Qabul qilindi: 17-noyabr 2026-yil • Ma’qullandi: 19-noyabr 2026-yil • Nashr qilindi: 21-noyabr 2026-yil

KIBERJINOYATLARNING KRIMINOLOGIK TAVSIFI VA KIBERJINOYATCHI SHAXSI TIPOLOGIYASI

Karimbaev Ersultan Polat ulı
Toshkent davlat yuridik universiteti
«Kiberhuquq» (70420127) mutaxassisligi magistratura talabasi

Annotatsiya. Maqolada kiberjinoyatlarning kriminologik tavsifi O‘zbekiston qonunchiligi, rasmiy statistika, sud amaliyoti va xorijiy tadqiqotlar asosida tahlil qilinadi. Maqsad kiberjinoyatchi shaxsini jinoyat sodir etish usuli va jinoiy tarmoqdagi roli bo‘yicha farqlash hamda milliy qonunchilikdagi bo‘shliqlarni aniqlashdan iborat. Formal-yuridik, qiyosiy-huquqiy (O‘zbekiston, Rossiya, Qozog‘iston), statistik ma’lumotlarni ikkilamchi tahlil qilish va kontent-tahlil metodlari qo‘llanildi. Ichki ishlar vazirligi ma’lumotlari kiberjinoyatchilikning asosiy qismi Jinoyat kodeksining XX¹ bobidagi jinoyatlar emas, axborot texnologiyalari yordamida sodir etiladigan firibgarlik va o‘g‘rilik ekanini ko‘rsatadi, sud amaliyoti esa XX¹ bob bo‘yicha ishlar doirasi torligini tasdiqlaydi. Xorijiy ma’lumotlar asosida xaker, kiberfiribgar va drop ajratildi. Qiyosiy tahlil Rossiya va Qozog‘istondan farqli ravishda O‘zbekistonda drop uchun javobgarlik hali belgilanmaganini, 168 va 169-moddalar o‘rtasidagi chegara esa javobgarlik yoshiga ta’sir qilishini ko‘rsatdi. Drop uchun tabaqalashtirilgan javobgarlik, 56-moddani to‘ldirish va sudlanganlar to‘g‘risidagi umumlashtirilgan statistikani e’lon qilish taklif etiladi.

Kalit so‘zlar: kiberjinoyat; kiberjinoyatchi shaxsi; kriminologik portret; kiberfiribgarlik; drop; latentlik; qiyosiy-huquqiy tahlil.

КРИМИНОЛОГИЧЕСКОЕ ОПИСАНИЕ КИБЕРПРЕСТУПЛЕНИЙ И ТИПОЛОГИЯ ЛИЧНОСТИ КИБЕРПРЕСТУПНИКА

Аннотация. В статье анализируется криминологическая характеристика киберпреступлений на основе законодательства Узбекистана, официальной статистики, судебной практики и зарубежных исследований. Цель состоит в том,

чтобы разграничить личность киберпреступника по способу совершения преступления и его роли в преступной сети, а также выявить пробелы в национальном законодательстве. Применялись формально-юридический, сравнительно-правовой (Узбекистан, Россия, Казахстан), вторичный анализ статистических данных и контент-анализ. Данные МВД показывают, что основная часть киберпреступности - это мошенничество и кражи, совершаемые с помощью информационных технологий, а не преступления, предусмотренные главой XX1 Уголовного кодекса, а судебная практика подтверждает узкий круг дел по главе XX1. На основе зарубежных данных были выделены хакер, кибермошенник и дробь. На основе зарубежных данных были выделены хакер, кибермошенник и дробь. Сравнительный анализ показал, что в отличие от России и Казахстана, в Узбекистане ответственность за драп еще не установлена, а граница между статьями 168 и 169 влияет на возраст ответственности. Предлагается дифференцированная ответственность за drop, дополнить статью 56 и опубликовать обобщенную статистику осужденных.

