

“RAQAMLI MAKONDA KIBERJINOYATCHILIK: ZAMONAVIY TAHDIDLAR VA HUQUQIY HIMOYA MEXANIZMLARI”

Mo'minova Nozimaxon Akmaljon qizi

*O'zbekiston Respublikasi Huquqni muhofaza qilish
akademiyasi “Tergov faoliyati” yo'nalishi 3-bosqich talabasi*

MAQOLA MALUMOTI

ANNOTATSIYA:

MAQOLA TARIXI:

Received: 04.02.2026

Revised: 05.02.2026

Accepted: 06.02.2026

KALIT SO'ZLAR:

*kiberjinoyat, raqamli
makon, fishing,
kiberxavfsizlik, Jinoyat
kodeksi, raqamli dalil.*

Ushbu maqolada raqamli makonda sodir etilayotgan zamonaviy kiberjinoyatlarning turlari, ularning jamiyat xavfsizligiga ta'siri va O'zbekiston Respublikasi qonunchiligidagi huquqiy himoya mexanizmlari tahlil qilinadi. Shuningdek, kiberjinoyatlarga qarshi kurashishda xalqaro tajriba va milliy qonunchilikni takomillashtirish masalalari ko'rib chiqiladi.

Bugungi kunda insoniyat hayotini internetsiz va raqamli texnologiyalarsiz tasavvur etib bo'lmaydi. Dunyo iqtisodiyoti, davlat boshqaruvi va hatto shaxsiy muloqotlar ham virtual makonga ko'chdi. Internet, mobil ilovalar, ijtimoiy tarmoqlar va elektron xizmatlar kundalik faoliyatimizni yengillashtirayotgan bir paytda, ular bilan bog'liq xavf-xatarlar ham ortib bormoqda. Xususan, raqamli makonda sodir etilayotgan kiberjinoyatlar shaxs, jamiyat va davlat xavfsizligiga jiddiy tahdid solmoqda.

Kiberjinoyatchilik — bu axborot-kommunikatsiya texnologiyalaridan foydalangan holda sodir etiladigan huquqbuzarliklar bo'lib, u shaxsiy ma'lumotlarni o'g'irlash, firibgarlik, noqonuniy kirish, zararli dasturlar tarqatish kabi ko'rinishlarda namoyon bo'ladi. Ushbu jinoyatlar tezkorligi, yashirinligi va hududiy chegaralarga bo'ysunmasligi bilan an'anaviy jinoyatlardan farq qiladi. Kiberjinoyatchilikning o'ziga xos xususiyati shundaki, jinoyat sodir etuvchi shaxs va jabrlanuvchi orasida minglab kilometr masofa bo'lishi mumkin. Masalan, agar ilgari o'g'ri uyingizga kirishi uchun eshikni buzishi kerak bo'lgan bo'lsa, hozirda u smartfoningizga kelgan oddiy bir "shubhali havola" (link) orqali hamyoningizni bo'shatishi mumkin. Statistika shuni ko'rsatadiki, so'nggi yillarda bank kartalaridan pul o'g'irlash va shaxsiy ma'lumotlarni tovlamachilik yo'li bilan qo'lga kiritish holatlari keskin ortgan. Bu esa milliy qonunchiligimizdagi huquqiy himoya mexanizmlarini qayta ko'rib chiqishni va raqamli makonda xavfsizlikni ta'minlashning yangi usullarini joriy etishni taqozo etmoqda.

=====

Zamonaviy sharoitda kiberjinoyatchilikka qarshi samarali kurashish faqat texnik choralar bilangina emas, balki mustahkam huquqiy mexanizmlar orqali ham ta'minlanishi lozim. Shu bois, raqamli makonda yuzaga kelayotgan zamonaviy kiberxavflarni aniqlash, ularning oldini olish hamda huquqiy himoya mexanizmlarini takomillashtirish dolzarb masalalardan biri hisoblanadi.

Raqamli makonda kiberjinoyatchilikning asosiy turlari va zamonaviy tahdidlar

Raqamli makon kengaygani sari kiberjinoyatchilik turlari ham ko'payib bormoqda. Hozirgi kunda eng ko'p uchraydigan kiberjinoyatlar qatoriga internet orqali firibgarlik, shaxsiy ma'lumotlarni o'g'irlash, bank kartalari va elektron hamyonlarni buzish, ijtimoiy tarmoqlarda soxta sahifalar ochish hamda zararli dasturlar (viruslar) tarqatishni kiritish mumkin.

