

**KIBERFIRIBGARLIK BILAN KURASHISH: MILLIY MUAMMOLAR VA
XALQARO AMALIYOT**

Atemov Bobur Uskenbayevich

Toshkent viloyati prokuraturasi

Ichki ishlar organlarida qonunchilik ijrosi ustidan nazorat bo'limi prokurori,
adliya maslahatchisi.

<https://doi.org/10.5281/zenodo.23270594>

Annotatsiya. Maqolada raqamli iqtisodiyot sharoitida axborot-kommunikatsiya texnologiyalari vositasida sodir etilayotgan firibgarlik (kiberfiribgarlik) jinoyatlarining yuridik tabiati, jinoyat tarkibi belgilari va ularga qarshi kurashishdagi milliy muammolar tahlil qilingan. O'zbekiston Respublikasi Jinoyat kodeksining 168-moddasi uchinchisi qismi "g" bandi, Oliy sud Plenumining 2023-yil 23-iyundagi 17-son qarori tushuntirishlari, kiberfiribgarlikni axborot tizimiga ruxsatsiz kirib sodir etilgan o'g'rilikdan farqlash mezonlari, "drop" hisobvaraqlar va kripto-aktivlar orqali mablag'larni legallashtirish, elektron dalillarni to'plash masalalari yoritilgan. Budapesht va Xanoy konvensiyalari, AQSh, Buyuk Britaniya, Germaniya, Avstriya, Fransiya, Bolgariya va Rossiya Federatsiyasi tajribasi qiyosiy-huquqiy usulda o'rganilib, milliy qonunchilik va huquqni qo'llash amaliyotini takomillashtirish bo'yicha takliflar ilgari surilgan.

Kalit so'zlar: kiberfiribgarlik, kiberjinoyatchilik, kompyuter firibgarligi, aldash, ishonchni suiiste'mol qilish, axborot tizimi, kvalifikatsiya, drop karta, kripto-aktivlar, raqamli dalillar, texnologik neytrallik, Budapesht konvensiyasi.

Аннотация. В статье анализируются юридическая природа и признаки состава мошенничества, совершаемого с использованием информационно-коммуникационных технологий (кибермошенничества), а также национальные проблемы противодействия ему в условиях цифровой экономики. Рассмотрены пункт «г» части третьей статьи 168 Уголовного кодекса Республики Узбекистан, разъяснения Постановления Пленума Верховного суда от 23 июня 2023 года № 17, критерии разграничения кибермошенничества и кражи с неправомерным доступом к информационной системе, вопросы «дроп»-счетов, легализации средств через крипто-активы и собирания электронных доказательств. Сравнительно-правовым методом изучены Будапештская и Ханойская конвенции, опыт США, Великобритании, Германии, Австрии, Франции, Болгарии и Российской Федерации; сформулированы предложения по совершенствованию законодательства и правоприменительной практики.

Ключевые слова: кибермошенничество, киберпреступность, компьютерное мошенничество, обман, злоупотребление доверием, информационная система, квалификация, дроп-карта, крипто-активы, цифровые доказательства, технологическая нейтральность, Будапештская конвенция.

Abstract. The article analyses the legal nature and elements of fraud committed through information and communication technologies (cyber-fraud) and the national problems of countering it in the digital economy. It examines paragraph "g" of Part 3 of Article 168 of the Criminal Code of the Republic of Uzbekistan, the guidance of Supreme Court Plenum Resolution

No. 17 of 23 June 2023, the criteria distinguishing cyber-fraud from theft committed by unauthorised access to an information system, “drop” accounts, laundering of proceeds through crypto-assets and the collection of electronic evidence. Using a comparative law approach, the Budapest and Hanoi Conventions and the experience of the USA, the United Kingdom, Germany, Austria, France, Bulgaria and the Russian Federation are examined, and proposals are made for improving legislation and law enforcement practice.

Keywords: cyber-fraud, cybercrime, computer-related fraud, deception, abuse of trust, information system, criminal qualification, drop card, crypto-assets, digital evidence, technological neutrality, Budapest Convention.

