YANGI O‘ZBEKISTON, YANGI TADQIQOTLAR JURNALI
Volume 5 Issue 7 Noyabr 2026
https://phoenixpublication.net/ Online ISSN: 3030-3494

MOLIYAVIY KIBERJINOYATLARNING TURLARI, AMALGA OSHIRISHNING USULLARI VA ULARGA QARSHI KURASHISHNING HUQUQIY ASOSLARI

Salomova Ruxshona Rasul qizi
Toshkent davlat yuridik universiteti Huquq va texnologiyalar sho`basi
Kiber huquqi yo`nalishi magistranti

Annotatsiya. *Maqolada moliyaviy kiberjinoyatlarning mazmuni, turlari va sodir etilish usullari tahlil qilingan. O‘zbekiston Respublikasi Ichki ishlar vazirligi, AQSh Federal qidiruv byurosi va Buyuk Britaniya bank sektori statistikasi asosida jinoyatchilik dinamikasi ko‘rsatib berilgan. O‘zbekistonning Jinoyat kodeksi, “Kiberxavfsizlik to‘g‘risida”gi qonuni, 2025–2026-yillarda qabul qilingan Prezident hujjatlari hamda Budapesht va Xanoy konvensiyalari, Yevropa Ittifoqi, AQSh va Qozog‘iston qonunchiligi qiyosiy o‘rganilgan. Tadqiqot natijasida milliy qonunchilikdagi bo‘shliqlar aniqlanib, “dropper”lik uchun javobgarlik, bank va to‘lov tashkilotlarining zararni qoplash majburiyati hamda xalqaro hamkorlikni kengaytirish bo‘yicha takliflar ishlab chiqilgan.*

Kalit so‘zlar: *moliyaviy kiberjinoyat, firibgarlik, fishing, ijtimoiy muhandislik, dropper, antifrod tizimi, kiberxavfsizlik, Budapesht konvensiyasi.*

Аннотация: *В статье анализируются сущность, виды и способы совершения финансовых киберпреступлений. На основе статистики Министерства внутренних дел Республики Узбекистан, ФБР США и банковского сектора Великобритании показана их динамика. Также рассмотрены Уголовный кодекс РУз, Закон “О кибербезопасности”, президентские акты 2025-2026 годов, а также Будапештская и Ханойская конвенции, законодательство Европейского Союза, США, России и Казахстана. В результате исследования выявлены пробелы в национальном законодательстве и выработаны предложения по установлению ответственности за “дропперство”, обязательству банков и платежных организаций возмещать ущерб, а также по расширению международного сотрудничества.*

Ключевые слова: *финансовое киберпреступление, мошенничество, фишинг, социальная инженерия, дроппер, антифрод-система, кибербезопасность, Будапештская конвенция.*

Abstract. *This article examines the essence, types and methods of committing financial cybercrimes. Based on statistics from the Ministry of Internal Affairs of the Republic of Uzbekistan, the US Federal Bureau of Investigation (FBI), and the UK banking sector, the dynamics of cybercrime are demonstrated. The Criminal Code of Uzbekistan, the law “On*

Cybersecurity," Presidential decrees adopted in 2025-2026, as well as the Budapest and Hanoi Conventions, and the legislation of the European Union, the USA, and Kazakhstan are comparatively analyzed. As a result of the research, gaps in national legislation have been identified, and proposals have been developed regarding liability for "money mule activity" (dropper activity), the obligation of banks and payment organizations to compensate for damages, and the expansion of international cooperation.

Keywords: *financial cybercrime, fraud, phishing, social engineering, money mule(dropper), anti-fraud system, cybersecurity, Budapesht Convention*

Raqamlashuv jinoyatchilikni ham onlayn muhitga ko`chirmoqda. Moliyaviy xizmatlar raqamlashgani sari jinoyatchilik ham shu muhitga ko‘chmoqda. O‘zbekistonda bu jarayon ayniqsa keskin kechdi. Xususan, 2019-yilda 18 turdagi 863 ta kiberjinoyat qayd etilgan bo‘lsa, 2024-yilda ularning soni 62 turda 58 800 taga yetdi, ya’ni besh yilda 68 baravar oshdi. Shu davrda kiberjinoyatlarning barcha jinoyatlardagi ulushi 6,2 foizdan 44,4 foizga ko‘tarildi[125]. 2025-yilda fuqarolardan kiberjinoyat yo‘li bilan qariyb 1,9 trln so‘m o‘g‘irlangan.[126] Muammo faqat O‘zbekistonga xos emas. AQSh Federal qidiruv byurosining Internet jinoyatlari bilan ishlash markazi (IC3) 2025-yilda 1 008 597 ta shikoyat qabul qilgan, e’lon qilingan zarar esa 20,877 mlrd dollarni tashkil etib, bir yilda 26 foizga o‘sgan[127]. Demak, moliyaviy kiberjinoyat global hodisa bo‘lib, unga qarshi kurash ham milliy, ham xalqaro huquqiy vositalarni talab qiladi.