Zamonaviy tahdidlarning asosiy xususiyati shundaki, jinoyatchi jabrlanuvchi bilan bevosita aloqaga kirmasdan turib ham zarar yetkazishi mumkin. Masalan, fishing (soxta havolalar orqali ma'lumotlarni qo'lga kiritish) usuli orqali foydalanuvchilar o'zlari bilmagan holda login, parol yoki bank kartasi ma'lumotlarini jinoyatchilarga topshirib qo'ymoqda. Bundan tashqari, sun'iy intellekt va avtomatlashtirilgan dasturlar yordamida ommaviy kiberhujumlar amalga oshirilayotgani ham jiddiy xavf tug'dirmoqda.

Kiberjinoyatlarni maqsadiga ko'ra ikki guruhga bo'lish mumkin: Birinchisi, Kompyuterga qarshi jinoyatlar ya'ni maqsad tizimni ishdan chiqarish (viruslar, DoS-hujumlar). Ikkinchisi, Kompyuter yordamidagi jinoyatlar ya'ni kompyuter shunchaki qurol (firibgarlik, shaxsiy ma'lumotlarni o'g'irlash, tuhmat) hisoblanadi.

Yangi avlod kiberjinoyatlariga misol qilib Deepfake tahdidini keltirish mumkin. Bu — sun'iy intellekt yordamida insonning yuzi va ovozi o'xshatish texnologiyasi. Buning huquqiy xavfi jinoyatchilar korxona rahbarining ovozi o'xshatib (Deepfake audio), buxgalterga pul o'tkazish bo'yicha topshiriq berish holatlari uchrayapti. Bu huquqda "shaxsni soxtalashtirish" (impersonation) muammosini keltirib chiqaradi.

Agar klassik jinoyatchilikda 'izlar' barmoq izlari orqali topilgan bo'lsa, kiber-makonda jinoyatchining 'izi' uning IP-manzili va raqamli imzosidir. Biroq, anonimizatorlar (VPN) va kriptovalyutalar bu izlarni o'chirishga xizmat qilayotgani bugungi kunda huquqni muhofaza qilish organlari oldidagi eng katta texnik va huquqiy muammodir.

Kiberjinoyatchilikka qarshi kurashda huquqiy mexanizmlarning ahamiyati

Huquqiy mexanizm — bu shunchaki qog'ozdagi qonun emas, balki jinoyatni aniqlashdan tortib, aybdorni jazolashgacha bo'lgan yaxlit tizimdir. Kiberjinoyatchilikka qarshi samarali kurashishda huquqiy mexanizmlar muhim o'rin tutadi. Qonunchilikda kiberjinoyat tushunchasining aniq belgilanishi, javobgarlik choralarining ko'zda tutilishi va huquqni muhofaza qiluvchi organlarning vakolatlari mustahkamlanishi zarur.

Ko'plab davlatlar raqamli xavfsizlikni ta'minlash maqsadida maxsus qonunlar va strategiyalarni qabul qilgan. Masalan, Yevropa Ittifoqida shaxsiy ma'lumotlarni himoya

qilish bo'yicha umumiy reglament (GDPR) amal qiladi. Ushbu hujjat fuqarolarning shaxsiy ma'lumotlarini qayta ishlash va saqlashda qat'iy talablarni belgilab, ularni noqonuniy foydalanishdan himoya qiladi. Qoidalarni buzgan tashkilotlarga katta miqdorda jarima qo'llanilishi belgilangan.

Agar raqamli makonda jazo muqarrarligi belgilanmasa, kiberjinoyatchilik "daromadli va xavfsiz" sohaga aylanadi. Qonunda jazolarning qat'iy belgilanishi (masalan, JK 168-moddasidagi 8 yilgacha ozodlikdan mahrum qilish) potensial jinoyatchilarni to'xtatib turuvchi asosiy omildir.

Bugungi kunda O'zbekiston jinoyat qonunchiligi raqamli jinoyatlarga nisbatan ancha "shafqatsiz"lashgan. Xususan, Jinoyat kodeksining 168-moddasi (Firibgarlik) ga kiritilgan o'zgartirishlarga ko'ra, jinoyatni axborot texnologiyalaridan foydalanib sodir etish "og'irlashtiruvchi holat" hisoblanadi(168-moddasi 3-qismi "g" bandi). Oddiy misol qilib, agar ko'chada birovni aldab pulini olsangiz, bu oddiy firibgarlik, lekin buni plastik karta yoki Telegram orqali qilsangiz, sizga kamida 5 yildan 8 yilgacha ozodlikdan mahrum qilish jazosi tayinlanishi mumkin. Shuningdek, Jinoyat kodeksining XX¹ bobi (278¹-278⁷-moddalar) aynan kompyuter tizimiga ruxsatsiz kirish va ma'lumotlarni o'chirish kabi xatti-harakatlarni jinoiy javobgarlikka tortadi.