Ключевые слова: киберпреступность; личность киберпреступника; криминологический портрет; кибермошенничество; drop; латентность; сравнительно-правовой анализ.

CRIMINOLOGICAL DESCRIPTION OF CYBERCRIMES AND TYPOLOGY OF CYBERCRIMINAL IDENTITY

Abstract. This article analyzes the criminological characteristics of cybercrimes based on the legislation of Uzbekistan, official statistics, judicial practice, and foreign studies. The objective is to differentiate the personality of a cybercriminal according to the modus operandi and their role within a criminal network, as well as to identify gaps in national legislation. Formal-legal and comparative-legal methods (comparing Uzbekistan, Russia, and Kazakhstan), secondary analysis of statistical data, and content analysis were applied. Data from the Ministry of Internal Affairs indicate that the vast majority of cybercrime consists of fraud and theft committed using information technologies, rather than offenses stipulated under Chapter XX¹ of the Criminal Code, while judicial practice confirms a narrow scope of cases prosecuted under Chapter XX¹. Based on foreign research, three

offender types were identified: the hacker, the cyber fraudster, and the money mule (drop). Comparative analysis revealed that, unlike in Russia and Kazakhstan, criminal liability for "dropping" (acting as a money mule) has not yet been established in Uzbekistan, and the boundary between Articles 168 and 169 affects the minimum age of criminal responsibility. The study proposes introducing differentiated liability for drops, amending Article 56, and publishing aggregated statistics on convicted offenders.

Keywords: cybercrime; personality of a cybercriminal; criminological profile; cyber fraud; drop (money mule); latency; comparative-legal analysis.

1. Kirish

Kiberjinoyatchilik bugun milliy chegaralar bilan cheklanmaydigan jinoyatchilik turiga aylangan va buni xalqaro huquq ham tan olgan. Yevropa Kengashining 2001-yilgi Budapesht konvensiyasi bu sohadagi birinchi xalqaro shartnoma bo‘lib, kompyuter tizimlariga qarshi va ular yordamida sodir etiladigan qilmishlarni kriminallashtirish standartlarini belgilab bergan [2]. 2024-yil dekabrda BMT Bosh Assambleyasi Kiberjinoyatchilikka qarshi konvensiyani qabul qildi [1]. Konvensiya 2025-yil oktabrda Hanoyda imzolash uchun ochildi va O‘zbekiston nomidan uni Oliy Majlis Qonunchilik palatasi Spikeri N. Ismoilov imzoladi [11].

Ichki ishlar vazirligi ma’lumotiga ko‘ra, 2021–2025-yillarda kiberjinoyatlar soni 4 865 tadan 62 440 taga yetgan [12], 2025-yilda esa ular respublikada sodir etilgan barcha jinoyatlarning 49,6 foizini tashkil etgan [13]. 2026-yilning dastlabki to‘qqiz oyida axborot texnologiyalari yordamida 69 962 ta jinoyat sodir etilgan [14]. 2026-yil mart oyida v tasdiqlandi [7], IIV tizimida esa 2026-yil “Kiberjinoyatlarga qarshi kurashish yili” deb e’lon qilindi [15].

Kiberjinoyatda jinoyatchi va jabrlanuvchi bir-birini ko‘rmaydi, ular turli davlatlarda bo‘lishi mumkin. Bitta sxema bir vaqtda yuzlab odamga zarar yetkazadi: masalan, soxta “Yagona darcha” orqali amalga oshirilgan bitta sxemadan 456 kishi jabr ko‘rgan [16]. Bunday jinoyatlarning latentligi ham yuqori.

Huquqiy tartibga solish esa bu o‘zgarishlardan orqada qolmoqda. Jinoyat kodeksida “kiberjinoyat” tushunchasi yo‘q, kiberjinoyatchi shaxsi bo‘yicha rasmiy statistika e’lon

qilinmaydi. Drop, ya’ni kiberjinoyat sodir etishda o‘z nomidagi bank kartasi, hisob raqami, SIM-kartasi yoki elektron hamyonidan foydalanishga yo‘l qo‘ygan shaxs tushunchasi PQ-153-son qarorda berilgan [8], biroq uning javobgarligi hali qonunda belgilanmagan.

