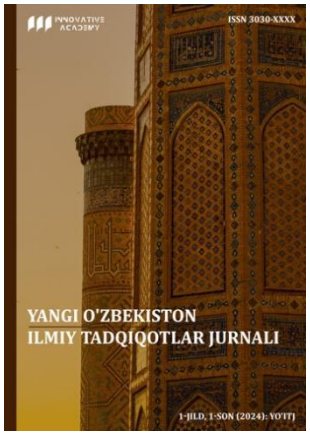

RAQAMLI MAKONDAGI JINOYATLAR VA ULARNING SUD-HUQUQIY TALQINI

To'lqinova Visola Ulug'bek qizi

Toshkent davlat yuridik universiteti

Jinoiy odil sudlov fakulteti talabasi

E-mail: visolatolqinova05@gmail.com

https://doi.org/10.5281/zenodo.20520488

ARTICLE INFO

Qabul qilindi: 11-may 2026 yil
Ma'qullandi: 15-may 2026 yil
Nashr qilindi: 31-may 2026 yil

KEY WORDS

kiberjinoyat, sud amaliyoti, kiberfiribgarlik, kibero'g'irlik, elektron dalil, shaxsga doir ma'lumotlar, bank kartalari, onlayn kredit, O'zbekiston Jinoyat kodeksi, kiberxavfsizlik.

ABSTRACT

Mazkur maqolada O'zbekistonda kiberjinoyatlar bo'yicha sud amaliy- otining normativ, statistik va doktrinal asoslarini tahlil qilinadi. Tadqiqotning markaziy g'oyasi shundan iboratki, milliy amaliyotda kiber- jinoyat faqat Jinoyat kodeksining axborot texnologiyalari sohasiga bag'ishlangan maxsus normalari bilan cheklanmaydi; aksariyat hollarda u ***klassik Mulki tarkiblar, shaxsga doir ma'lumotlar himoyasi va elektron dalillar rejimi bilan kesishgan holda*** *namoyon bo'ladi. O'zbekiston Respublikasining* ***"Kiberxavfsizlik to'g'risida"****gi Qonuni 3-moddasida* ***kiberjinoyatchilik*** *- axborotni egallash, uni o'zgartirish, yo'q qilish yoki axborot tizimlari va resurslarini ishdan chiqarish maqsadida kibermakonda dasturiy ta'minot va texnik vositalardan foydalanilgan holda amalga oshiriladigan jinoyatlar yig'indisi*[1] *deb ta'riflanadi, shu bois sud amaliyotining vazifasi faqat texnik hujumni tasvirlash emas, balki uning huquqiy mohiyatini aniqlashdan iborat. Maqolada Oliy sud plenum qarorlari, Oliy sudning 2024yilgi jinoyat ishlari bo'yicha statistika byulleteni, Ichki ishlar vazirligi va Prezident uzurida e'lon qilingan rasmiy tahliliy ma'lumotlar, Markaziy bankning antifrod va onlayn kredit xavfsizligiga doir yangi normativ talablari, shuningdek mahalliy va xorijiy ilmiy manbalar asosida O'zbekistonda kiberjinoy-atlarning o'sish sur'ati, ularning sud-huquqiy kvalifikatsiyasi va amaliy muammolari ochib beriladi. Muallifning asosiy xulosasi shuki, bugungi milliy sud amaliyoti* ***"klassik jinoyat + raqamli vosita"*** *formulasidan* ***"raqamli muhitning o'zi jinoyatning maydoni, quroli va iziga aylangan"*** *bosqichga o'tgan.*

[1] O'zbekiston Respublikasining 2022-yil 15-apreldagi O'RQ-764-son *"Kiberxavfsizlik to'g'risida"*gi Qonuni

KIRISH (INTRODUCTION)

So‘nggi yillarda O‘zbekistonda kiberjinoyatlar masalasi nazariy tadqiqot mavzusi bo‘lib qolmay, jinoiy adliyaning eng og‘riqli amaliy yo‘nalishlaridan biriga aylandi. Rasmiy ma’lumotlarga ko‘ra, 2019-yilda axborot texnologiyalari yor- damida sodir etilgan 18 turdagi 863 ta jinoyat qayd etilgan bo‘lsa, 2024-yilda bunday jinoyatlar 62 turga yetib, jami 58 800 tani tashkil etgan; besh yil ichidagi o‘sish 68 baravar deb baholangan[2]. Aynan shu manbada 2023-yilda umumiy inoyatchilik tarkibida kiberjinoyatlarning ulushi 6,2 foiz bo‘lgan bo‘lsa, 2024- yilda u 44,4 foizga chiqqani, demak deyarli har ikkinchi jinoyatning raqamli komponent kasb etgani qayd etiladi[3]. Bu raqamlar sud amaliyotiga ikki tomonlama bosim tushiradi: bir tomondan, **jinoyat tarkiblarini to‘g‘ri kvalifikatsiya qilish** masalasi murakkablashadi; ikkinchi tomondan esa, dalillarni yig‘ish, ularni saqlash va sudga maqbul shaklda taqdim etish talablari yangi sifat bosqichiga ko‘tariladi.