KIRISH

Raqamli iqtisodiyot va axborot-kommunikatsiya texnologiyalarining jadal rivojlanishi mulkiy tajovuzlarning yangi, transmilliy va yuqori darajada yashirin shakllarini yuzaga keltirmoqda. Jinoyatchi va jabrlanuvchi oʻrtasidagi bevosita aloqa oʻrnini telefon qoʻngʻiroqlari, messenjerlar, soxta saytlar va mobil ilovalar egallab, aldov texnologik vositalar orqali ommaviy tus olmoqda. 2025-yil 3-noyabrda Prezidentga taqdim etilgan maʼlumotlarga koʻra, soʻnggi besh yilda mamlakatimizda kiberjinoyatlar soni 68 baravarga oshgan, faqat 2025-yilning oʻzida 46 mingdan ortiq holat qayd etilib, jismoniy va yuridik shaxslarga 1,2 trillion soʻmdan ortiq zarar yetkazilgan.¹ Ichki ishlar vazirligi maʼlumotiga koʻra, 2019-yilda axborot texnologiyalari orqali 863 ta jinoyat sodir etilgan boʻlsa, 2024-yilda ularning soni 58,8 mingga yetgan.²

Bu jinoyatlarning salmoqli qismi aldash yoki ishonchni suiisteʼmol qilishga asoslangan firibgarlik koʻrinishida sodir etilmoqda. Oʻzbekiston Respublikasi Konstitutsiyasining 31-moddasida har kimning yozishmalari, telefon orqali soʻzlashuvlari, pochta, elektron va boshqa xabarlar sir saqlanishi huquqi kafolatlangan.³ Kiberfiribgarlar koʻpincha aynan shu maxfiy maʼlumotlarni – bir martalik kodlar, akkaunt va karta rekvizitlarini – qoʻlga kiritishga intilgani bois, ular nafaqat mulkiy huquqlarga, balki shaxsning konstitutsiyaviy daxlsizligiga ham tajovuz qiladi. Shu sababli kiberfiribgarlikka qarshi kurashning milliy muammolarini xalqaro tajriba bilan qiyoslab oʻrganish dolzarb ilmiy-amaliy vazifadir.

ASOSIY QISM

Oʻzbekiston Respublikasining 2022-yil 15-apreldagi “Kiberxavfsizlik toʻgʻrisida”gi Qonunida kiberjinoyatchilik kibermakonda dasturiy taʼminot va texnik vositalardan foydalanib sodir etiladigan jinoyatlar majmui sifatida taʼriflanadi.⁴ Kiberfiribgarlik ushbu jinoyatlar ichida eng keng tarqalgani boʻlib, Jinoyat kodeksida (JK) alohida jinoyat tarkibi emas, balki firibgarlikning ogʻirlashtirilgan turi sifatida – axborot tizimidan, shu jumladan axborot

¹ Soʻnggi besh yilda kiberjinoyatlar soni 68 barobarga oshgan // Anhor.uz, 03.11.2025. – URL: <https://anhor.uz/uz/news/s-nggi-besh-jilda-kiberzhinojatlar-soni-68-barobarga-oshgan/>

² Kiberjinoyatlarni jilovlash orqali xavfsiz kibermakon yaratish // Oʻzbekiston Respublikasi Ichki ishlar vazirligi, 07.05.2025. – URL: <https://gov.uz/uz/iiv/news/view/52319>

³ Oʻzbekiston Respublikasining Konstitutsiyasi (2023-yil 30-aprel). – 31-modda // Qonunchilik maʼlumotlari milliy bazasi. – URL: <https://lex.uz/docs/6445145>

⁴ Oʻzbekiston Respublikasining 2022-yil 15-apreldagi “Kiberxavfsizlik toʻgʻrisida”gi OʻRQ-764-son Qonuni. – 3-modda // Qonunchilik maʼlumotlari milliy bazasi. – URL: <https://lex.uz/docs/5960604>

texnologiyalaridan foydalanib sodir etilgan firibgarlik (JK 168-moddasi uchinchi qismi “g” bandi) tarzida belgilangan.⁵ 2022-yil 19-oktabrdagi O‘RQ-794-son Qonun bilan ushbu qilmish uchun jazo kuchaytirilib, besh yildan sakkiz yilgacha ozodlikdan mahrum qilish nazarda tutildi.⁶

Oliy sud Plenumining 2023-yil 23-iyundagi 17-son qarorida firibgarlik o‘zganing mulkini yoki mulkka bo‘lgan huquqini aldash yoki ishonchni suiiste‘mol qilish yo‘li bilan qonunga xilof ravishda va tekin qo‘lga kiritish, bunda mulkdor yoki vakolatli shaxsning mulkni o‘zi berishi yoxud olib qo‘yilishiga imkon yaratishi sifatida tavsiflangan.⁷ Qarorning 22-bandida esa axborot texnologiyalaridan foydalanib firibgarlik deganda moliya, bank muassasalari va fondlardagi mulkni kompyuter texnikasi, aloqa vositasi, planshet yoki boshqa texnik qurilmalar yordamida manipulyatsiya qilish orqali aldov yo‘li bilan talon-toraj qilish tushunilishi, u axborotni o‘zgartirish yoki kompyuter tizimiga yolg‘on axborot kiritish yo‘li bilan ham sodir etilishi mumkinligi tushuntirilgan.⁸ Plenum, shuningdek, kreditni onlayn olish uchun o‘zga shaxsning texnik vositalari maxsus kodlari yoki elektron raqamli imzosidan aldov yo‘li bilan foydalanishni firibgarlik deb baholagan, bankdagi pul mablag‘lari bilan bog‘liq firibgarlikni esa mablag‘ aybdor yoki boshqa shaxs hisobvarag‘iga o‘tkazilgan paytdan tugallangan deb hisoblagan.⁹