Kiberjinoyatchilarni tiplarga ajratish rus va G‘arb kriminologiyasida yangilik emas, milliy adabiyotda esa yagona portret yondashuvi ustun. Ushbu maqolaning maqsadi xorijda shakllangan farqlashni O‘zbekiston qonunchiligi va mavjud ma’lumotlarga tatbiq etish hamda drop javobgarligini qiyosiy tahlil qilishdan iborat. Maqola uchta savolga javob izlaydi: amaliyotda kiberjinoyatlarning qaysi guruhi ustun; xaker, kiberfiribgar va drop bir-biridan qanday farq qiladi; milliy qonunchilik bu farqni qay darajada hisobga oladi.

2. Adabiyotlar tahlili va metodlar

Rus kriminologiyasida M.A. Prostoserdov kibermakonda iqtisodiy jinoyat sodir etuvchilarni an’anaviy jinoyatlarni internet orqali sodir etuvchilar va xakerlarga ajratgan [17]. R.R. Gayfutdinov shuhratparastlik (тщеславия) motivini tobora g‘arazgo‘ylik (корыстной заинтересованность) siqib chiqarayotganini qayd etgan [18]. M.V. Talan va B.E. Shavaleev esa elektron to‘lov vositalari orqali firibgarlik qiluvchilar orasida ilgari sudlanganlar ulushi yuqoriligini ko‘rsatgan [19].

G‘arb adabiyotida E.R. Leukfeldt va hammualliflari kiberjinoiy tarmoqlarda o‘g‘irlangan mablag‘ni o‘z hisobvarag‘i orqali o‘tkazib beruvchi shaxslar qatlami borligini ko‘rsatgan [20]. Buyuk Britaniya Milliy jinoyatchilik agentligi (NCA) ma’lumotiga ko‘ra, 2015-yilda kompyuter tizimlariga qarshi jinoyatlar bo‘yicha gumon qilinuvchilarning o‘rtacha yoshi 17 bo‘lgan [21]. L. Bekkers, A. Moneva va E.R. Leukfeldt kiberjinoyatchilar an’anaviy jinoyatchilardan alohida guruh ekanini, moliyaviy kiberjinoyatchilar esa an’anaviy jinoyatchilarga yaqinroq ekanini aniqlagan [22].

Milliy adabiyotda mavzu ko‘proq jinoyat-huquqiy va kriminalistik jihatdan o‘rganilgan. A.K. Rasulev Jinoyat kodeksining XX¹ bobi asosida alohida bo‘lim yaratishni taklif qilgan [23], B.B. Murodov va N.A. Xushvaqtova bunday jinoyatlarni tergov qilishda jamoatchilik bilan hamkorlik masalalarini tahlil qilgan [24]. D.R. Do‘smatov kiberjinoyatning odatiy subyektini 16–35 yoshli, ilgari sudlanmagan, kompyuter texnologiyalari bo‘yicha maxsus bilimga ega shaxs sifatida tavsiflagan [25]. Bu tavsif

xorijiy tadqiqotlarda qayd etilgan xaker va kiberfiribgar o‘rtasidagi farqni hisobga olmaydi.

Tadqiqotda Jinoyat kodeksi (XX¹ bob, 17, 56, 167–169-moddalar), huquqbuzarliklar profilaktikasi va kiberxavfsizlik to‘g‘risidagi qonunlar, Prezidentning farmon va qarori tahlil qilindi [3–8]. Normalar 2026-yil 1-noyabr holatiga ko‘ra o‘rganildi. Sud hujjatlari portalida XX¹ bob moddalari bo‘yicha e’lon qilingan qarorlar soni va 278²-modda bo‘yicha qarorlarda qilmishning qanday kvalifikatsiya qilingani o‘rganildi [26].