Kiberjinoyatchilikning huquqiy mohiyatini tushunishda konstitutsiyaviy fon alohida ahamiyatga ega. Konstitutsiyamizga ko‘ra, har kim o‘z sha’ni va obro‘siga qilingan tajovuzlardan, shaxsiy hayotiga aralashishdan himoyalanish huquqiga ega; yozishmalar va telefonda so‘zlashuvlar sirini oshkor qilish faqat qonunda nazarda tutilgan hollarda va tartibda mumkin[4]. Shu sababli kiberjinoyatlarga qarshi kurashish faqat repressiv siyosat emas, balki shaxsiy hayot, bank siri va shaxsga doir ma’lumotlarni himoya qilish bilan uzviy bog‘liq konstitutsiyaviy masaladir. **“Shaxsga doir ma’lumotlar to‘g‘risida”**gi Qonun ma’lumotlarga ishlov berishda qonuniylik, ishonchlilik, mutanosiblik va maxfiylik tamoyillarini belgilaydi, operator esa ma’lumotlarning himoyalan- ganligini ta’minlaydigan huquqiy, tashkiliy va texnik choralarni ko‘rishi lozim[5].

Sud amaliyoti nuqtai nazaridan eng muhim masala shundaki, O‘zbekistonda kiberjinoyatlarning barchasi ham ***Jinoyat kodeksining XX[1] bobidagi*** maxsus tarkiblar bilan qamrab olinmaydi. Haqiqatan ham, 278[2]-modda kompyuter axborotidan ruxsatsiz foydalanishni, 278[4]-modda axborotni noqonuniy modi- fikatsiya qilishni, 278[6]-modda zarar keltiruvchi dasturlarni yaratish yoki tar- qatishni jinoyat deb belgilaydi. Biroq bank kartalaridan pul yechib olish, onlayn kredit rasmiylashtirish, fishing havolalari yuborish yoki jabrlanuvchidan tasdiqlash kodi olish bilan bog‘liq ko‘plab ishlar 168-modda (firibgarlik), 169-modda (o‘g‘irlik) va ayrim hollarda 141[2]-modda (shaxsga doir ma’lumotlar to‘g‘risidagi qonunchilikni buzish) bilan kesishadi[6].Shu ma’noda kiberjinoyat sud amaliyotida mustaqil “texnik” hodisa emas; u **an’anaviy jinoyat-huquqiy kategoriyalarning raqamli muhitdagi yangi ko‘rinishi**dir.

Mahalliy ilmiy adabiyotlar ham aynan shu g‘oyani tasdiqlaydi. B. Elomonov kiberfiribgarlikni raqamli qurilmalar orqali aldash yoki ishonchni suiiste’mol qilish yo‘li bilan mulkiy manfaat ko‘rishga qaratilgan xatti-harakat sifatida izohlaydi va kiberfiribgarlikning klassik firibgarlikdan asosiy farqi vosita va muhitning raqamli tus olganidadir, deya ta’kidlaydi[7]. A.

---

[2] O‘zbekiston Respublikasi Ichki ishlar vazirligi, *“Kiberjinoyatlarni jilovlash orqali xavfsiz kibermakon yaratish, sohada muammolarni bartaraf etish orqali aholining kundalik turmushida uchrayotgan salbiy holatlarni bartaraf etish masalalari”, 2025-yil 7-may.*

[3] IIVning yuqoridagi 2025-yil 7-maydagi rasmiy tahliliy materiali

[4] O‘zbekiston Respublikasi Konstitutsiyasi (2023-yil yangi tahrir)

[5] O‘zbekiston Respublikasining 2019-yil 2-iyuldagi O‘RQ-547-son *“Shaxsga doir ma’lumotlar to‘g‘risida”*gi Qonuni, 5-, 13- va 27[1]-moddalar