Texnologiya qanchalik rivojlanmasin, u faqat qurol bo'lib qolaveradi. Ushbu qurol kimning qo'lida ekanligi va undan foydalanish oqibatlari uchun javobgarlikni esa faqat Huquqiy mexanizm belgilaydi. Shuning uchun ham, kiber-makonda huquq ustuvorligini ta'minlash — milliy xavfsizlikning ajralmas qismidir.

Xorijiy davlatlar tajribasi va Kiberjinoyatchilikning oldini olishda profilaktika choralarining ro'li

AQSh kiberjinoyatchilikka qarshi kurashda kompleks yondashuvni qo'llaydi. Bu mamlakatda maxsus kiberxavfsizlik agentliklari faoliyat yuritib, davlat va xususiy sektor hamkorligi yo'lga qo'yilgan. Banklar, kompaniyalar va davlat organlari o'rtasida axborot almashinuvi tizimi mavjud bo'lib, bu kiberhujumlarning oldini olishga yordam beradi. AQSHda kiberjinoyatlar bilan nafaqat politsiya, balki FTB (FBI) tarkibidagi maxsus bo'limlar shug'ullanadi. Ularda "Cyber Action Teams" (Kiber harakat guruhlari) mavjud bo'lib, ular dunyoning istalgan nuqtasidagi xakerlarni kuzatish imkoniga ega.

Yevropa Ittifoqi (Budapesht konvensiyasi): Bu kiberjinoyatchilikka qarshi kurash bo'yicha dunyodagi birinchi xalqaro shartnomadir. Unga ko'ra, davlatlar bir-biriga raqamli dalillarni (IP-manzil, log-fayllar) tezkorlik bilan yetkazib berishga kelishgan.

Estoniya tajribasi ham e'tiborga loyiq. Ushbu davlat elektron hukumat tizimini rivojlantirish bilan birga, kuchli kiberxavfsizlik infratuzilmasini yaratgan. Maxsus milliy kiberxavfsizlik strategiyasi orqali davlat axborot resurslari va fuqarolarning ma'lumotlari himoya qilinadi. Bu davlat "Raqamli davlat" modelini qurgan. Ularda har bir fuqaro o'z

ma'lumotlari qayerda va kim tomonidan ko'rilganini onlayn kuzatib tura oladi. Bu shaffoflik kiber-tovlamachilik xavfini keskin kamaytiradi.

Janubiy Koreya esa aholi o'rtasida raqamli savodxonlikni oshirishga alohida e'tibor qaratadi. Maktab va oliy ta'lim muassasalarida kiberxavfsizlik asoslari o'rgatiladi. Natijada fuqarolar kiberxavflarni erta aniqlash va o'zlarini himoya qilish ko'nikmalariga ega bo'lmoqda. Shuningdek, Janubiy Koreya modeli (Tezkor javob berish), bu davlatda kiberjinoyatchilikka qarshi kurashuvchi maxsus politsiya bo'linmalari ("Cyber Bureau") mavjud. Ularning asosiy tajribasi — banklar va provayderlar bilan real vaqt rejimida (24/7) ma'lumot almashish tizimi yo'lga qo'yilgan. Agar shubhali tranzaksiya aniqlansa, tizim uni avtomatik bloklaydi.

Kiberjinoyatchilikka qarshi kurash faqat jazolash bilan cheklanib qolmasligi kerak. Eng samarali yo'l — bu profilaktika, ya'ni jinoyat sodir etilishining oldini olishdir. Bunda foydalanuvchilarning hushyorligi, kuchli parollardan foydalanish, shubhali havolalarga kirmaslik va axborot xavfsizligi qoidalariga rioya qilish muhim ahamiyatga ega. Shuningdek, davlat organlari tomonidan aholiga tushuntirish ishlari olib borilishi, ommaviy axborot vositalari orqali kiberxavfsizlik bo'yicha tavsiyalar berilishi kiberjinoyatlar sonining kamayishiga xizmat qiladi.

Xorijiy tajriba shuni ko'rsatadiki, eng zamonaviy texnologiya ham 'Inson faktori' oldida ojiz qolishi mumkin. Shuning uchun kiber-profilaktikaning eng samarali usuli — bu jamiyatda 'Kiber-sergaklik' instinktini shakllantirishdir. Kuchli huquqiy baza va yuksak raqamli madaniyat birlashgandagina kiber-makon xavfsiz hududga aylanadi.

