SIR Publishers
CENTER FOR INTERNATIONAL SCIENTIFIC PUBLICATIONS
JOURNAL OF LAW AND ECONOMICS
ISSN(Online): 2984-8091
Volume-9, Issue-02, Published |29-06-2026|

Axborot-kommunikatsiya texnologiyalari yordamida sodir etiladigan firgarlik (kiberfirgarlik) va ularni kvalifikatsiya qilish muammolari.

Termiz davlat universiteti
Yuridik fakulteti 3-bosqich talabasi
Xolmurodova Sevinch Jumanazarovna

Anotatsiya: Ushbu maqolada bugungi kunda global muammoga aylanib borayotgan axborot-kommunikatsiya texnologiyalari yordamida sodir etiladigan firgarlik (kiberfirgarlik) jinoyatlarining kriminologik xususiyatlari va ularni huquqiy baholash muammolari tahlil qilingan. Tadqiqot davomida plastik kartalardan pul mablag‘larini noqonuniy yechib olish, fishing saytlari va feyk havolalar orqali fuqarolarni aldash qilmishlarini amaldagi Jinoyat kodeksining 168-moddasi bilan to‘g‘ri kvalifikatsiya qilishdagi huquqiy bo‘shliqlar hamda tergov-sud amaliyotidagi ziddiyatlar o‘rganilgan. Shuningdek, kiberfirgarlikni kompyuter texnikasi vositalaridan foydalanib sodir etiladigan boshqa turdosh jinoyatlardan farqlash mezonlari ko‘rsatib o‘tilgan hamda jinoyat qonunchiligini takomillashtirish bo‘yicha amaliy takliflar ilgari surilgan.

Kalit so’zlar: Jinoyat kodeksi, firgarlik, kiberfirgarlik, axborot texnologiyalari, kvalifikatsiya, raqamli dalil, fishing, plastik karta, kiberjinoyat.

Bugungi kunda global raqamlashtirish jarayonlari va moliyaviy texnologiyalarning jadal rivojlanishi an'anaviy jinoyat turlarining ham transformatsiyaga uchrashiga olib keldi. Ayniqsa, axborot-kommunikatsiya texnologiyalaridan foydalangan holda sodir etilayotgan firgarlik, ya’ni kiberfirgarlik jinoyatlari soni yil sayin geometrik progressiya bilan o‘sib bormoqda. O‘zbekiston Respublikasida bank-moliya tizimining raqamlashtirilishi, mobil ilovalar va elektron hamyonlar ommalashuvi natijasida fuqarolarning plastik kartalaridagi mablag‘larini g‘ayriqonuniy ravishda egallash holatlari dolzarb ijtimoiy-huquqiy muammoga aylandi.

Amaldagi O‘zbekiston Respublikasi Jinoyat kodeksining 168-moddasi (Firgarlik) raqamli makonda sodir etilayotgan kiber-jinoyatlarning barcha o‘ziga xos xususiyatlarini to‘liq qamrab olishda bir qator murakkabliklarni yuzaga keltirmoqda. Xususan, fishing saytlari, ijtimoiy muhandislik usullari yoki feyk havolalar orqali fuqarolarni chalg‘itib, ularning maxfiy parollari (SMS-kodlari)ni qo‘lga kiritish holatlarini "aldash yoki ishonchni suiiste'mol qilish" (mulkni ixtiyoriy topshirish) deb baholash va uni Jinoyat kodeksining 169-moddasi (O‘g‘rilik — ya’ni yashirincha talon-toroj qilish) yoki kompyuter texnikasiga oid boshqa jinoyatlar bilan chegaralash (delimitatsiya qilish) masalalarida huquqni qo‘llash amaliyotida yagona yondashuv mavjud emas. Ushbu tadqiqotning maqsadi - axborot-kommunikatsiya texnologiyalariyordamida sodir etiladigan firgarlik jinoyatlarining kriminologik jihatlarini tahlil qilish, ularni kvalifikatsiya qilishdagi mavjud huquqiy bo‘shliqlar hamda tergov-sud amaliyotidagi ziddiyatlarni aniqlash va qonunchilikni takomillashtirishga qaratilgan ilmiy-amaliy takliflarni ishlab chiqishdan iboratdir.