[6] O‘zbekiston Respublikasi Jinoyat kodeksi

[7] Elomonov B.A., *Kiber firibgarlik tushunchasi va uning o‘ziga xos xususiyatlar*, *Ilm-fan va innovatsiya ilmiy-amaliy konferensiyasi*, 2023, 5–6-betlar

Muhammadiyev esa huquqiy informatika huquq, axborot va boshqaruv jarayonlari tutashgan fanlararo maydon ekanini, huquqni qo‘llash va sud faoliyatini axborotlashtirish yuridik amaliyot samaradorligini oshirishini qayd etadi[8]. Demak, kiberjinoyat masalasini sud amaliyotida to‘g‘ri hal qilish uchun nafaqat jinoiy norma, balki axborot oqimlari, ma’lumotlar bazalari, elektron izlar va institutsional boshqaruv logikasini ham huquqiy tahlilga qo‘shish talab etiladi.

METHODS (METODLAR)

Mazkur tadqiqot IMRAD strukturasiga muvofiq olib borildi. Biroq **empirik komponent uydirma so‘rovnoma yoki real hayotda o‘tkazilmagan in- tervyularga emas**, ochiq e’lon qilingan normativ va amaliy manbalar korpusining tizimli tahliliga tayandi. Tadqiqot materiali sifatida besh guruh manbalar tanlandi: birinchidan, Konstitutsiya, Jinoyat kodeksi, “Kiberxavfsizlik to‘g‘risida”gi va “Shaxsga doir ma’lumotlar to‘g‘risida”gi qonunlar; ikkinchidan, Oliy sud Plenumining firibgarlik ishlari bo‘yicha tushuntirishlari; uchinchidan, Oliy sudning 2024-yilgi statistik byulleteni; to‘rtinchidan, IIV, Prezi-dent va Markaziy bank e’lon qilgan rasmiy tahliliy ma’lumotlar; beshinchidan, mahalliy va xorijiy ilmiy manbalar.

Nazariy metod sifatida doktrinal tahlil qo‘llanib, “kiberjinoyat”, “kiberfiribgarlik”, “ruxsatsiz kirish”, “elektron dalil” va “shaxsga doir ma’lumotlar” tushunchalari o‘zaro solishtirildi. Normativ-qiyosiy metod orqali O‘zbekiston Jinoyat kodeksining 168, 169, 141^2 va 278^2–278^6-moddalari Buyuk Britaniyaning *Computer Misuse Act 1990* hamda Yevropa Kengashining 2001-yildagi Budapesht konvensiyasi bilan qiyoslandi[9].

Empirik metod sifatida esa **hujjatlar korpusi ustidan kontent-tahlil** qo‘llanildi. Tahlil birliklari sifatida 17 ta asosiy manba tanlandi. Ularning har biriga quyidagi savollar qo‘yildi: 1) qilmish qaysi norma bilan kvalifikatsiya qilinyapti; 2) aldov yoki ishonchni suiiste’mol qilish elementi bormi; 3) ruxsat- siz kirish yoki axborot modifikatsiyasi mavjudmi; 4) shaxsga doir ma’lumotlar jinoyatning vositasi yoki predmeti sifatida namoyon bo‘ladimi; 5) sud amaliy- oti qaysi normativ bo‘shliqni ko‘rsatmoqda. Bu yondashuv “respondentlar kim?” degan savolga aniq javob beradi: mazkur tadqiqotda inson respondentlar emas,

rasmiy hujjatlar, plenum qarorlari, statistik ma’lumotlar va ilmiy matnlarn- ing o‘zi empirik korpus vazifasini bajardi. Ilmiy halollik nuqtai nazaridan aynan shu usul kiberjinoyatlar singari yuqori aniqlik talab qiladigan mavzu uchun eng maqbul deb topildi.

NATIJALAR (RESULTS)

Tahlilning birinchi natijasi shuki, O‘zbekistonda kiberjinoyatlar bo‘yicha sud amaliyotining asosiy markazi texnik vosita emas, **qilmishning yuridik mohiyati**dir. Oliy sud Plenumi “axborot tizimidan, shu jumladan axborot texnologiyalar- idan foydalanib firibgarlik” deganda bank, moliya muassasalari va boshqa subyektlarda bo‘lgan mulkni aldov yo‘li bilan kompyuter texnikasi, aloqa vositalari, planshet va boshqa qurilmalar yordamida manipulyatsiya qilish orqali talon-toroj etishni tushunishini ko‘rsatadi[10].Plenum ayni paytda firibgarlik bilan 169-modda 3-qism “b” bandida nazarda tutilgan ruxsatsiz kirish yo‘li bilan sodir etilgan o‘g‘irlikni farqlashda jabrlanuvchining aldov oqibatida mulkini yoki unga bo‘lgan huquqni aybdorga **ixtiyoriy ravishda** o‘tkazgan-o‘tkazmaganiga qarash zarurligini ta’kidlaydi. Demak, sud amaliyotidagi asosiy kvalifikatsion mezon “texnika qo‘llanildimi?” emas, balki “jabrlanuvchining irodasi aldov bilan burildimi yoki mulk undan yashirincha tortib olindimi?” degan savoldir.