Kiberfiribgarlikka qarshi kurashdagi birinchi milliy muammo – uni axborot tizimiga qonunga xilof ravishda (ruxsatsiz) kirib yoki undan foydalanib sodir etilgan o‘g‘rilikdan (JK 169-moddasi uchinchi qismi) farqlashdir. Plenum mezoniga ko‘ra, firibgarlikda jabrlanuvchi aldov yoki ishonchi suiiste‘mol qilinishi oqibatida mulkni axborot texnologiyalari orqali aybdor egaligiga ixtiyoriy o‘tkazadi va mulk o‘z egaligidan chiqib ketayotganini anglaydi.¹⁰ Biroq amaliyotda eng ko‘p uchraydigan holatda – jabrlanuvchi “bank xodimi”ga SMS-kodni aytib bergan, mablag‘ni esa aybdorning o‘zi uning ishtirokisiz yechib olgan vaziyatda – jabrlanuvchi kodni bergan bo‘lsa-da, mulk chiqib ketayotganini anglamaydi. Bunday qilmishlar sud-tergov amaliyotida goh 168-modda, goh 169-modda bilan kvalifikatsiya qilinmoqda. Bizningcha, Plenumning “anglash” mezoniga ko‘ra bu holatlarda aldov faqat mulkka yashirin erishish vositasi bo‘lib xizmat qiladi va qilmish o‘g‘rilik sifatida baholanishi lozim; buni 17-son qarorga alohida misol tariqasida kiritish amaliyotni birxillashtiradi.

⁵O‘zbekiston Respublikasining Jinoyat kodeksi (22.09.1994). – 168-modda // Qonunchilik ma’lumotlari milliy bazasi. – URL: <https://lex.uz/docs/111453>

⁶O‘zbekiston Respublikasining 2022-yil 19-oktabrdagi “O‘zbekiston Respublikasining ayrim qonun hujjatlariga o‘zgartirish va qo‘shimchalar kiritish to‘g‘risida”gi O‘RQ-794-son Qonuni; Firibgarlikni axborot texnologiyalaridan foydalanib sodir etganlik uchun javobgarlik kuchaytirildi // Advice.uz, 20.10.2022. – URL: <https://advice.uz/uz/news/661>

⁷O‘zbekiston Respublikasi Oliy sudi Plenumining 2023-yil 23-iyundagi “Firibgarlikka oid ishlar bo‘yicha sud amaliyoti to‘g‘risida”gi 17-son qarori // Qonunchilik ma’lumotlari milliy bazasi. – URL: <https://lex.uz/docs/6523582>. – 3-band.

⁸O‘zbekiston Respublikasi Oliy sudi Plenumining 2023-yil 23-iyundagi “Firibgarlikka oid ishlar bo‘yicha sud amaliyoti to‘g‘risida”gi 17-son qarori // Qonunchilik ma’lumotlari milliy bazasi. – URL: <https://lex.uz/docs/6523582>. – 22-band.

⁹O‘zbekiston Respublikasi Oliy sudi Plenumining 2023-yil 23-iyundagi “Firibgarlikka oid ishlar bo‘yicha sud amaliyoti to‘g‘risida”gi 17-son qarori // Qonunchilik ma’lumotlari milliy bazasi. – URL: <https://lex.uz/docs/6523582>. – 7, 9-bandlar.

¹⁰O‘zbekiston Respublikasi Oliy sudi Plenumining 2023-yil 23-iyundagi “Firibgarlikka oid ishlar bo‘yicha sud amaliyoti to‘g‘risida”gi 17-son qarori // Qonunchilik ma’lumotlari milliy bazasi. – URL: <https://lex.uz/docs/6523582>. – 22, 26-bandlar.

Ikkinchi muammo – Plenum ta’rifida “manipulyatsiya” va “yolgʻon axborot kiritish” tushunchalari bilan jabrlanuvchining irodasi va anglashi talabi bir vaqtda qoʻllanayotganidir.