O‘zbekistonda so‘nggi ikki yilda bu sohada qator hujjatlar qabul qilindi: Prezidentning 2025-yil 30-apreldagi PQ-153-son qarori, 2026–2030-yillarga mo‘ljallangan Kiberxavfsizlik strategiyasini tasdiqlagan PF-38-son farmon, kiberjinoyatchilikka qarshi kurashish bo‘yicha qonun loyihalari. Ichki ishlar vazirligi tizimida 2026-yil "Kiberjinoyatchilikka qarshi kurash yili" deb e’lon qilingan. Shunga qaramay, kiberjinoyatlarning ochilish darajasi pastligicha qolmoqda.

Moliyaviy kiberjinoyat bu - raqamli moliyaviy texnologiyalar, to`lov ilovalari, onlayn banking va kriptoaktivlar orqali sodir etiladigan noqonuniy harakatlardir. Ammo O‘zbekiston qonunchiligida "moliyaviy kiberjinoyat" atamasi alohida ta’riflanmagan. "Kiberxavfsizlik to‘g‘risida"gi O‘RQ-764-son qonunning 3-moddasi kiberjinoyatni kiberkenglikda dasturiy ta’minotdan foydalanib, axborotni egallash, o‘zgartirish, yo‘q qilish yoki axborot tizimlari va resurslarini [128]ishdan chiqarish maqsadida sodir etiladigan jinoyatlar majmui sifatida

[125] O‘zbekiston Respublikasi Ichki ishlar vazirligi matbuot xizmati ma’lumoti Kun.uz, 2025-yil 29-may
[126] Spot.uz, 2026-yil 27-yanvar. Prezident raisligidagi videoselektor yig‘ilishi materiallari
[127] Federal Bureau of Investigation. Internet Crime Complaint Center (IC3). 2025 Internet Crime Report
[128] O‘zbekiston Respublikasining 2022-yil 15-apreldagi O‘RQ-764-son «Kiberxavfsizlik to‘g‘risida»gi qonuni

belgilaydi. Bu ta’rif axborotning o‘ziga qarshi qaratilgan qilmishlarni qamraydi, ammo pul mablag‘larini egallashni bevosita nomlamaydi. Xalqaro huquqda bu yondashuv kengroq tavsiflanadi. Budapesht konvensiyasining 7 va 8-moddalari kompyuter bilan bog‘liq qalbakilashtirish va firibgarlikni alohida tarkib sifatida ajratadi.[129] BMTning 2024-yil 24-dekabrda Bosh Assambleya tomonidan qabul qilingan Kiberjinoyatchilikka qarshi konvensiyasi ham axborot-kommunikatsiya texnologiyalari yordamida sodir etilgan firibgarlik va o‘g‘rilikni o‘z doirasiga kiritgan[130].

Hozirgi kunga kelib moliyaviy kiberjinoyatlarning bir necha turlari va sodir etilish usullari mavjud. Ichki ishlar vazirligi ma’lumotlariga ko‘ra, O‘zbekistonda 2024-yilda sodir etilgan kiberjinoyatlarning 98 foizi bank kartalari bilan bog‘liq bo‘lgan.

Usul	Ulushi %	Mazmuni
Zararli havola va dastur orqali karta yoki qurilmani egallash	60	Ijtimoiy tarmoqlarda APK fayl yuborish, telefonni masofadan boshqarish
SMS kod orqali qurilmani qo`lga kiritish	16	Bank xodimi yoki davlat organi nomidan qo`ng`iroq qilib(vishing), SMS kodni olish
Onlayn va savdo platformalarida aldash	11	Oldindan to`lovni olib tovarni yetkazmaslik
Turli sxemalar orqali mablag` jalb etish	9	Soxta investitsiya platformalari, moliyaviy piramidalar
Fuqaro nomiga onlayn kredit olish	4	Shaxsga doir ma`lumotlarni o`g`irlab, mikroqarz rasmiylashtirish

Ilmiy adabiyotlarda va xorij amaliyotida moliyaviy kiberjinoyatlar quyidagi asosiy turlarga ajratiladi:

- To‘lov kartalari va hisobvaraqlarga ruxsatsiz kirish – fishing, zararli dasturlar, SIM-kartani almashtirish (SIM-swap) orqali.