---

[8] Muhammadiyev A.O‘., *Huquqiy informatika*, Toshkent: Alisher Navoiy nomidagi O‘zbek iston Milliy kutubxonasi nashriyoti, 2006, elektron nusxaning 8–9-betlari va 152–153-betlari

[9] United Kingdom, *Computer Misuse Act 1990*; Council of Europe, *Convention on Cybercrime (Budapest Convention), CETS No. 185*

[10] O‘zbekiston Respublikasi Oliy sudi Plenumining 2023-yil 23-iyundagi 17-sonli *“Firibgar- likka oid ishlar bo‘yicha sud amaliyoti to‘g‘risida”*gi qarori, 22-band

Ikkinchidan, kiberjinoyatlarning amaliy massivi moliyaviy sohada to‘plangan. IIV tahliliga ko‘ra, 2024-yilda qayd etilgan kiberjinoyatlarning 98 foizi bank kartalari bilan bog‘liq kiberfiribgarlik va kibero‘g‘irlikka to‘g‘ri keladi. Ularning 60 foizi zararli havola yoki zararli dasturlar yuborish, 16 foizi SMS-kodlarni qo‘lga kiritish, 4 foizi onlayn kredit rasmiylashtirish, 11 foizi marketpleys platformalar orqali aldash, 9 foizi esa boshqa sxemalar hissasiga to‘g‘ri kelgan[11]. Bu natija plenumning firibgarlik va o‘g‘irlikni farqlash haqidagi tushuntirishlari bilan to‘liq uyg‘unlashadi: amaliyotda ko‘plab ishlarning yadro qismi ay- nan aldov mexanizmiga bog‘liq.

Uchinchidan, kiberjinoyatlarni baholashda shaxsga doir ma’lumotlar muammosi periferik masala emas. 2026-yilda shaxsga doir ma’lumotlar bazalar- ini O‘zbekiston hududida saqlash va ularni davlat reyestrida ro‘yxatdan o‘tkazish talablari yanada kuchaytirildi. Bu o‘zgarishlar shuni ko‘rsatadiki, raqamli tajovuzning ilk bosqichi ko‘pincha bevosita ma’lumotni qo‘lga kiritish yoki undan noqonuniy foydalanishdan boshlanadi. Ayni sababli 141[2]-modda bilan 168 va 169-moddalar o‘rtasidagi chegara kelgusida yanada dolzarb bo‘ladi.

To‘rtinchidan, sud-amaliy kontekstni umumiy jinoyat statistikasi bilan o‘qish zarur. Oliy sudning 2024-yilgi byulleteniga ko‘ra, 2024-yilda jami 61 502 nafar shaxs sudlangan, ulardan 2 214 nafari voyaga yetmaganlar bo‘lgan[12]. Jazo turlari tarkibida 20 655 ta ozodlikdan mahrum qilish, 14 644 ta ozodlikni cheklash va 1 080 ta shartli hukm qayd etilgan[13]. Albatta, ochiq byulleten modda-kesimidagi barcha kiberjinoyat hukmlarini alohida jadval ko‘rinishida bermaydi; biroq umumiy statistik fon kiberjinoyatlar jadal ortayotgan bir vaqtda jinoiy siyosatning qaysi instrumentlari faol qo‘llanayotganini ko‘rsatadi.