Formal-yuridik metod orqali kiberjinoyat tarkiblari va ular orasidagi nomuvofiqliklar aniqlandi. Qiyosiy-huquqiy tahlil uchun Rossiya va Qozog‘iston tanlandi, chunki ikkalasi ham 2025-yilda bank kartasi va hisobvarag‘ini boshqa shaxsga berganlik uchun jinoiy javobgarlik belgilagan. Statistik ma’lumotlar IIV rahbarlarining rasmiy bayonotlari va Prezident huzuridagi yig‘ilishlar materiallaridan olindi, chunki kiberjinoyatchilik bo‘yicha alohida statistik to‘plam e’lon qilinmaydi. Rus, ingliz va o‘zbek tillaridagi 70 dan ortiq ilmiy manba ko‘rib chiqildi, ulardan foydalanilganlari ro‘yxatda keltirilgan. Tadqiqot muallifning o‘z so‘rovnomasi yoki jinoyat ishlari materiallariga tayanmaydi, bu uning cheklovi hisoblanadi.

3. Natijalar

3.1. Kiberjinoyatlar tasnifi va determinatsiyasi

“Kiberjinoyatchilik” tushunchasi “Kiberxavfsizlik to‘g‘risida”gi qonunning 3-moddasida berilgan [5], Jinoyat kodeksida bunday atama yo‘q, shu sababli tasnifni kodeks tuzilmasidan kelib chiqib amalga oshiramiz.

Birinchi guruhni axborot tizimining o‘ziga qarshi qaratilgan jinoyatlar tashkil etadi. Ular Jinoyat kodeksining XX¹ bobida (278¹–278⁹-moddalar) jamlangan bo‘lib, kompyuter yoki tarmoqsiz sodir etilishi mumkin emas [3]. Ikkinchi guruh — axborot texnologiyasi faqat vosita bo‘lgan an’anaviy jinoyatlar: o‘zlashtirish yoki rastrata (167-modda 3-qism “g” bandi), firibgarlik (168-modda 3-qism “v” bandi) va o‘g‘rilik (169-modda 3-qism “b” bandi) [3]. 167 va 168-moddalardagi bu bandlar 2026-yil iyun oyida yangi tahrirda bayon etilgan [6].

Statistika ikkinchi guruh ustunligini ko‘rsatadi. 2025-yilda firibgarliklarning 82 foizi va o‘g‘riliklarning 76 foizi kibermakonda sodir etilgan [27], kiberjinoyatlarning qariyb 96

foizi esa elektron to‘lov tizimlari bilan bog‘liq [13]. 2026-yil 17-noyabr holatiga XX¹ bob bo‘yicha e’lon qilingan qarorlarning aksariyati kripto-aktivlar muomalasi to‘g‘risidagi qonunchilikni buzish (673 ta) va kompyuter axborotini modifikatsiyalash (221 ta) bilan bog‘liq. Kompyuter axborotidan ruxsatsiz foydalanish bo‘yicha 43 ta, kompyuter sabotaji bo‘yicha birorta ham qaror yo‘q [26]. Bu raqamlar ishlar sonini emas, barcha instansiyalar qarorlarini bildiradi. 278²-modda bo‘yicha 43 ta qaror 20 ta ishga tegishli bo‘lib, ulardan 17 tasida bu modda firibgarlik, o‘g‘rilik, tovlamachilik yoki o‘zlashtirish bilan birga qo‘llangan [26]. Portal 168 va 169-moddalar bo‘yicha qarorlarni band kesimida ajratmaydi, shu sababli asosiy massa haqidagi xulosa birinchi navbatda IIV ma’lumotlariga tayanadi. Sud amaliyoti esa XX¹ bob bo‘yicha ishlar doirasi torligini va ruxsatsiz kirish odatda mulkni egallash vositasi bo‘lishini ko‘rsatadi. Bizning fikrimizcha, faqat XX¹ bob doirasidagi kriminologik tavsif hodisaning katta qismini chetda qoldiradi.