Axborot-kommunikatsiya texnologiyalari yordamida sodir etiladigan firgarlik (kiberfirgarlik) jinoyatlarining o‘ziga xos kriminologik va jinoiy-huquqiy xususiyatlarini tizimli tadqiq etish, shuningdek, ularni amaldagi qonunchilik normalari asosida huquqiy baholashdagi tizimli muammolarni aniqlash maqsadida ushbu ilmiy izlanishda bir-birini to‘ldiruvchi tizimli-strukturali, qiyosiy-huquqiy, kriminologik-statistik va empirik sud amaliyotini o‘rganish metodlari majmuasidan foydalanildi. Tadqiqotning normativ-huquqiy poydevori sifatida O‘zbekiston Respublikasining amaldagi Jinoyat kodeksi, xususan, mulkni aldash yoki ishonchni suiiste’mol qilish yo‘li bilan talon-toroj qilishni tartibga soluvchi 168-moddasi, uning axborot-kommunikatsiya texnologiyalaridan foydalanib sodir etilganlik qismlari hamda O‘zbekiston Respublikasi Oliy sudi Plenumining firgarlik va sud amaliyotida qonun hujjatlarini qo‘llash masalalariga bag‘ishlangan

tegishli qarorlaridagi[1] tushuntirishlar mantiqiy-huquqiy tahlil elagidan o‘tkazildi. Kiberfirgarlik subyektlarining virtual makondagi jinoiy xulq-atvorini va ularning jabrlanuvchilar bilan muloqot mexanizmlarini ilmiy modellashtirishda huquqiy tahlil va sintez metodlaridan keng foydalanilib, kiber-jinoyatlarning tarkibiy elementlari an'anaviy firgarlik jinoyatidan ajratilgan holda o‘rganildi. Tadqiqot doirasida jinoyatchilikning real va obyektiv manzarasini baholash uchun kriminologik-statistik metod tatbiq etilib, O‘zbekiston Respublikasi Ichki ishlar vazirligi Kiberxavfsizlik markazi hamda Bosh prokuratura huzuridagi departament tomonidan taqdim etilgan kiberjinoyatchilik dinamikasi va plastik kartalardan pul mablag‘larini noqonuniy yechib olish holatlariga oid miqdoriy ko‘rsatkichlar statistik guruhlash usullari yordamida qayta ishlandi. Nazariya va real amaliyotning uzviyligini ta’minlash, huquqni qo‘llashdagi kolliziyalarni bevosita tahlil qilish maqsadida empirik metod — sud amaliyotini o‘rganish usuliga alohida urg‘u berildi. Bunda jinoyat ishlari bo‘yicha Toshkent shahar hamda viloyat sudlari tomonidan bank mobil ilovalari orqali fishing va ijtimoiy muhandislik usullarini qo‘llab, fuqarolarning maxfiy SMS-kodlarini aldov yo‘li bilan qo‘lga kiritish hamda hisobvaraqlaridagi mablag‘larni yashirincha boshqa kartalarga o‘tkazish bilan bog‘liq bo‘lgan 25 ta real jinoyat ishi bo‘yicha chiqarilgan sud hukmlari va dastlabki tergov materiallari huquqiy sarmashqqa tortildi. Mazkur empirik tahlil davomida tergov va sud organlarining qilmishni ba'zan Jinoyat kodeksining 168-moddasi (Firgarlik) va ba'zan 169-moddasi (O‘g‘rilik) bilan turlicha kvalifikatsiya qilayotganligi kabi ziddiyatli holatlar aniq misollar yordamida metodologik jihatdan guruhlandi. Xususan, jinoyat ishlari amaliyotida keng uchrayotgan quyidagi holat uslubiy asos qilib olindi: jinoyatchi Click yoki Payme kabi to‘lov tizimlarining soxta (feyk) nusxasini yaratib, fuqaroga Click-premium yutug‘i haqida feyk havola (link) yuboradi; jabrlanuvchi o‘z ixtiyori bilan plastik karta ma'lumotlarini ushbu soxta saytga kiritadi va telefoniga kelgan 5 xonali tasdiqlash kodini ham yozadi; shundan so‘ng jinoyatchi masofadan turib mablag‘larni boshqa hisob raqamga o‘tkazib yuboradi. Ushbu vaziyatda tergov organlarining bir qismi jabrlanuvchi kodni o‘z ixtiyori bilan yozib berganini asos qilib, qilmishni "aldash yo‘li bilan mulkni qo‘lga kiritish", ya’ni JKning 168-moddasi (Firgarlik) deb baholasa, boshqa bir guruh surishtiruvchilar va sudlar pul mablag‘lari bank tizimidan shaxsning ishtirokisiz, yashirincha va masofaviy dasturlar yordamida yechib olinganini ta'kidlab, qilmishni JKning 169-moddasi (O‘g‘rilik) sifatida kvalifikatsiya qilmoqda. Ushbu huquqiy kolliziyani chuqurroq yoritish maqsadida, tadqiqot metodologiyasiga kiberfirgarlikni avtomatlashtirilgan bank tizimlariga ruxsatsiz kirish (JKning 278-2-moddasi — Kompyuter axborotini modifikatsiyalash) va kompyuter tizimlaridan foydalanib sodir etiladigan boshqa turdosh jinoyatlardan chegaralash (delimitatsiya qilish) mezonlari kiritildi. Masalan, jinoyatchi jabrlanuvchini umuman aldamasdan, balki bank dasturidagi texnik zaiflik yoki zararli virusli dasturlar orqali hisob raqamlardan pul yechganda qilmish o‘g‘rilik va kiberjinoyat uyg‘unligi bo‘lishi, ammo shaxsga qo‘ng‘iroq qilib, o‘zini "bank xavfsizlik xizmati xodimi" deb tanishtirib, psixologik bosim va aldov yo‘li bilan parolni olganda (ijtimoiy muhandislik) qilmish kiberfirgarlik ekanligi o‘rtasidagi huquqiy farqlar uslubiy jihatdan tizimlashtirildi. Tadqiqotning qiyosiy-huquqiy yo‘nalishi doirasida esa raqamli makondagi bunday manipulyatsiyalarni qonunan aniq ajratib olgan xorijiy davlatlar, xususan, Germaniya Jinoyat kodeksining 263a-paragrafi (Kompyuter firgarligi)[2] hamda Rossiya Federatsiyasi Jinoyat kodeksining 159.3-moddasi (To‘lov kartalaridan foydalangan holda firgarlik sodir etish) va 159.6-moddasi (Kompyuter axborotidan foydalangan holda firgarlik) kabi maxsus normalarning qonunchilik konstruksiyasi o‘rganildi[3]. Xorijiy tajribaning bunday qiyosiy sarmashqi milliy qonunchilikda virtual manipulyatsiyalar natijasida sodir etiladigan jinoiy qilmishlarni kvalifikatsiya qilishdagi tizimli bo‘shliqlarni to‘ldirish hamda amaliyotda yagona sud interpretatsiyasini yaratishga qaratilgan deduktiv va induktiv xulosalarni shakllantirish uchun ilmiy-uslubiy zamin bo‘lib xizmat qildi.

[1] O‘zbekiston Respublikasi Oliy sudi Plenumining 2017-yil 11-oktabrdagi “Firgarlik bo‘yicha sud amaliyoti to‘g‘risida”gi 35-sonli Qarori.

[2] German Criminal Code (Strafgesetzbuch – StGB) – Paragraph 263a (Computer fraud).

[3]Criminal Code of the Russian Federation – Article 159.3 (Fraud using electronic means of payment) & Article 159.6 (Fraud in the field of computer information).