Xulosa va takliflar

Xulosa qilib aytganda, raqamli makonda kiberjinoyatchilik zamonaviy jamiyat uchun jiddiy huquqiy va ijtimoiy tahdid sifatida namoyon bo'lmoqda. Axborot-kommunikatsiya texnologiyalarining jadal rivojlanishi inson hayotini qulaylashtirgan bo'lsa-da, ularning noqonuniy qo'llanilishi shaxs, jamiyat va davlat manfaatlariga sezilarli zarar yetkazmoqda. Kiberjinoyatlarning yashirinligi, tezkorligi va transchegaraviy xususiyati ularni aniqlash va oldini olish jarayonini murakkablashtirmoqda.

Tadqiqot natijalari shuni ko'rsatadiki, kiberjinoyatchilikka qarshi samarali kurash faqat texnik himoya choralari tayanib qolmasligi lozim. Ushbu sohada mustahkam huquqiy mexanizmlar, jazo muqarrarliligi, huquqni muhofaza qiluvchi organlarning maxsus vakolatlari hamda xalqaro hamkorlik muhim ahamiyat kasb etadi. O'zbekiston Respublikasi jinoyat qonunchiligida kiberjinoyatlar uchun javobgarlikning kuchaytirilishi raqamli makonda huquq ustuvorligini ta'minlashga qaratilgan muhim qadam hisoblanadi.

Xorijiy davlatlar tajribasi, xususan AQSh, Estoniya va Janubiy Koreya amaliyoti kiberxavfsizlikni ta'minlashda huquqiy tartibga solish, texnologik himoya va raqamli savodxonlikning o'zaro uyg'unligi eng samarali model ekanini ko'rsatadi. Shu bois, raqamli

makonda xavfsiz muhitni shakllantirish davlat organlari, xususiy sektor va fuqarolarning oʻzaro hamkorligiga asoslanishi zarur.

Umuman olganda, kuchli huquqiy baza, samarali profilaktika va yuksak raqamli madaniyat uygʻunlashgan taqdirdagina kiberjinoyatchilikka qarshi barqaror va ishonchli himoya tizimini yaratish mumkin boʻladi. Kiberjinoyatlarning transmilliy xususiyatini inobatga olib, xalqaro shartnomalar va axborot almashinuvi mexanizmlaridan faol foydalanish lozim.

Xorij tajribasidan (masalan, Budapesht konvensiyasi) kelib chiqib, raqamli dalillarni (IP-manzil, log-fayllar) tezkorlik bilan yigʻish va xalqaro miqyosda almashish boʻyicha huquqiy hamkorlikni kuchaytirish lozim.

Janubiy Koreya tajribasiga tayanib, maktab va oliy taʼlim muassasalarida kiberxavfsizlik asoslarini oʻrgatishni majburiy darajaga koʻtarish, bu orqali aholining "raqamli madaniyati"ni yuksaltirish zarur.

Oʻzbekiston Respublikasi qonunchiligida kiberjinoyatlar uchun javobgarlikning kuchaytirilishi va maxsus "Kiberxavfsizlik toʻgʻrisida"gi qonunining qabul qilinishi ushbu yoʻnalishdagi muhim qadamlardir. Biroq, xalqaro tajriba shuni koʻrsatadiki, eng mukammal qonun ham "inson omili" va raqamli savodxonlik yetarli boʻlmagan joyda oʻz samarasini yoʻqotishi mumkin. Faqatgina zamonaviy texnologik yechimlar, mustahkam huquqiy baza va yuksak raqamli madaniyat uygʻunligi orqali kiber-makonni barcha uchun xavfsiz va ishonchli hududga aylantirish mumkin. Texnologiya shunchaki vosita, uning ezgu maqsadlarga xizmat qilishi esa bevosita biz yaratgan huquqiy mexanizm va ijtimoiy hushyorlikka bogʻliqdir.

Foydalanilgan adabiyotlar

1. Oʻzbekiston Respublikasining Konstitutsiyasi. – Toshkent: Oʻzbekiston, 2023.
2. Oʻzbekiston Respublikasi Jinoyat kodeksi.
3. Oʻzbekiston Respublikasining "Axborotlashtirish toʻgʻrisida"gi Qonuni.
4. Oʻzbekiston Respublikasining "Shaxsga doir maʼlumotlar toʻgʻrisida"gi Qonuni.
5. Oʻzbekiston Respublikasining "Kiberxavfsizlik toʻgʻrisida"gi Qonuni, 15.04.2022 yildagi OʻRQ-764-son.
6. "Raqamli makonda kiberjinoyatchilik: Zamonaviy tahdidlar va huquqiy himoya mexanizmlari" mavzusidagi tahliliy materiallar.
7. Council of Europe. Convention on Cybercrime (Budapest Convention), 2001.
8. European Union. General Data Protection Regulation (GDPR), 2016.
9. United Nations Office on Drugs and Crime (UNODC). Cybercrime and Digital Evidence.
10. FBI. Cyber Crime and Cyber Security Overview.