Beshinchidan, moliyaviy sektor bo‘yicha normativ bazaning o‘zi sud amaliyotiga yangi logika olib kirmoqda. Markaziy bankning 2024-yilda yangilangan nizomida to‘lov tizimi operatorlari va to‘lov xizmatlari yetkazib beruvchilari uchun shubhali frod operatsiyalarini aniqlash, antifrod xizmatini joriy etish, ruxsatsiz kirishga qarshi kamida yiliga ikki marta tekshiruv o‘tkazish, real vaqt rejimida monitoring yuritish kabi talablar belgilangan[14]. ***O‘zbekiston Respublikasi Markaziy banki Boshqaruvining 2026-yil 21-yanvardagi 3759-sonli Nizom*** esa onlayn kredit (mikroqarz) jarayonidagi frod holatlari yuzasidan jabrlanuvchi deb e’tirof etilgan shaxsdan foiz va jarimalarni undirishni to‘xtatish, ayrim hollarda undirib olingan to‘lovlarni sud qarori asosida qaytarish, “***Firibgarlik haqida xabar berish***” bo‘limini joriy etish va bank hamda to‘lov tashkilotlarida antifrod tizimlarini majburiy ishlatishni nazarda tutadi[15]. Bu holat kiberjinoyatlar bo‘yicha sud amaliyotining endifaqat “ayblanuvchi–jabrlanuvchi” chizig‘ida emas, balki “***ayblanuvchi–jabrlanuvchi– moliyaviy operatorning komplayensi***” uchburchagida o‘qilishini ko‘rsatadi.

Quyidagi jadvalda Kiberjinoyatlar va sudlov kontekstining ayrim rasmiy ko‘rsatkichlari:

Ko‘rsatkich	Qiymat	Huquqiy-amaliy xulosa
2019-yilda qayd etilgan kiberjinoyatlar	863 ta	Boshlang’ich taqqoslash nuqtasi
2024-yilda qayd etilgan jinoyatlar	58 800 ta	Kiberjinoyatning ommaviylashgani

[11] O‘zbekiston Respublikasi Ichki ishlar vazirligi, 2025-yil 7-maydagi rasmiy tahliliy material

[12] O‘zbekiston Respublikasi Oliy sudi, *Jinoyat ishlari bo‘yicha sudlarning 2024-yildagi faoliyat yakunlarining asosiy ko‘rsatkichlari*, PDFning 2- va 12-betlari

[13] O‘zbekiston Respublikasi Oliy sudi, *Jinoyat ishlari bo‘yicha sudlarning 2024-yildagi faoliyat yakunlarining asosiy ko‘rsatkichlari*, PDFning 2-, 12- va 15-betlari

[14] O‘zbekiston Respublikasi Markaziy banki boshqaruvining 2024-yil 21-mayda ro‘yxatdan o‘tkazilgan 3513-sonli nizomi, 30-, 33- va 40-boblar

[15] O‘zbekiston Respublikasi Adliya vazirligida 2026-yil 21-yanvarda 3759-son bilan ro‘yxat- dan o‘tgan *“Kredit va to‘lov tashkilotlari, to‘lov tizimi operatorlari tomonidan bank kar- talari, hisobvaraqlar va onlayn kredit (mikroqarz) bilan bog‘liq firibgarlik holatlari nati- jasida yetkazilgan moddiy zararni qoplash tartibi to‘g‘risida”*gi Nizom, 27–31 va 36-bandlar

So'nggi 5 yildagi o'sish	68 barobar	Tergov va sudlar uchun yukning keskin oshgani
2024-yilda umumiy jinoyatchilikdagi ulushi	44.4 %	Raqamli komponent markaziylashgani
Bank kartalari bilan bog'liq ulushi	98%	Asosoiy sud amaliyoti moliyaviy segmentda
Usullar tarkibi	60% havola/dastur; 16% SMS-kod; 4% onlayn kredit; 11% marketpleys; 9% boshqa	Tipik sxemalarni kvalifikatsiya qilish imkonini beradi
2024-yilda jami sudlanganlar	61 502 nafar	Kiber ishlarni umumiy jinoiy siyosat fonida o'qish zarur

Manba: O'zbekiston Respublikasi Ichki ishlar vazirligining 2025-yil 7-maydagi rasmiy tahliliy materiali (2019–2024 yillardagi kiberjinoyatlar dinamikasi va sxemalar tarkibi) hamda O'zbekiston Respublikasi Oliy sudining 2024-yilgi statistik byulleteni, PDFning 2-, 12- va 15-betlari.

Mahalliy ilmiy manbalar natijalarni kuchaytiradi. M. Axmadaliyev kiberx- avfsizlikni faqat texnik muammo sifatida ko'rish yetarli emasligini, u iqtisodiy, huquqiy va tashkiliy omillar bilan chambarchas bog'liqligini ta'kidlaydi[16]. Sh. Muxammatqulov esa kibermuhitda sodir etilayotgan aksariyat mulkiy jinoy atlar kundalik hayotdagi jinoyatlar bilan o'xshash kvalifikatsiyaga ega bo'lsa- da, ulardagi usul va muhitning raqamli xususiyati ularni tergov qilish va is- botlashni tubdan murakkablashtirishini qayd etadi[17]. A. Otajonov va Sh.Nazarov esa kiberjinoyatlarni ikki katta guruhga - **kibertexnologiyalardan foydalanib sodir etiladigan** va **kibertexnologiyalarning o'ziga qarshi qaratilgan** jinoyatlarga ajratish amaliy jihatdan qulay ekanini ko'rsatadi[18].