[129] Convention on Cybercrime
[130] United Nations Convention against Cybercrime

- Ijtimoiy muhandislikka asoslangan firibgarlik – jabrlanuvchi o‘zi pul o‘tkazadi (inglizcha “authorised push payment”, APP). Bunda texnik himoya emas, inson ishonchi buziladi.

- Investitsion va kripto firibgarlik - yuqori daromad va’da qiluvchi soxta platformalar.

- Biznes elektron pochtasini buzish (BEC) - kompaniya rahbari yoki hamkori nomidan soxta to‘lov topshirig‘i.

- To‘lov va bank infratuzilmasiga hujumlar - to‘lov talab qiluvchi dastur hujumlari (ransomware), tizim zaifliklaridan foydalanish.

- Mablag‘larni legallashtirish - “dropper”lar, ya’ni o‘z kartasi yoki hisobvarag‘ini jinoyatchilarga beruvchi shaxslar orqali pulni yashirish.

O‘zbekiston uchun xos jihat shundaki, hozirgi kunlarda jinoyatlarning ko`pchiligi transchegaraviy xarakterga ega. IIV ma’lumotlariga ko‘ra, kiberjinoyatlarning 90 foizi xorijdan turib sodir etilmoqda. 2026-yil mart oyida e’lon qilingan ma’lumotlarga ko‘ra, so‘nggi bir yilda firibgarliklarning 82 foizi va o‘g‘riliklarning 76 foizi onlayn tarzda sodir etilgan. Uchta bank tizimidagi zaiflik tufayli 3 025 nafar mijoz 17 mlrd so‘m zarar ko‘rgan.[131]

Xorijiy ma’lumotlar muammoning global miqyosini ko‘rsatadi. AQShda 2025-yilda investitsion jinoyatlardan zarar 8,6 mlrd dollardan, shu jumladan kripto-investitsion firibgarlikdan 7,2 mlrd dollardan oshgan. BEC hujumlaridan zarar 3 mlrd dollarga yaqin bo‘lgan, fishing esa barcha shikoyatlarning qariyb beshdan birini tashkil etgan. Buyuk Britaniyada 2024-yilda firibgarlik orqali 1,17 mlrd funt sterling o‘g‘irlangan. Shundan 722 mln funt ruxsatsiz operatsiyalarga, 450,7 mln funt APP firibgarligiga to‘g‘ri keladi. APP holatlarining 70 foizi onlayn platformalarda boshlangan. Banklar esa urinilgan har 1 funtlik ruxsatsiz firibgarlikdan 67 pensini to‘xtatib qolgan.[132]

Bugungi kunda O`zbekiston Respublikasida moliyaviy kiberjinoyatlarning oldinini olish va ularga qarshi kurashish bilan bog`liq ijtimoiy munosabatlar bir qator normativ-huquqiy hujjatlar bilan tartibga solingan. Xususan, mazkur sohadagi huquqiy munosabatlarni tartibga solishga qaratilgan quyidagi qonunchilik normalarini ko`rsatish mumkin:

Moliyaviy kiberjinoyatlar asosan mulkka qarshi jinoyatlar sifatida kvalifikatsiya qilinadi. Jinoyat kodeksining 168-moddasi (firibgarlik) va 169-moddasi (o‘g‘rilik) kompyuter texnikasi vositalaridan foydalanish yoki kompyuter tizimiga ruxsatsiz kirish yoki undan foydalanishni og‘irlashtiruvchi belgi sifatida nazarda tutadi[133]. Bundan tashqari, 2007-yil 26-

[131] Advice.uz, 2026-yil 13-mart.
[132] UK Finance. Annual Fraud Report 2025. Press-reliz
[133] lex.uz/docs/111457.

dekabrdagi qonun bilan Kodeksga “Axborot texnologiyalari sohasidagi jinoyatlar” bobi kiritilgan[134]. Dastlan unda yettita tarkib bor edi:

- 278¹-modda - Axborotlashtirish qoidalarini buzish;
- 278²-modda - Kompyuter axborotidan qonunga xilof (ruxsatsiz) foydalanish;
- 278³-modda - Kompyuter tizimidan, shuningdek telekommunikatsiya tarmoqlaridan qonunga xilof ravishda (ruxsatsiz) foydalanish uchun maxsus vositalarni o‘tkazish maqsadini ko‘zlab tayyorlash yoxud o‘tkazish va tarqatish
- 278⁴-modda - Kompyuter axborotini modifikatsiyalash;
- 278⁵-modda - Kompyuter sabotaji;
- 278⁶-modda - Zarar keltiruvchi dasturlarni yaratish, ishlatish yoki tarqatish;
- 278⁷-modda - Telekommunikatsiya tarmog‘idan qonunga xilof ravishda (ruxsatsiz)foydalanish.

2024-yil 19-yanvardagi O‘RQ-899-son qonun bu tizimni kengaytirdi. Tovlamachilik (165-modda) tarkibiga jabrlanuvchining axborot resurslarini yo‘q qilish, o‘zgartirish, egallash yoki bloklash bilan qo‘rqitish qo‘shildi. Kodeksga “Kriptoaktivlar aylanmasi sohasidagi qonunchilikni buzish” (278⁸-modda) va “Mayning faoliyatini qonunga xilof ravishda amalga oshirish” (278⁹-modda) uchun javobgarlik kiritildi. Ma’muriy javobgarlik to‘g‘risidagi kodeksga “Mobil qurilmaning xalqaro o‘ziga xos identifikatsiya kodini yoki abonent qurilmasining identifikatsiyalash modulini qonunga xilof ravishda uchun o`zgartirish 155³-modda qo‘shildi[135]. Shuningdek, “Kiberxavfsizlik to‘g‘risida”gi qonunga asosan Davlat xavfsizlik xizmatini kiberxavfsizlik sohasidagi vakolatli organ etib belgilagan (11-modda) va muhim axborot infratuzilmasi obyektlarini himoya qilish talablarini belgilab berilgan. O`zbekiston Respublikasi Prezidenti tomonidan 2025-2026 yillarda bir qancha islohotlar amalga oshirildi. Prezidentning 2025-yil 30-apreldagi PQ-153-son qarori sohada burilish yasadi. Unga ko‘ra:

- Ichki ishlar vazirligi kiberjinoyatchilikka qarshi kurashish bo‘yicha vakolatli organ etib belgilandi;
- o‘z bank kartasi, hisobvarag‘i, SIM-kartasi hamda elektron hamyonini kiberjinoyat sodir etish uchun boshqalarga berganlik uchun ma’muriy va jinoiy javobgarlik joriy etilishi belgilandi;
- kiberxavfsizlik talablarini bajarmagan bank va to‘lov tashkilotlari mijozlarga yetkazilgan moddiy zararni o‘z hisobidan qoplashi ko‘zda tutildi;

[134] UzA. Jinoyat kodeksining XX¹ bobi «Axborot texnologiyalari sohasidagi jinoyatlar», 2007-yil 26-dekabr
[135] O‘zbekiston Respublikasining 2024-yil 19-yanvardagi O‘RQ-899-son qonuni

- eng ko‘p kiberjinoyat qayd etilgan bank va to‘lov tashkilotlari ro‘yxatini har oy e’lon qilish, Markaziy bankda markazlashgan antifrod tizimini 2025-yil 1-sentabrgacha yaratish vazifasi qo‘yildi;

- jinoyatni axborot texnologiyalari yordamida sodir etish jazoni og‘irlashtiruvchi holat sifatida belgilanishi nazarda tutildi.

Prezidentning 2026-yil 10-martdagi PF-38-son farmoni bilan 2026–2030-yillarga mo‘ljallangan Kiberxavfsizlik strategiyasi tasdiqlandi. Strategiyada kiberjinoyatlar uchun jinoiy va ma’muriy javobgarlikni kuchaytirish, fishingga qarshi platforma yaratish, shubhali qo‘ng‘iroqlarni aniqlash va bloklash, banklarga antifrod talablarini qo‘yish vazifalari belgilangan. Kiberxavfsizlik va kiberjinoyatchilikka qarshi kurashish bo‘yicha milliy muvofiqlashtiruvchi kengash tuziladigan bo‘ldi. Nihoyat, kiberjinoyatchilikka qarshi kurashish bo‘yicha ikki qonun loyihasi 2026-yil 28-aprelda Qonunchilik palatasida birinchi o‘qishda qabul qilinib, 22-iyulda Senatga yuborildi[136]. Loyihalarda banklarning shubhali operatsiyalarni o‘z vaqtida aniqlash va zararni qoplash majburiyati, jabrlanuvchilarga yordam ko‘rsatish, elektron dalillarni olish tartibi hamda sud nazorati ostida bank hisobvaraqlari, elektron hamyon va kriptoaktivlar bo‘yicha operatsiyalarni vaqtincha to‘xtatish choralari nazarda tutilgan.