Xorijiy doktrinada inson ishtirokisiz faqat ma’lumotlarga ishlov berish natijasiga ta’sir ko’rsatish (masalan, bank tizimiga yolgʻon to’lov topshirig’ini kiritish) “kompyuter firibgarligi” deb ataladi, chunki mashinani aldash mumkin emas. Milliy qonunchilikda bunday qilmishlar uchun alohida norma yo’qligi ularni firibgarlik va o’g’rilik o’rtasidagi “kulrang zona”da qoldirmoqda. Uchinchi muammo – jazoning tabaqalashtirilmaganligi: 168-moddaning uchinchi qismi “g” bandi zarar miqdoridan qat’i nazar besh yildan sakkiz yilgacha ozodlikdan mahrum qilishni nazarda tutadi. To’g’ri, JK 168-moddasi beshinchi qismiga ko’ra zarar qoplanganda ozodlikni cheklash va ozodlikdan mahrum qilish qo’llanilmaydi,¹¹ ammo zarar qoplanmagan oz miqdordagi holatlarda sanksiya adolatlilik prinsipiga har doim ham mos kelavermaydi.

To’rtinchi muammo – jinoiy guruhlarining “infratuzilma” ishtirokchilari javobgarligi.

Kiberfiribgarlik odatda vazifalari taqsimlangan guruh tomonidan sodir etiladi: qo’ng’iroq qiluvchi “operatorlar”, zararli dasturlarni tarqatuvchilar, “drop” karta va hisobvaraqlarni yig’uvchi va sotuvchilar hamda mablag’ni kripto-aktivlarga aylantirib xorijga chiqaruvchilar. Prezidentning 2025-yil 30-apreldagi PQ-153-son qarori bilan droplar uchun ma’muriy va jinoiy javobgarlik belgilash, Markaziy bankda droplar reyestrini yuritish, shubhali o’tkazmalarga aloqador kartalarni tezkor bloklash tizimini yaratish vazifalari belgilandi.¹² Kripto-aktivlar bilan bog’liq qismda JK 278⁸-moddasi qo’llanilmoqda, biroq bu shaxslarning firibgarlikdagi ishtirokchilik roli ko’pincha baholanmay qolmoqda. Ichki ishlar vazirligi, Istiqbolli loyihalar milliy agentligi va Bosh prokuraturaning 2024-yil 25-dekabrda 3591-son bilan ro’yxatdan o’tkazilgan qo’shma buyrug’i bilan tasdiqlangan yo’riqnoma kripto-aktivlarni tergovga qadar tekshiruv va tergov davomida xatlash, olib qo’yish, zararni qoplash uchun undirish hamda dalil sifatida e’tirof etish tartibini va bunda mutaxassis ishtirokining majburiyligini belgiladi.¹³

Beshinchi muammo – isbotlash va elektron dalillar. 2024-yil 21-noyabrdagi O’RQ-1003-son Qonun bilan Jinoyat-protsessual kodeksiga raqamli dalillar tushunchasi kiritilib, ishtirokchilarga elektron ma’lumotlarning ko’chirma nusxasini taqdim etish huquqi berildi.¹⁴

Biroq protsessual talablar buzilgan holda olingan ma’lumotlar JPK 95¹-moddasiga ko’ra maqbul bo’lmagan dalil deb topilishi,¹⁵ xorijiy xosting, domen va platforma provayderlaridan

¹¹ O’zbekiston Respublikasi Oliy sudi Plenumining 2023-yil 23-iyundagi “Firibgarlikka oid ishlar bo’yicha sud amaliyoti to’g’risida”gi 17-son qarori // Qonunchilik ma’lumotlari milliy bazasi. – URL: <https://lex.uz/docs/6523582>. – 29-band.

¹² O’zbekiston Respublikasi Prezidentining 2025-yil 30-apreldagi “Axborot texnologiyalari yordamida sodir etiladigan jinoyatlarga qarshi kurashish faoliyatini yanada kuchaytirishga qaratilgan chora-tadbirlar to’g’risida”gi PQ-153-son qarori // Qonunchilik ma’lumotlari milliy bazasi. – URL: <https://lex.uz/docs/7511145>. – 5, 11, 12-bandlar.