MUHOKAMA (DISCUSSION)

O'zbekistondagi kiberjinoyatlar manzarasi bir dahshatli haqiqatni ko'rsatmoqda: **endi seyfning eshigi sindirilmayapti, seyf jabrlanuvchining o'zi qo'li bilan ochdirilmoqda**. SMS-kod so'rash, bank xodimi sifatida qo'ng'iroq qilish, fishing havola yuborish, onlayn kreditni masofadan rasmiylashtirish bularning hammasi jinoyatning tashqi texnik ko'rinishlari, xolos. Uning ichki yadro qismi esa jabrlanuvchining irodasini manipulyatsiya qilish, ma'lumotiga egalik qilish va mulkka shunday yo'l bilan erishishdan iborat. Shu bois sud amaliy- otida firibgarlik va o'g'irlik o'rtasidagi chiziqning aniq tortilishi tasodifiy emas; bu chiziqning noto'g'ri chizilishi butun hukmning to'g'riligiga ta'sir qiladi.

Bu yerda yana bir nozik, ammo hayratlanarli muammo mavjud: kiberjinoyatda dalil juda ko'p, biroq u ayni paytda nihoyatda mo'rt. IP-manzil, log-fayl, tranzaksiya tarixi, mobil qurilma identifikatori, biometrik tasdiqlash izi, chat yozishmalari - bularning hammasi jinoyatning elektron soyasidir. Lekin soyani ushlash qanchalik qiyin bo'lsa, elektron dalilni protsessual jihatdan "***qotirib qo'yish***" ham shunchalik mushkul**. Budapesht konvensiyasi 15-moddasi** cybercrime protseduralari inson huquqlari va erkinliklari, jumladan mutanosiblik tamoyiliga bo'ysunishi shartligini belgilaydi[19]. Shunday ekan, **kuchli dalil faqat topilgan dalil emas, qonuniy topilgan dalildir**. Bu fikr O'zbekiston sharoitida ayniqsa muhim, chunki raqamli izni saqlab qolish tezkorlikni talab etsa, konstitutsiyaviy kafolatlar, mutanosiblik va nazoratni talab qiladi.

[16] Axmadaliyev M.E., *Raqamli iqtisodiyotda kiberxavfsizlik muammolari va ularning xalqaro boshqaruv mexanizmlari*, *Oriental Renaissance: Innovative, Educational, Natural and So- cial Sciences*, 2025, 69–71-betlar

[17] Muxammatqulov Sh.E., *Kiberjinoyatchilik va unga qarshi kurashish bo'yicha normativ- huquqiy hujjatlar tahlili*, 2023, 84–85-betlar

[18] Otajonov A.A., Nazarov Sh.O'., *Kiberjinoyatchilik tushunchasi, turlari va unga qarshi kurashishning huquqiy choralari*, *Journal of Modern Development*, 2026, 76–77-betlar

[19] Council of Europe, *Convention on Cybercrime*

Muhokamaning uchinchi yo‘nalishi — ***institutsional mas’uliyat***. 2026-yil mart oyidagi prezident taqdimotida uchta bank tizimidagi zaiflik oqibatida 3 025 nafar fuqaroga 17 milliard so‘m zarar yetgani qayd etildi va operatorlar hamda to‘lov tashkilotlarining kiberxavfsizlik talablariga rioya etmagan hollarda mod- diy javobgarligini kuchaytirish zarurligi ta’kidlandi[20]. Bu juda muhim buril- ishdir: kiberjinoyat endi faqat jinoyatchining shaxsiy chaqqonligiga bog‘liq hodisa sifatida emas, balki **institutsional zaifliklar bilan oziqlanadigan tizimli xavf** sifatida ko‘rilmoqda. Agar bank foydalanuvchini yetarli darajada identifikatsiya qilmasa, shubhali tranzaksiyani real vaqt rejimida ushlamasa yoki antifrod signalini inkor etsa, unda zarar faqat jinoiy hujumdan emas, balki boshqaruv xatosidan ham tug‘iladi.