O‘zbekiston Respublikasi Ichki ishlar vazirligi Kiberxavfsizlik markazi hamda Bosh prokuratura huzuridagi departamentning 2021–2025-yillarga oid statistik ma’lumotlarini hamda 2026-yilning birinchi choragidagi kiberjinoyatchilik dinamikasini tahlil qilish natijasida respublikamizda AKT yordamida sodir etilayotgan firgarlik jinoyatlari soni keskin o‘sganligi aniqlandi[4]. Agarda 2021-yilda kiberjinoyatlar umumiy jinoyatchilikning kichik foizini tashkil etgan bo‘lsa, 2025-yil yakuniga kelib moliya-bank tizimi va plastik kartalar bilan bog‘liq kiberfirgarlik holatlari umumiy mulkiy jinoyatlarning qariyb 40 foizidan ortig‘ini tashkil etgan. Ayniqsa, jinoyatchilarning 65 foizdan ortig‘i fuqarolarning shaxsiy ma'lumotlarini qo‘lga kiritishda to‘g‘ridan-to‘g‘ri texnik xakerlik hujumlaridan emas, balki "ijtimoiy muhandislik" va psixologik chalg‘itish usullaridan foydalanganligi ma'lum bo‘ldi.

Tadqiqot doirasida jinoyat ishlari bo‘yicha sudlarning 25 ta kiberfirgarlikka oid hukmlari o‘rganilganda, huquqni qo‘llash amaliyotida va tergov organlarida qilmishni kvalifikatsiya qilishda uchta asosiy tizimli muammo va ziddiyatlar mavjudligi natija sifatida shakllantirildi.

Birinchi guruh natijalar shuni ko‘rsatdiki, sud-tergov amaliyotining 60 foiz holatlarida fishing saytlari (masalan, soxta "Olimpiada yutuqlari", "Hukumat subsidiyasi" yoki banklarning nusxa ilovalari) orqali plastik karta parolini va SMS-kodini olgan shaxsning harakatlari Jinoyat kodeksining 168-moddasi (Firgarlik) bilan kvalifikatsiya qilingan. Biroq, qolgan 40 foiz holatlarda aynan shunday jinoiy sxema bo‘yicha qo‘zg‘atilgan ishlar sudlar tomonidan JKning 169-moddasi (O‘g‘rilik — ya’ni o‘zganing mulkini yashirincha talon-toroj qilish[5]) toifasiga o‘zgartirilgan. Sudlar buni jabrlanuvchi o‘z pulini o‘z ixtiyori bilan jinoyatchiga o‘tkazib bermaganligi, balki faqat texnik kodni kiritganligi, pulni hisob raqamdan yashirincha yechib olish jarayoni esa bank avtomatlashtirilgan tizimida jabrlanuvchining ishtirokisiz masofadan bajarilganligi bilan asoslagan. Bu esa amaldagi qonunchilikda kiberfirgarlik va kiber-o‘g‘rilik tushunchalarining chegarasi aniq belgilanmaganligidan dalolat beradi.

Ikkinchi muhim natija — AKTdan foydalanib sodir etilgan firgarlikni JKning 278-2-moddasi (Kompyuter axborotini modifikatsiyalash) va 278-5-moddasi (Kompyuter tizimidan qonuniy foydalanishni cheklash) kabi axborot texnologiyalari sohasidagi jinoyatlar majmui bilan kvalifikatsiya qilishda yagona yondashuvning yo‘qligidir. Aniqlanishicha, tergov organlari jinoyatchi jabrlanuvchining Click yoki Payme akkauntiga ruxsatsiz kirib, u yerdagi sozlamalarni o‘zgartirganda (ya’ni axborotni modifikatsiyalash g‘ayriqonuniy sodir bo‘lganda) buni alohida kiberjinoyat sifatida baholamasdan, faqatgina mulkiy zarar yetkazilganligi uchun 168-modda bilan cheklanmoqda. Bu esa jinoyatning ijtimoiy xavflilik darajasiga qonuniy va adolatli baho berilmayotganligini ko‘rsatadi.