Shuningdek, sud amaliyotining tahlili shun ko`rsatmoqdaki, moliyaviy kiberjinoyatlar va dropperlik bilan bog`liq ishlar shaxsga doir ma`lumotlar xavfsizligini to`liq ta`minlanmaganligi yuzasidan ham kelib chiqmoqda. Xususan, Farg‘ona va Toshkent shaharlarida ijaraga olingan xonalarda "kol-markaz" tashkil etgan 34 kishilik uyushgan jinoiy guruh 70 mingdan ortiq fuqarolarning ma`lumotlar bazasini noqonuniy qo‘lga kiritib, asosan keksalar va nochor insonlarning ishonchiga kirish orqali yirik transchegaraviy moliyaviy jinoyatni amalga oshirdi. Operatorlar SIP-telefoniya ilovalari orqali o‘zlarini bank hamda huquq-tartibot organlari xodimlari deb tanishtirib, soxta dori vositalari uchun kompensatsiya va’da qilgan hamda “soliq” bahonasida jabrlanuvchilardan 9,5 million rubldan ortiq (taxminan 124 ming dollar) mablag‘ni firibgarlik yo‘li bilan undirib, 470 ming dollarlik litsenziyasiz kripto-operatsiyalarni bajargan. Yozyovon tuman jinoyat ishlari bo‘yicha sudi ushbu ayyorona tuzoqqa chek qo‘yib, jinoiy guruhning 21 nafar a'zosiga 3 yil 6 oydan 9 yil 6 oygacha bo‘lgan ozodlikdan mahrum qilish jazosini tayinladi.

Huquqiy nuqtai nazardan ushbu ish kiberjinoyatchilikning ko‘p qirrali va xavfli mohiyatini ochiq ko‘rsatadi, sud qilmishni shunchaki odatiy firibgarlik (168-modda) emas, balki daromadlarni legallashtirish (243-modda), telekommunikatsiya tarmog`idan qonunga xilof ravishda (ruxsatsiz) kirish (278[7]-modda) hamda kripto-aktivlar aylanmasi sohasidagi

[136] Spot.uz, 2026-yil 22-iyul

qonunchilikni buzish (278[8]-modda) kabi alohida jinoyatlar majmui sifatida to‘g‘ri kvalifikatsiya qildi. Bu holat jinoyatchilarning pul izini yashirish uchun “drop” kartalar va kripto-hamyonlardan foydalanganini hamda jabrlanuvchilar xorijda joylashgani sababli yetkazilgan zararni qaytarish amalda murakkabligini namoyon etadi. Shuning uchun ushbu ish muhim saboq beradi ya`ni kiberjinoyatlarga qarshi kurashishda faqat qat'iy jazo choralariga tayanib qolmay, shaxsiy ma'lumotlar himoyasi, bank monitoringi va aholining ijtimoiy muhandislik tuzoqlaridan ogohligini oshirish hal qiluvchi ahamiyatga egadir[137]

Moliyaviy kiberjinoyatchilikka qarshi kurashish mexanizmlarini takomillashtirishda xalqaro standartlar va ilg`or xorijiy tajribani o`rganish muhim ahamiyat kasb etadi. Xususan, Yevropa Ittifoqi va xalqaro tashkilotlarning bu boradagi huquqiy yondashuvlarini O`zbekiston Respublikasining milliy qonunchiligi bilan qiyosiy tahlil qilish mavjud bo`shliqlarni aniqlash hamda samarali chora-tadbirlarni ishlab chiqish imkonini beradi.Quyidagi jadvalda xalqaro va Yevropa darajasidagi asosiy hujjatlar hamda ularning tartibga solish mexanizmlari keltirilgan:

T/r	Davlat/Tashkilot	Asosiy hujjat	Yechim
1	Yevropa Kengashi	Budapesht konvensiyasi (2001) 2-qo`shimcha protokoli (2022)	Elektron dalillar bo`yicha tezkor hamkorlikni amalga oshiradi.
2	BMT	Kiberjinoyatchilikka qarshi konvensiya (2024)	2025-yil oktabrda Xanoyda 72davlat imzolagan; kuchga kirmagan
3	Yevropa Ittifoqi	2019/713-son direktiva PSD2 (2015/2366)	Naqd pulsiz to‘lov firibgarligini jinoyat deb belgilaydi va kuchli autentifikatsiya, mijoz javobgarligini cheklashni joriy etgan
4	AQSH	18 U.S.C. §1030 (CFAA), §1343; Elektron pul o‘tkazmalari to‘g‘risidagi qonun	Kompyuter tizimlariga ruxsatsiz kirish hamda elektron pul o‘tkazmalari orqali sodir etiladigan firibgarlik uchun qat’iy federal jinoiy javobgarlikni belgilaydi. Shuningdek,

[137] https://anhor.uz/uzl/news/34-jinoiy-guruh

			iste'molchilarning huquqlarini himoya qilish va moliyaviy javobgarlik chegaralarini tartibga soladi.
5	Qozog`iston	JK 232[1]-modda (2025-yil 16-sentabrdan)	Kiberfiribgarlik sxemalarida vositachilik qilish (dropperlik) hamda bank kartalari va hisob varaqalarini noqonuniy o`tkazishni alohida jinoyat sifatida belgilab, mol-mulkni musodara qilgan holda 7 yilgacha ozodlikdan mahrum qilish jazosini joriy etgan.
5	Buyuk Britaniya	Computer Misuse Act (1990):APP firibgarligi uchun majburiy kompensatsiya qoidalati (PSR,2024-yil 7-oktaybr	85 000 funt sterliggacha zararni majburiy qoplaydi, xarajatni yuboruvch va qabul qiluvchi banklar o`rtasida 50/50 nisbatda taqsimlash orqali “dropper”hisoblarini nazorat qiladi va antifrod tizimini kuchaytiradi.

Yuqoridagi xalqaro hujjatlar va xorijiy davlatlar tajribasini o‘zaro qiyoslaganda, Buyuk Britaniya modeli amaliy natijadorlik nuqtayi nazaridan eng yuqori samaradorlikni ko‘rsatganini alohida ta’kidlash lozim. Xususan, majburiy kompensatsiya mexanizmi joriy etilgach, dastlabki bir yil ichida (2024-yil oktabr -2025-yil iyun) APP firibgarligidan ko‘rilgan zararning 88 foizi (ilgari bu ko‘rsatkich 66 foiz edi) jabrlanuvchilarga qaytarilib, jami 112 mln funt sterling miqdoridagi mablag‘ qoplab berilgan. Bu yondashuv nafaqat fuqarolar huquqlarini real himoya qildi, balki banklarni ham antifrod tizimlariga faol sarmoya kiritishga iqtisodiy jihatdan rag‘batlantirdi.[138]

Olingan natijalar O‘zbekistonda moliyaviy kiberjinoyatga qarshi kurashning huquqiy bazasi so‘nggi ikki yilda sezilarli darajada yangilanganini ko‘rsatadi. Biroq qonunchilik hali ham jinoyatchilik sur’atidan orqada qolmoqda. Fikrimcha, buning bir nechta sababi bor.

[138] A&O Shearman FinReg, 2025-yil 8-oktabr

Birinchidan, tushunchaviy apparat to‘liq shakllanmagan. Kriminologiyada kiberjinoyatlar odatda ikki guruhga ajratiladi: faqat kompyuter muhitida mavjud bo‘ladigan jinoyatlar (cyber-dependent) va an’anaviy jinoyatning texnologiya yordamida sodir etiladigan shakllari (cyber-enabled)[139]. Moliyaviy kiberjinoyatlarning aksariyati ikkinchi guruhga kiradi. O‘zbekiston Jinoyat kodeksi esa ularni bir tomondan XX¹ bobdagi axborot jinoyatlari, ikkinchi tomondan 168 va 169-moddalardagi mulkiy jinoyatlar orqali tartibga soladi. Natijada bir qilmish ikki bobga bo‘linib ketadi, kvalifikatsiyada xatolar yuzaga keladi. D.Uoll ta’kidlaganidek, tarmoq texnologiyalari jonoyat imkoniyatlarini va miqyosini tubdan o`rgartiradi; bitta jinoyatchi bir vaqtning o‘zida minglab jabrlanuvchiga yetib boradi[140]. Qonun buni hisobga olib, ommaviylikni og‘irlashtiruvchi belgi sifatida nazarda tutishi kerak.