Mahalliy ilmiy adabiyotda ham shunga yaqin fikrlar uchraydi. Axmadaliyev davlat-xususiy sektor hamkorligi va raqamli madaniyatni oshirmasdan turib, kiberxavfsizlik siyosati to‘liq ishlamasligini ko‘rsatadi[21]. Muhammadiyevning fanlararo yondashuvi esa huquqiy informatika yuridik faoliyat samaradorligini oshirish uchun axborot tizimlarini tartibli boshqarish zarurligini oldindan sez ganini ko‘rsatadi[22]. Shunday qilib, doktrina ham, normativ baza ham, rasmiy statistika ham bitta xulosaga olib keladi: **kiberjinoyatga qarshi kurashish sud binosidan ancha oldin-ma’lumotni himoyalash, tranzaksiyani tekshirish va raqamli savodxonlikni oshirish bosqichida boshlanadi**.

Mazkur tahlildan kelib chiqib, qonunchilik va amaliyot uchun to‘rtta taklif ilgari suriladi.

Birinchidan, axborot texnologiyalaridan foydalanib sodir etiladigan jinoyat- larni normativ jihatdan **cyber-dependent** va **cyber-enabled** toifalarga ajratish maqsadga muvofiq. Bugungi amaliyotda bu farq plenum qarorlari va huquqni qo‘llash amaliyotida bilvosita mavjud, biroq qonun matnida aniq algoritm shak- lida ifodalanmagan. Bunday yondashuv 168, 169, 141^2 va 278-moddalar o‘rtasidagi chegara masalalarini sezilarli aniqlashtiradi.

Ikkinchidan, Jinoyat-protsessual kodeksiga **elektron dalillar bo‘yicha maxsus bob** kiritilishi lozim. Unda elektron tashuvchini ko‘zdan kechirish, nusxalash, xesh-kod bilan tasdiqlash, trafik ma’lumotlarini tezkor saqlab qolish, bulutli ma’lumotni talab qilish va chain of custody talablarini alohida belgilash zarur. Aks holda amaliyot elektron dalilni yig‘ishda bir xilda shakllanmaydi va sudlarning maqbullik bahosi bir xil bo‘lmay qoladi.

Uchinchidan, banklar va to‘lov tashkilotlari uchun **zararni taqsimlashning aralash modeli** huquqiy jihatdan mustahkamlanishi kerak. 3759-sonli Nizom va prezident yig‘ilishidagi ko‘rsatmalar mazkur yo‘nalishda muhim qadam bo‘ldi, ammo bu qoidalar maxsus qonun yoki kodeks darajasida mustahkamlanmasa, sud amaliyotida bir xil standart shakllanmaydi.

To‘rtinchidan, “***drop***” shaxslar, ya’ni o‘z karta, SIM-karta, akkaunt yoki hisobvaraqlarini kiberjinoyat zanjirida vositachilik uchun taqdim etgan shaxslar bo‘yicha **differensial javobgarlik modeli** joriy etilishi kerak. Chunki kiberjinoyat amaliyotida asosiy ijrochi ko‘pincha ko‘rinmaydi, ammo moliyaviy izlar aynan shu vositachilar orqali aylanadi. Ularning roli bexabar yordamchimi, beparvo foydalanuvchimi yoki uyushgan tarmoq ishtirokchisimi - ana shu farq jazo siyosatida aks etishi shart.

XULOSA

O‘zbekistonda kiberjinoyatlar bo‘yicha sud amaliyoti bugun jinoiy adliyaning chekka bo‘g‘ini emas, balki **eng markaziy frontlaridan biri**ga aylandi. Rasmiy statistikalar kiberjinoyatlar soni va ulushining portlovchi o‘sishini ko‘rsatmoqda; plenum qarorlari esa firibgarlik, o‘g‘irlik, ruxsatsiz kirish va shaxsga doir ma’lu- motlar buzilishi o‘rtasidagi nozik chegaralarni amaliy jihatdan belgilab bermoqda. Tadqiqot shuni ko‘rsatdiki, milliy sud amaliyotida “**kiberjinoyat**” tushunchasi faqat maxsus texnik tarkiblar doirasida emas, balki an’anaviy jinoyat huquqiy kategoriyalarning raqamli transformatsiyasi sifatida yashaydi.