¹³ Tergovga qadar tekshiruvni amalga oshirishda va jinoyatlarni tergov qilish davomida aniqlangan kripto-aktivlarni olib qo’yish, xatlash, saqlash hamda topshirish tartibi to’g’risidagi yo’riqnoma (Adliya vazirligida 25.12.2024-yilda 3591-son bilan ro’yxatdan o’tkazilgan) // Qonunchilik ma’lumotlari milliy bazasi. – URL: <https://lex.uz/docs/-7282772>

¹⁴ O’zbekiston Respublikasining 2024-yil 21-noyabrdagi “O’zbekiston Respublikasining ayrim qonun hujjatlariga raqamli dalillar bilan ishlash tizimini takomillashtirishga qaratilgan o’zgartirish va qo’shimchalar kiritish to’g’risida”gi O’RQ-1003-son Qonuni // Qonunchilik ma’lumotlari milliy bazasi. – URL: <https://lex.uz/doc-passport/7228758>

loglar va IP-ma'lumotlarni olish esa faqat xalqaro hamkorlik orqali mumkinligi tergovni sekinlashtirmoqda. PQ-153-son qarorda huquqni muhofaza qiluvchi organlarning bank siriga oid so'rovlarini bajarishning aniq muddatlarini belgilash, Ichki ishlar vazirligi, Bosh prokuratura va Markaziy bank o'rtasida elektron ma'lumot almashinuvi platformasini ishga tushirish va Markaziy bankda markazlashgan antifrod tizimini joriy etish nazarda tutilgani ushbu muammoni qisman hal etishga qaratilgan.¹⁶

XORIJIY TAJRIBA VA QIYOSIY-HUQUQIY TAHLIL

Yevropa Kengashining 2001-yildagi Kiberjinoyatlar to'g'risidagi Budapesht konvensiyasi 8-moddasida "kompyuter bilan bog'liq firibgarlik" – ma'lumotlarni kiritish, o'zgartirish, o'chirish yoki kompyuter tizimi faoliyatiga aralashish orqali boshqa shaxsga mulkiy zarar yetkazib, iqtisodiy manfaat olishni jinoyat deb topish talab etiladi.¹⁷ Konvensiya texnologik neytrallik prinsipiga asoslanib, muayyan texnologiyani emas, balki qilmish mohiyatini tavsiflaydi; uning 16–18 va 29–30-moddalari esa elektron ma'lumotlarni tezkor saqlash va davlatlararo tezkor hamkorlik mexanizmlarini belgilaydi. PQ-153-son qaror bilan Tashqi ishlar vazirligiga Budapesht konvensiyasiga muayyan shartlar asosida qo'shilish masalasini o'rganib, takliflar kiritish topshirilgani bu yo'nalishdagi muhim qadamdir.¹⁸ Shuningdek, 2024-yil 24-dekabrda BMT Bosh Assambleyasi tomonidan qabul qilinib, 2025-yil 25-oktabrda Xanoyda imzolash uchun ochilgan BMTning Kiberjinoyatchilikka qarshi konvensiyasi ham elektron dalillar almashinuvi bo'yicha universal hamkorlik asosini yaratadi.¹⁹

AQSh federal qonunchiligida kiberfiribgarlik ikki asosiy norma bilan qamrab olinadi: himoyalangan kompyuterga ruxsatsiz yoki vakolat doirasidan chiqib kirish orqali firibgarlik niyatida qimmatlik qo'lga kiritish (Computer Fraud and Abuse Act, 18 U.S.C. § 1030(a)(4)) hamda elektr aloqa vositalaridan foydalangan holda firibgarlik (wire fraud, 18 U.S.C. § 1343).²⁰

Ikkinchi norma texnologik neytral bo'lib, telefon, internet yoki messenjer orqali aldovning barcha shakllariga qo'llaniladi. Buyuk Britaniyada esa tizimga ruxsatsiz kirish va ma'lumotlarga aralashish Computer Misuse Act 1990 bilan, mulkiy natija esa Fraud Act 2006 bilan baholanadi.²¹

Fraud Act 2006 2-bo'limining 5-qismiga ko'ra, yolg'on ma'lumot inson ishtirokisiz ishlaydigan har qanday tizim yoki qurilmaga taqdim etilgan bo'lsa ham taqdim etilgan hisoblanadi. Bu yechim "mashinani aldab bo'lmaydi" degan muammoni qonun darajasida bartaraf

¹⁵O'zbekiston Respublikasining Jinoyat-protsessual kodeksi (22.09.1994). – 95¹-modda // Qonunchilik ma'lumotlari milliy bazasi. – URL: <https://lex.uz/docs/111460>

¹⁶O'zbekiston Respublikasi Prezidentining 2025-yil 30-apreldagi "Axborot texnologiyalari yordamida sodir etiladigan jinoyatlarga qarshi kurashish faoliyatini yanada kuchaytirishga qaratilgan chora-tadbirlar to'g'risida"gi PQ-153-son qarori // Qonunchilik ma'lumotlari milliy bazasi. – URL: <https://lex.uz/docs/7511145>. – 5, 9, 16-bandlar.