Ikkinchidan, ochilish darajasi pastligining asosiy sabablaridan biri jinoyatlarning aksariyati xorijdan sodir etilishidir; shuningdek, tezkor muzlatishning yo'qligi va elektron dalillarni olish murakkabligi ham ta'sir qiladi. IIV ma'lumotlariga ko'ra, 90 foizi xorijdan sodir etilmoqda.. O‘zbekiston Budapesht konvensiyasining ishtirokchisi emas, BMT konvensiyasi esa hali kuchga kirmagan. Shu bois xorijiy provayderlar va banklardan elektron dalillarni olish, pul mablag‘larini tezkor muzlatish ikki tomonlama kelishuvlarga bog‘liq bo‘lib qolmoqda.

Uchinchidan, javobgarlik taqsimoti hali qonun darajasida mustahkamlanmagan. PQ-153-son qarorda banklarning zararni qoplash majburiyati prinsip sifatida belgilangan, ammo mexanizm qonun darajasida mustahkamlanmagan. Uchta bank tizimidagi zaiflik tufayli 3 025 mijozning 17 mlrd so‘m yo‘qotgani bu masalaning amaliy ahamiyatini ko‘rsatadi. Buyuk Britaniya tajribasi bank va jabrlanuvchi o‘rtasida xavfni taqsimlash firibgarlikka qarshi kurashning eng kuchli iqtisodiy rag‘bati ekanini isbotladi. Shu bilan birga, to‘liq kompensatsiya mijozlarning ehtiyotsizligini rag‘batlantirishi mumkin. Shuning uchun Yevropa Ittifoqidagidek “qo‘pol ehtiyotsizlik” istisnosini nazarda tutish oqilona bo‘ladi.

To‘rtinchidan, “dropper”lar masalasi juda muammoli. Jinoiy pullar odatda o‘z kartasini oz haq evaziga bergan shaxslar orqali yuviladi. Qozog‘iston bu qilmish uchun 7 yilgacha ozodlikdan mahrum qilishni nazarda tutgan. Biroq bunday chora ehtiyotkorlikni talab qiladi: dropperlar orasida voyaga yetmaganlar va ijtimoiy jihatdan zaif shaxslar ko‘p. Shuning uchun, birinchi marta va jinoiy maqsadni ehtiyotsizlik oqibatida sodir etilgan qilmish uchun ma’muriy javobgarlik, bila turib va tizimli ravishda sodir etilgani uchun esa jinoiy javobgarlik belgilanishi adolatli bo‘ladi.

Beshinchidan, profilaktika texnologik va ijtimoiy jihatdan muvozanatlashishi kerak. Faqat 2026-yilning to‘qqiz oyida 43 001 ta bank kartasi bloklangani va 38 mingdan ortiq fishing

[139] McGuire M., Dowling S. Cyber crime: A review of the evidence
[140] Wall D.S. Cybercrime: The Transformation of Crime in the Information Age. – Cambridge: Polity Press, 2007.

dasturi to‘xtatilgani antifrod tizimlarining samarasini ko‘rsatadi. Ammo jinoyatlarning 60 foizi fuqaroning o‘zi zararli faylni o‘rnatishi bilan boshlanadi. Demak, moliyaviy savodxonlik texnik himoyadan kam ahamiyatga ega emas. Bundan tashqari, sun’iy intellekt yordamida ovoz va tasvirni soxtalashtirish (deepfake) ijtimoiy muhandislikni yanada xavfli qiladi, bu esa yangi huquqiy javoblarni talab etadi.

Moliyaviy kiberjinoyat bugun O‘zbekistonda jinoyatchilikning eng tez o‘sayotgan turi bo‘lib, barcha jinoyatlarning qariyb yarmini tashkil etmoqda. Uning asosiy shakllari - zararli dasturlar orqali karta va qurilmani egallash, ijtimoiy muhandislik, onlayn savdo va investitsion firibgarlik hamda “dropper”lar orqali mablag‘larni legallashtirish. Davlat 2025-2026-yillarda institutsional va strategik asoslarni yaratdi, lekin ularni qonun darajasida mustahkamlash jarayoni hali yakunlanmagan.