---

[20] O‘zbekiston Respublikasi Prezidenti huzuridagi 2026-yil 12-martdagi yig‘ilish axboroti

[21] Axmadaliyev M.E., ko‘rsatilgan asar, 71-bet

[22] Muhammadiyev A.O‘., ko‘rsatilgan darslik, elektron nusxaning 8–9-betlari

Maqolaning asosiy ilmiy xulosasi shundan iboratki, O‘zbekistonda kiberji- noyatni samarali huquqiy boshqarish uchun uchta tayanch birlashtirilishi zarur: birinchisi - **aniq kvalifikatsiya**; ikkinchisi - **qonuniy va ishonchli elektron dalil**; uchinchisi - **institutsional antifrod va ma’lumot himoyasi rejimi**.Shu uch omil uyg‘unlashgan taqdirdagina kiberjinoyatlarga qarshi kurashish amaliyoti jazolovchi tizimdan oldini oluvchi, himoya qiluvchi va tiklovchi tizimga aylanadi. Aks holda jinoyatchi bir qadam oldinda, huquq esa bir qadam ortda qolaveradi.

FOYDALANILGAN ADABIYOTLAR RO‘YXATI:

1. O‘zbekiston Respublikasi Konstitutsiyasi. https://lex.uz/acts/-20596.
2. O‘zbekiston Respublikasi Jinoyat kodeksi. https://lex.uz/uz/docs/-111453.
3. O‘zbekiston Respublikasining 2022-yil 15-apreldagi O‘RQ-764-son “Kiberx- avfsizlik to‘g‘risida”gi Qonuni. https://lex.uz/acts/-5960604 .
4. O‘zbekiston Respublikasining 2019-yil 2-iyuldagi O‘RQ-547-son “Shaxsga doir ma’lumotlar to‘g‘risida”gi Qonuni. https://lex.uz/docs/-4396419.
5. O‘zbekiston Respublikasi Oliy sudi Plenumining 2023-yil 23-iyundagi 17- sonli “Firibgarlikka oid ishlar bo‘yicha sud amaliyoti to‘g‘risida”gi qarori. https://lex.uz/docs/-6523582.
6. O‘zbekiston Respublikasi Oliy sudi. Jinoyat ishlari bo‘yicha sudlarning 2024- yildagi faoliyat yakunlarining asosiy ko‘rsatkichlari. https://stat.sud.uz/ assets/uploads/criminal/pdf/criminal-2024-full.pdf
7. O‘zbekiston Respublikasi Ichki ishlar vazirligi. Kiberjinoyatlarni jilovlash orqali xavfsiz kibermakon yaratish..., 2025-yil 7-may. https://gov.uz/oz/ iiv/news/view/52319
8. O‘zbekiston Respublikasi Markaziy banki boshqaruvining 3513-sonli nizomi. https://lex.uz/docs/-6933268.
9. 2026-yil 21-yanvarda 3759-son bilan ro‘yxatdan o‘tgan onlayn kredit va bank kartalari bilan bog‘liq frod holatlarida moddiy zararni qoplash tartibi to‘g‘risidagi Nizom. https://lex.uz/docs/8007760.
10. O‘zbekiston Respublikasi Prezidentining 2026-yil 12-martdagi yig‘ilishi axboroti. https://president.uz/oz/lists/view/9009.
11. Council of Europe. Convention on Cybercrime (Budapest Convention), CETS No. 185. https://www.coe.int/en/web/conventions/full-list?module= treaty-detail&treatynum=185.
12. United Kingdom. Computer Misuse Act 1990.https://www.legislation. gov.uk/ukpga/1990/18/contents.
13. Elomonov B.A. Kiber firibgarlik tushunchasi va uning o‘ziga xos xususiy- atlar. Ilm-fan va innovatsiya ilmiy-amaliy konferensiyasi, 2023. https://in-academy.uz/index.php/si/article/download/17677/12223/15703.
14. Muxammatqulov Sh.E. Kiberjinoyatchilik va unga qarshi kurashish bo‘yicha normativ-huquqiy hujjatlar tahlili. 2023. https://in-academy.uz/index.php/ zdit/article/download/19073/13054.
15. Axmadaliyev M.E. Raqamli iqtisodiyotda kiberxavfsizlik muammolari va ularning xalqaro boshqaruv mexanizmlari. Oriental Renaissance, 2025. https://oriens.uz/media/journalarticles/12_Axmadaliyev_Mansurbek_Erkaboy_ ogli_64-75.pdf.
16. Otajonov A.A., Nazarov Sh.O‘. Kiberjinoyatchilik tushunchasi, turlari va unga qarshi kurashishning huquqiy choralari. Journal of Modern Develop- ment, 2026. https://journalss.org/index.php/mod/article/download/18651/17932.
17. Muhammadiyev A.O‘. Huquqiy informatika. Toshkent: Alisher Navoiy no- midagi O‘zbekiston Milliy kutubxonasi nashriyoti, 2006. https://kutubxona. adpi.uz/preview?filename=huquqiyinformatika.pdf.