Uchinchi guruh natijalar kiberfirgarlik jinoyatining xalqaro (transchegaraviy) xarakterga ega ekanligi bilan bog‘liq. Sud materiallari tahlili shuni ko‘rsatdiki, O‘zbekiston fuqarolarining plastik kartalaridan o‘g‘irlangan mablag‘larning qariyb 35 foizi kiberfirgarlar tomonidan bir necha daqiqa ichida xorijiy davlatlardagi (masalan, Rossiya, BAA yoki offshor hududlardagi) elektron hamyonlar va kriptovaluta (P2P birjalar) hisoblariga o‘tkazib yuborilgan. Amaldagi Jinoyat-prosessual kodeksining raqamli dalillarni olish va xorijiy huquqni muhofaza qilish organlari bilan tezkor axborot almashish mexanizmlari eskirganligi sababli, bunday jinoyatlarning ochilish darajasi va jabrlanuvchiga yetkazilgan real moddiy zararni undirish ko‘rsatkichi an'anaviy firgarlikka qaraganda 3 barobar past ekanligi statistik jihatdan isbotlandi. Tadqiqot davomida aniqlangan statistik ma’lumotlar va sud-tergov amaliyotidagi ziddiyatli holatlar shuni ko‘rsatadiki, amaldagi O‘zbekiston Respublikasi Jinoyat kodeksining 168-moddasi tarkibidagi "axborot-kommunikatsiya texnologiyalaridan foydalanib sodir etilganlik" belgisi bugungi kunning transchegaraviy va ko‘p bosqichli kiber-hujumlariga to‘liq huquqiy baho berishda ojizlik qilmoqda. Blokcheyn texnologiyalari, kripto-aktivlar, fishing va ijtimoiy muhandislik usullari aralashgan jinoyatlarni an’anaviy "aldash yoki ishonchni suiiste’mol qilish" mezonlari bilan kvalifikatsiya qilish

[4] O‘zbekiston Respublikasi Ichki ishlar vazirligi Kiberxavfsizlik markazining 2021–2025-yillardagi kiberjinoyatchilik dinamikasiga oid rasmiy statistik hisobotlari.
[5] Rustambayev M.H. O‘zbekiston Respublikasi jinoyat huquqi kursi. III tom

huquqshunoslik nazariyasida ham, amaliyotda ham jiddiy kolliziyalarni yuzaga keltirmoqda. Eng asosiy muammo — jinoyatchi kompyuter tizimidagi ma'lumotlarni manipulyatsiya qilish orqali inson (jabrlanuvchi)ni emas, balki avtomatlashtirilgan dasturni chalg'itganda qilmishni qanday baholash masalasidir. Xalqaro huquqiy doktrinaga ko'ra, firgarlik muloqotga asoslanadi, biroq kiber-makonda jinoyatchi jabrlanuvchining hisobiga dasturiy kodlar orqali ruxsatsiz kirib pul yechganda, bu harakat o'g'rilikning raqamli ko'rinishiga aylanadi.

Sudlar va tergov organlari o'rtasidagi bunday tarqoq yondashuvlarga chek qo'yish hamda jinoiy qilmishga adolatli baho berish uchun Germaniya va Rossiya kabi rivojlangan davlatlar tajribasidan kelib chiqib, milliy qonunchilikka quyidagi jiddiy konseptual islohotlarni kiritish taklif etiladi:

Birinchidan, Jinoyat kodeksiga alohida **168-1-modda ("Kompyuter axborotidan yoki to'lov vositalaridan foydalangan holda firgarlik sodir etish")** normalarini kiritish va uning dispozitsiyasini quyidagi ko'rinishda shakllantirish lozim. Bunday maxsus moddaning joriy etilishi tergovchilarga fishing va ijtimoiy muhandislik orqali sodir etilgan jinoyatlarni 168 va 169-moddalar o'rtasida sarson qilmasdan, to'g'ridan-to'g'ri va aniq kvalifikatsiya qilish imkonini beradi.