Tadqiqot natijalariga tayanib, milliy qonunchilik va huquqni qo‘llash amaliyotini takomillashtirish bo‘yicha bir qator kompleks choralarni amalga oshirish maqsadga muvofiq. Xususan, “Kiberxavfsizlik to‘g‘risida”gi qonunga “moliyaviy kiberjinoyat” tushunchasini kiritish, shuningdek, 168 va 169-moddalarda jinoyatni ommaviy (ko‘p sonli jabrlanuvchiga qarshi) hamda sun’iy intellekt yordamida yaratilgan soxta ovoz va tasvirlardan foydalanib sodir etishni og‘irlashtiruvchi holat sifatida belgilash zarur. Shu bilan birga, “dropper”lik faoliyati uchun javobgarlikni tabaqalashtirib, birinchi marta va ehtiyotsizlik natijasida sodir etilganda ma’muriy, bila turib va takroran sodir etilganda esa jinoiy javobgarlik choralarini qo‘llash lozim. Jabrlanuvchilarning moliyaviy huquqlarini samarali himoya qilish maqsadida bank va to‘lov tashkilotlari zimmasiga yetkazilgan zararni qoplash majburiyatini (yuqori chegara, aniq muddatlar va mijozning qo‘pol ehtiyotsizligi istisnosini ko‘rsatgan holda) yuklash, shubhali o‘tkazmalarni banklararo 24/7 rejimida muzlatish hamda mablag‘larni sudgacha qaytarish mexanizmini joriy etish talab etiladi. Bundan tashqari, telekom operatorlari uchun qo‘ng‘iroqlarni markirovka qilish va soxta raqamlarni bloklash majburiyatini qonunda mustahkamlash, xalqaro hamkorlikni kuchaytirish uchun esa Budapesht konvensiyasiga qo‘shilish hamda BMTning Kiberjinoyatchilikka qarshi konvensiyasini imzolash va ratifikatsiya qilish masalasini ko‘rib chiqish muhim ahamiyat kasb etadi. Ushbu choralar tizimli ravishda hayotga tatbiq etilsa, kiberjinoyatchilikka qarshi kurashish “jazolash” tamoyilidan “oldini olish va zararni tiklash” modeliga o‘tadi.

Foydalanilgan adabiyotlar

1.O‘zbekiston Respublikasining Jinoyat kodeksi. 1994-yil 22-sentabr // lex.uz/docs/111457.

2.O‘zbekiston Respublikasining Ma’muriy javobgarlik to‘g‘risidagi kodeksi. 1994-yil 22-sentabr.

3.O‘zbekiston Respublikasining “Kiberxavfsizlik to‘g‘risida”gi qonuni. 2022-yil 15-aprel, O‘RQ-764 // lex.uz/uz/docs/5960609.

5.O‘zbekiston Respublikasining 2024-yil 19-yanvardagi O‘RQ-899-son qonuni // lex.uz/docs/6763849.

6.O‘zbekiston Respublikasi Prezidentining 2025-yil 30-apreldagi PQ-153-son qarori.

7.O‘zbekiston Respublikasi Prezidentining 2026-yil 10-martdagi PF-38-son farmoni // lex.uz/uz/docs/-8079286.

8.Convention on Cybercrime (ETS No. 185). -Budapest, 23 November 2001.

9.Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence (CETS No. 224). - Strasbourg, 2022.

10.United Nations Convention against Cybercrime. - New York, 24 December 2024.

11.Directive (EU) 2019/713 of the European Parliament and of the Council of 17 April 2019 on combating fraud and counterfeiting of non-cash means of payment.

12.Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market (PSD2).

13.Computer Fraud and Abuse Act, 18 U.S.C. §1030; Wire Fraud, 18 U.S.C. §1343

14.Electronic Fund Transfer Act, 15 U.S.C. §1693 et seq.; Regulation E, 12 CFR Part 1005

15.Уголовный кодекс Республики Казахстан от 03.07.2014 № 226-V (ст. 232¹).

16.McGuire M., Dowling S. Cyber crime: A review of the evidence. Home Office Research Report 75. London: Home Office, 2013.

17.Wall D.S. Cybercrime: The Transformation of Crime in the Information Age. – Cambridge: Polity Press, 2007.

18.Federal Bureau of Investigation. 2025 Internet Crime Report. - Washington: IC3, 2026.

19.UK Finance. Annual Fraud Report 2025. London, 2025.

20.O‘zbekiston Respublikasi Ichki ishlar vazirligi rasmiy axborotlari (2025–2026) // gov.uz/oz/iiv.

21.Kun.uz, Spot.uz, Gazeta.uz, Advice.uz, UzA axborot agentliklari materiallari (2025–2026).