¹⁷Convention on Cybercrime (Budapest, 23.11.2001). Council of Europe, ETS No. 185. – Art. 8, 16–18, 29–30.

¹⁸O'zbekiston Respublikasi Prezidentining 2025-yil 30-apreldagi "Axborot texnologiyalari yordamida sodir etiladigan jinoyatlarga qarshi kurashish faoliyatini yanada kuchaytirishga qaratilgan chora-tadbirlar to'g'risida"gi PQ-153-son qarori // Qonunchilik ma'lumotlari milliy bazasi. – URL: <https://lex.uz/docs/7511145>. – 17-band.

¹⁹United Nations Convention against Cybercrime. Adopted by UN General Assembly resolution 79/243 of 24 December 2024 (opened for signature in Hanoi on 25 October 2025).

²⁰18 U.S.C. § 1030 (Computer Fraud and Abuse Act); 18 U.S.C. § 1343 (Fraud by wire, radio, or television).

²¹Computer Misuse Act 1990, ss. 1–3; Fraud Act 2006, s. 2 (United Kingdom). – URL: <https://www.legislation.gov.uk>

etadi. Germaniya Jinoyat kodeksining 263a-paragrafida “kompyuter firibgarligi” (Computerbetrug) – dasturni noto‘g‘ri tuzish, noto‘g‘ri yoki to‘liq bo‘lmagan ma’lumotlardan yoxud ma’lumotlardan ruxsatsiz foydalanish orqali ma’lumotlarga ishlov berish natijasiga ta’sir ko‘rsatib, mulkiy zarar yetkazish uchun alohida javobgarlik belgilangan.²² Qonun chiqaruvchi aldov obyekti inson bo‘lmagan holatlarda klassik firibgarlik normasini qo‘llash mumkin emasligini inobatga olgan.²³ Avstriya Jinoyat kodeksining 148a-paragrafi (ma’lumotlarga ishlov berishni firibgarlik maqsadida suiiste’mol qilish) jazoni zarar miqdoriga qarab tabaqalashtiradi: 5 ming va 300 ming yevrodan ortiq zarar alohida og‘irlashtiruvchi belgi hisoblanadi.²⁴ Bolgariya Jinoyat kodeksining 212a-moddasida ham kompyuter ma’lumotlarini kiritish, o‘zgartirish yoki o‘chirish orqali mulkiy manfaat olish alohida “kompyuter firibgarligi” tarkibi sifatida belgilangan.²⁵

Fransiya Jinoyat kodeksida aldov orqali mulk olish an’anaviy firibgarlik (escroquerie, 313-1-modda) normasi bilan, avtomatlashtirilgan ma’lumotlarni qayta ishlash tizimlariga ruxsatsiz kirish va ularga aralashish esa 1988-yilgi “Godfrain qonuni” asosida kiritilgan 323-1–323-7-moddalar bilan baholanadi; tizimga ruxsatsiz kirishning o‘zi zarar yetkazilmasa ham tugallangan jinoyat hisoblanadi.²⁶ Rossiya Federatsiyasida esa elektron to‘lov vositalaridan foydalanib firibgarlik (159.3-modda) va kompyuter axboroti sohasidagi firibgarlik (159.6-modda) alohida normalar sifatida mavjud bo‘lib, RF Oliy sudi Plenumi jabrlanuvchining hisob ma’lumotlaridan, ular qanday olinganidan qat’i nazar, foydalanib mablag‘ni yechib olishni – dasturiy ta’minotga ta’sir ko‘rsatilmagan bo‘lsa – o‘g‘rilik sifatida baholashni tushuntirgan.²⁷ Shunday qilib, xorijiy davlatlarda ikki model shakllangan: alohida “kompyuter firibgarligi” normasi (Germaniya, Avstriya, Bolgariya, Rossiya) yoki texnologik neytral umumiy firibgarlik normasini kompyuter jinoyatlari normalari bilan birga qo‘llash (AQSh, Buyuk Britaniya, Fransiya).

TAHLIL NATIJALARI VA TAKLIFLAR

Birinchidan, Oliy sud Plenumining 17-son qarori 22-bandini jabrlanuvchi bir martalik kod yoki rekvizitlarni aldov ta’sirida bergan, mablag‘ni esa aybdorning o‘zi o‘tkazgan holatlarga oid aniq tushuntirish bilan to‘ldirish maqsadga muvofiq. Ikkinchidan, Budapesht konvensiyasi 8-moddasi va Germaniya, Avstriya tajribasi asosida JK XX¹ bobiga yoki 168-moddaga inson aldanmagan holda ma’lumotlarga ishlov berish natijasiga ta’sir ko‘rsatish orqali mulk egallashni qamrab oluvchi “kompyuter firibgarligi” normasini kiritish, uning sanksiyasini zarar miqdori (ancha, ko‘p, juda ko‘p) va uyushgan guruh ishtirokiga qarab tabaqalashtirish taklif etiladi.