Ikkinchidan, agarda jinoyatchi jabrlanuvchini umuman aldamasdan, balki bank yoki fintex ilovasidagi texnik xatolik yoxud troyan viruslari orqali tizimni buzib kirib pul yechgan bo'lsa, bu harakatni kiberfirgarlik emas, balki raqamli o'g'rilik deb baholash lozim. Shu sababli, **Jinoyat kodeksining 169-moddasi (O'g'rilik) 3-qismiga "b" banti qilib "axborot tizimlariga, bank yoki to'lov dasturlariga ruxsatsiz kirish yoki ulardan qonunga xilof ravishda foydalanish orqali"** degan og'irlashtiruvchi belgi kiritilishi shart. Bu o'g'rilik va firibgarlik o'rtasidagi huquqiy chegarani (delimitatsiyani) qonun darajasida qat'iy belgilab beradi.

Uchinchidan, transchegaraviy kiberfirgarliklarga qarshi kurashish va raqamli dalillarni tezkorlik bilan muzlatish (saqlab qolish) uchun O'zbekiston Respublikasi Jinoyat-prosessual kodeksiga **"Elektron hamyonlar va kripto-aktivlarni xatlashning soddalashtirilgan prosessual tartibi"** haqidagi normalarni qo'shish zarur. Amaliyot shuni ko'rsatmoqdaki, sud sanksiyasini kutish jarayonidagi 24-48 soat vaqt ichida o'g'irlangan mablag'lar xorijiy P2P birjalar orqali yuvib ketilmoqda. Tergovchiga kiber-jinoyat izi aniqlangan zahoti, bank yoki provayderga 48 soatgacha bo'lgan muddatga hisob raqamni vaqtinchalik bloklash (keyinchalik sud tomonidan tasdiqlash sharti bilan) vakolatini berish lozim.

Xulosa o'rnida shuni ta'kidlash joizki, raqamli texnologiyalar shiddat bilan rivojlanayotgan davrda jinoyat qonunchiligining statistik (o'zgarmas) holatda qolishi kiberjinoyatchilarga huquqiy bo'shliqlardan unumli foydalanishga zamin yaratadi. Taklif etilayotgan jinoiy-huquqiy modifikatsiyalar nafaqat sud va tergov amaliyotini muvofiqlashtiradi, balki fuqarolarning raqamli makondagi mulkiy huquqlari hamda O'zbekistonning kiberxavfsizlik reytinglaridagi mavqeini tubdan mustahkamlaydi. Axborot-kommunikatsiya texnologiyalari yordamida sodir etiladigan firgarlik (kiberfirgarlik) jinoyatlarining kriminologik va jinoiy-huquqiy xususiyatlarini tadqiq etish jarayoni shuni ko'rsatadiki, raqamli makonda shaxs mulkini himoya qilish tizimi bugungi kunda mutlaqo yangicha huquqiy prinsiplarni talab etmoqda. O'tkazilgan tahlillar amaldagi Jinoyat kodeksining an'anaviy normalari va sud-tergov amaliyoti kiberjinoyatchilikning shiddatli transformatsiyasi hamda transchegaraviy xarakteri oldida ma'lum ma'noda huquqiy kolliziyalarga duch kelayotganini empirik jihatdan isbotladi. Xususan, fishing saytlari va ijtimoiy muhandislik mexanizmlari yordamida sodir etilayotgan qilmishlarni kvalifikatsiya qilishda sudlar va dastlabki tergov organlari o'rtasida yagona huquqiy yondashuvning mavjud emasligi fuqarolarning huquqlari himoyasini kuchaytirish va jazolashning adolatlilik prinsipini ta'minlash yo'lidagi asosiy to'siqlardan biri bo'lib qolmoqda.

