texnik ziddiyat yuzaga keladi.

Xulosa

Bundan xulosa qilishimiz mumkinki bizning Kiber sohadagi qonuchilik tizimimiz yetarlicha mukammal emas va o'zgartirishlarga muhtoj. O'zbekistonda kiberxavfsizlik sohasi ikkinchi darajali texnik muammodan milliy xavfsizlik va raqamli suverenitet masalasi darajasiga qarab tobora rivojlanib bormoqda. "Kiberxavfsizlik to'g'risida"gi qonunning (2022) qabul qilinishi raqamli tizimlar, ma'lumotlar va foydalanuvchilarni himoya qilish uchun huquqiy asos yaratishda katta qadam bo'ldi. Biroq, ushbu asosni amaliy amalga oshirish haligacha e'tibortalab masala bo'lib qolmoqda. Ko'pgina tashkilotlarda hali ham malakali mutaxassislar, zamonaviy infratuzilma va yagona milliy kiberhujum kabi hodisalarga javob berish tizimi yetishmaydi.

Xalqaro standartlarga erishish uchun O'zbekiston o'z qonunlarini global amaliyotlar, masalan, Janubiy Koreya va Yevropa Ittifoqida qo'llaniladigan amaliyotlar bilan uyg'unlashtirishda davom etishi kerak, ushbu davlatlarda kiberxavfsizlik siyosati raqamli boshqaruv va ta'lim bilan chuqur integratsiyalashgan. Jamoatchilik xabardorligini oshirish, professional tayyorgarlikka investitsiya kiritish va davlat va xususiy sektor o'rtasidagi hamkorlikni rivojlantirish ham juda muhimdir. Xulosa qilib aytganda, O'zbekiston kiberxavfsizlik ekotizimini shakllantirishda sezilarli yutuqlarga erishgan bo'lsa-da, keyingi rivojlanish kuchli

institutlarni yaratish, texnologik innovatsiyalarni rag'batlantirish va raqamlashtirishning har bir bosqichi paydo bo'layotgan kibertahdidlardan samarali himoya bilan mos kelishini ta'minlashga bog'liq.

Foydalanilgan adabiyotlar:

1. **O‘zbekiston Respublikasi “Kiberxavfsizlik to‘g‘risida”gi Qonuni**, № ZRU-764 (2022-yil aprel). Blackswan nashriyoti.
“O‘tgan yili O‘zbekiston veb-resurslariga 11,2 milliondan ortiq kiberhujumlar uyushtirildi.” Kun.uz (2023). Kun.uz axborot portali.
“O‘zbekiston 2024-yilning birinchi choragida 3 milliondan ortiq kiberhujumlar haqida xabar berdi.” Kun.uz (2024). Kun.uz axborot portali.
“2025-yil uchun O‘zbekistonda asosiy kiberxavf tahdidlari prognozi.” UzCERT (2024). UzCERT xizmati.
Internet Society Pulse: O‘zbekiston bo‘yicha hisobot. pulse.internetsociety.org.
K-ISMS, ISMS-P sertifikatsiya tizimi (KISA). kisa.or.kr; Amazon Web Services, Inc.
Kim & Chang: “Koreyada axborot xavfsizligi bilan bog‘liq sertifikatsiya talablari.” kimchang.com.
Milliy Kiberxavfsizlik Tashkiloti: Koreya Respublikasi bo‘yicha hisobot. CCDCOE (2022).