Uchinchidan, jinoiy sxemadan xabardor bo‘lgan holda drop karta va hisobvaraqlarni yig‘uvchi, sotuvchi hamda mablag‘ni kripto-aktivlar orqali legallashtiruvchi shaxslarning

²²Strafgesetzbuch (StGB). – § 263a Computerbetrug. – URL: https://www.gesetze-im-internet.de/stgb/_263a.html

²³Жалинский А.Э. Современное немецкое уголовное право. – М.: Проспект, 2006.

²⁴ Strafgesetzbuch (Österreich). – § 148a Betrügerischer Datenverarbeitungsmissbrauch. – URL: <https://www.ris.bka.gv.at>

²⁵Наказателен кодекс на Република България. – Чл. 212а.

²⁶Code pénal (France). – Art. 313-1, 323-1 – 323-7. – URL: <https://www.legifrance.gouv.fr>

²⁷Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ. – Ст. 159.3, 159.6; Постановление Пленума Верховного Суда РФ от 30.11.2017 № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате». – П. 17, 21.

harakatlari firibgarlikda ishtirokchilik sifatida, zarur hollarda jinoiy faoliyatdan olingan daromadlarni legallashtirish (JK 243-modda) bilan jinoyatlar majmui tariqasida baholanishi lozim; xabardor bo'lmagan droplar uchun esa PQ-153-son qarorda nazarda tutilgan alohida javobgarlik normasi qonunda belgilanishi kerak. To'rtinchidan, PQ-153-son qarorga muvofiq Budapesht konvensiyasiga qo'shilish masalasini hal etish va BMTning Kiberjinoyatchilikka qarshi konvensiyasiga qo'shilish xorijiy provayderlardan elektron dalillarni olish muddatlarini keskin qisqartiradi. Beshinchidan, banklarning antifrod tizimlari, telekommunikatsiya operatorlarining soxta qo'ng'iroqlarni cheklash tizimi va huquqni muhofaza qiluvchi organlarning ma'lumot almashinuv platformasi yagona tezkor javob mexanizmiga birlashtirilishi, har yili noyabr oyida o'tkaziladigan "Kibermadaniyatni yuksaltirish oyligi" esa kiberfiribgarlik profilaktikasining doimiy vositasiga aylantirilishi lozim.²⁸

XULOSA

Kiberfiribgarlik an'anaviy firibgarlikning raqamli makondagi davomi bo'lsa-da, uning masofaviyligi, anonimligi va transchegaraviy xususiyati kvalifikatsiya, isbotlash va jinoiy daromadlarni qaytarish bo'yicha yangi muammolarni yuzaga keltirmoqda. Milliy qonunchilikda JK 168-moddasi uchinchi qismi "g" bandi, Oliy sud Plenumining 17-son qarori, O'RQ-1003-son Qonun, 3591-son yo'riqnoma va PQ-153-son qaror bilan mustahkam asos yaratilgan.

Biroq kiberfiribgarlik va kibero'g'rilik chegarasini aniq belgilash, "kompyuter firibgarligi" uchun alohida norma joriy etish, jazoni zarar miqdoriga qarab tabaqalashtirish, droplar va kripto-legallashtiruvchilarning ishtirokchilik javobgarligini ta'minlash hamda xalqaro konvensiyalarga qo'shilish orqali transchegaraviy hamkorlikni kuchaytirish kiberfiribgarlikka qarshi kurash samaradorligini oshirishning asosiy yo'nalishlari hisoblanadi.

FOYDALANILGAN ADABIYOTLAR RO'YXATI

Normativ-huquqiy hujjatlar

1. O'zbekiston Respublikasining Konstitutsiyasi. 30.04.2023. // <https://lex.uz/docs/6445145>
2. O'zbekiston Respublikasining Jinoyat kodeksi. 22.09.1994. // <https://lex.uz/docs/111453>
3. O'zbekiston Respublikasining Jinoyat-protsessual kodeksi. 22.09.1994. // <https://lex.uz/docs/111460>
4. O'zbekiston Respublikasining "Kiberxavfsizlik to'g'risida"gi Qonuni. 15.04.2022, O'RQ-764-son. // <https://lex.uz/docs/5960604>
5. O'zbekiston Respublikasining "O'zbekiston Respublikasining ayrim qonun hujjatlariga o'zgartish va qo'shimchalar kiritish to'g'risida"gi Qonuni. 19.10.2022, O'RQ-794-son. // lex.uz
6. O'zbekiston Respublikasining "O'zbekiston Respublikasining ayrim qonun hujjatlariga raqamli dalillar bilan ishlash tizimini takomillashtirishga qaratilgan o'zgartirish va