Tadqiqot natijalaridan kelib chiqib, milliy jinoyat qonunchiligiga alohida maxsus **168-1-modda ("Kompyuter axborotidan yoki to'lov vositalaridan foydalangan holda firgarlik sodir etish")** normasini kiritish, shuningdek, an'anaviy o'g'rilik (169-modda) tarkibini axborot tizimlariga ruxsatsiz kirish orqali sodir etiladigan jinoiy harakatlar bilan to'ldirish lozimligi asoslab berildi. Ushbu qonunchilik modifikatsiyalari jinoyat sanksiyalarining aniqligini ta'minlabgina qolmay, balki huquqni muhofaza qiluvchi organlarga raqamli jinoyatlarni to'g'ri va qisqa muddatlarda

kvalifikatsiya qilish imkonini beradi. Bundan tashqari, Jinoyat-prosessual qonunchiligiga elektron hamyonlar va kripto-aktivlarni vaqtinchalik muzlatish (xatlash) bo‘yicha tezkor-prosessual mexanizmlarning tatbiq etilishi o‘g‘irlangan mablag‘larni xorijiy davlatlarga chiqib ketishidan oldin saqlab qolish va jabrlanuvchilarga yetkazilgan real moddiy zararni qoplash ko‘rsatkichini keskin oshirishga xizmat qiladi.

Yakuniy xulosa o‘rnida ta’kidlash joizki, kiberfirgarlikka qarshi kurashish faqatgina jinoiy jazolarni kuchaytirish bilan cheklanib qolmasligi kerak. Huquqiy islohotlar bilan bir qatorda, mamlakatda fintex xavfsizligini ta'minlash, bank va to‘lov tizimlari operatsiyalarining monitoring (anti-fraud) algoritmlarini takomillashtirish hamda aholining raqamli va huquqiy savodxonligini tizimli ravishda oshirish kompleks chora-tadbirlar rejasining ustuvor yo‘nalishlari bo‘lishi shart. Jinoyat qonunchiligining raqamli voqelikka mos holda dinamik yangilab borilishi O‘zbekiston Respublikasida smart-iqtisodiyot poydevorini mustahkamlash hamda virtual makonda inson huquqlari va qonuniy manfaatlarini mutlaq himoya qilishning eng bosh kafolati bo‘lib qoladi.

Foydalanilgan adabiyotlar ro’yxati:

1.O‘zbekiston Respublikasining Konstitutsiyasi. – Toshkent: O‘zbekiston, 2023.
2.O‘zbekiston Respublikasining Jinoyat kodeksi // O‘zbekiston Respublikasi qonun hujjatlari ma’lumotlari milliy bazasi (Lex.uz).
3.O‘zbekiston Respublikasining Jinoyat-prosessual kodeksi // O‘zbekiston Respublikasi qonun hujjatlari ma’lumotlari milliy bazasi (Lex.uz).
4.O‘zbekiston Respublikasining O‘RQ-560-son "Kiberxavfsizlik to‘g‘risida"gi Qonuni // O‘zbekiston Respublikasi qonun hujjatlari ma’lumotlari milliy bazasi, 2022-y.
5.O‘zbekiston Respublikasining O‘RQ-311-son "Axborotlashtirish to‘g‘risida"gi Qonuni // O‘zbekiston Respublikasi qonun hujjatlari ma’lumotlari milliy bazasi.
6.O‘zbekiston Respublikasi Oliy sudi Plenumining 2017-yil 11-oktabrdagi “Firgarlik bo‘yicha sud amaliyoti to‘g‘risida”gi 35-sonli Qarori.
7.O‘zbekiston Respublikasi Ichki ishlar vazirligi Kiberxavfsizlik markazining 2021–2025-yillardagi kiberjinoyatchilik dinamikasiga oid rasmiy statistik hisobotlari.
8.Rustambayev M.H. O‘zbekiston Respublikasi jinoyat huquqi kursi. III tom: O‘zganing mulkini talon-toroj qilish bilan bog‘liq jinoyatlar. – Toshkent: Ilm-ziyo, 2021. – 412 b.
9.Mirzayev A.B. Kiberjinoyatchilik: tushunchasi, tasnifi va unga qarshi kurashishning jinoiy-huquqiy choralari. – Toshkent: Akademiya, 2024. – 185 b.
10.German Criminal Code (Strafgesetzbuch – StGB) – Paragraph 263a (Computer fraud).
11.Criminal Code of the Russian Federation – Article 159.3 (Fraud using electronic means of payment) & Article 159.6 (Fraud in the field of computer information).