²⁸O'zbekiston Respublikasi Prezidentining 2025-yil 30-apreldagi "Axborot texnologiyalari yordamida sodir etiladigan jinoyatlarga qarshi kurashish faoliyatini yanada kuchaytirishga qaratilgan chora-tadbirlar to'g'risida"gi PQ-153-son qarori // Qonunchilik ma'lumotlari milliy bazasi. – URL: <https://lex.uz/docs/7511145>. – 8, 9, 10, 16-bandlar.

- qo'shimchalar kiritish to'g'risida"gi Qonuni. 21.11.2024, O'RQ-1003-son. // <https://lex.uz/doc-passport/7228758>
7. O'zbekiston Respublikasi Prezidentining "Axborot texnologiyalari yordamida sodir etiladigan jinoyatlarga qarshi kurashish faoliyatini yanada kuchaytirishga qaratilgan chora-tadbirlar to'g'risida"gi qarori. 30.04.2025, PQ-153-son. // <https://lex.uz/docs/7511145>
8. O'zbekiston Respublikasi Oliy sudi Plenumining "Firibgarlikka oid ishlar bo'yicha sud amaliyoti to'g'risida"gi qarori. 23.06.2023, 17-son. // <https://lex.uz/docs/6523582>
9. Tergovga qadar tekshiruvni amalga oshirishda va jinoyatlarni tergov qilish davomida aniqlangan kripto-aktivlarni olib qo'yish, xatlash, saqlash hamda topshirish tartibi to'g'risidagi yo'riqnoma (Adliya vazirligida 25.12.2024-yilda 3591-son bilan ro'yxatdan o'tkazilgan). // <https://lex.uz/docs/-7282772>

Xalqaro hujjatlar va xorijiy qonunchilik

10. Convention on Cybercrime (Budapest, 23 November 2001). Council of Europe, ETS No. 185.
11. United Nations Convention against Cybercrime. UN General Assembly resolution 79/243 of 24 December 2024.
12. Computer Fraud and Abuse Act, 18 U.S.C. § 1030; Fraud by wire, radio, or television, 18 U.S.C. § 1343 (USA).
13. Computer Misuse Act 1990; Fraud Act 2006 (United Kingdom).
14. Strafgesetzbuch (StGB) der Bundesrepublik Deutschland. § 263a.
15. Strafgesetzbuch (StGB) der Republik Österreich. § 148a.
16. Code pénal (France). Art. 313-1, 323-1 – 323-7.
17. Наказателен кодекс на Република България. Чл. 212а.
18. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ.
19. Постановление Пленума Верховного Суда Российской Федерации от 30.11.2017 № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате».

Ilmiy adabiyotlar

20. Жалинский А.Э. Современное немецкое уголовное право. – М.: Проспект, 2006.
21. Рахманова С., Очилов Х. Ўзгалир мулкини компьутер воситалиридан фойдаланиб, талин-торож қилиш жиноятларида объект // Рақамли технологиялар соҳасидаги ҳуқуқбузарликларга қарши курашиш ҳамда ахборот хавфсизлигини таъминлашнинг ташкилий-ҳуқуқий масалалари. – 2022. – Т. 1, № 1. – Б. 172–185.
22. Brenner S.W. Cybercrime: Criminal Threats from Cyberspace. – Santa Barbara: Praeger, 2010.
23. McGuire M., Dowling S. Cyber Crime: A Review of the Evidence. Research Report 75. – London: Home Office, 2013.
24. Wall D.S. Cybercrime: The Transformation of Crime in the Information Age. – Cambridge: Polity Press, 2007.

Internet manbalar

25. So‘nggi besh yilda kiberjinoyatlar soni 68 barobarga oshgan // Anhor.uz, 03.11.2025. – URL:<https://anhor.uz/uz/news/s-nggi-besh-jilda-kiberzhinojatlar-soni-68-barobarga-oshgan/>
26. O‘zbekiston Respublikasi Ichki ishlar vazirligi. Kiberjinoyatlarni jilovlash orqali xavfsiz kibermakon yaratish (07.05.2025). – URL: <https://gov.uz/uz/iiv/news/view/52319>