Determinatsiya omillarini V.A. Bugaev va A.V. Chayka tasnifi [28] hamda rutin faoliyat nazariyasi [29] asosida uch guruhga ajratdik: texnologik omillar jinoyat vositasini, institutsional omillar nazoratning holatini, vaziyatli omillar esa jinoyatchi va nishonning uchrashishini tavsiflaydi.

Texnologik omillar. Anonimlik va masofaviylik jinoyatchini jabrlanuvchidan ham, huquqni muhofaza qiluvchi organlardan ham uzoqlashtiradi. Uning izi esa bir nechta hisobvaraq va to‘lov tizimlari bo‘ylab tarqalib ketadi.

Institutsional omillar. 2025-yilda Toshkent shahrida 16 mingdan ortiq kiberjinoyat qayd etilgan, ularning fosh etilishi 8 foizga ham yetmagan [30]. Respublika bo‘yicha 2026-yilning to‘qqiz oyida 69 962 ta shunday jinoyat qayd etilgan [14], yil boshidan 17 483 ta kiberjinoyat fosh etilgan [15]. Biroq bu ikki ko‘rsatkich bir xil hisob asosida berilganmi, manbalardan aniq emas. Latentlik bo‘yicha rasmiy ko‘rsatkich e’lon qilinmaydi, D.R. Do‘smatov uni 85–95 foiz deb baholaydi [25].

Vaziyatli omillar. Rutin faoliyat nazariyasiga ko‘ra, jinoyat motivlangan jinoyatchi, mos nishon va himoyaning yo‘qligi kesishganda sodir bo‘ladi. E.R. Leukfeldt va M. Yar ma’lumotlariga ko‘ra, onlayn muhitda bu elementlardan eng izchil ta’sir ko‘rsatgani nishonning ko‘rinuvchanligi bo‘lgan, boshqalari esa jinoyat turiga qarab turlicha namoyon

bo‘lgan [29]. Toshkent shahri IIBB ma’lumotiga ko‘ra, kiberfiribgarlik jabrlanuvchilarining qariyb 90 foizi 40 yoshdan 80 yoshgacha bo‘lgan shaxslardir [31]. Bu ko‘rsatkich faqat poytaxtga tegishli va hisoblash usuli e’lon qilinmagan, ammo u jinoyatchilar raqamli ko‘nikmasi kamroq guruhlarni nishonga olayotganini taxmin qilishga asos beradi.

3.2. Kiberjinoyatchining kriminologik portreti: xaker, kiberfiribgar va drop

M.A. Prostoserdov tavsifidagi umumiy kiberjinoyatchi o‘rtacha 24 yoshli, ilgari sudlanmagan, oliy o‘quv yurti talabasi yoki bitiruvchisi bo‘lgan erkakdir [17]. Biroq u tahlil qilgan ishlarda sudlanganlar 22 foizni tashkil etgan va ular asosan an’anaviy kiberjinoyatchilar guruhiga to‘g‘ri kelgan [17].

Quyidagi tiplar ikki xil mezonga tayanadi. Xaker va kiberfiribgar jinoyat sodir etish usuli bo‘yicha ajratiladi: birinchisi texnik bilimga, ikkinchisi ijtimoiy aktiv muloqatga tayanadi. Drop esa jinoiy tarmoqdagi roli bo‘yicha ajratiladi va har ikki sxemada uchrashi mumkin. Shu sababli tiplar bir-birini istisno etmaydi. Ular asosan Rossiya va G‘arb ma’lumotlariga tayanadi, O‘zbekistonda esa sudlanganlar to‘g‘risidagi bunday ma’lumotlar e’lon qilinmaydi, shu sababli model milliy amaliyot uchun gipotezadir.

Xaker. Kompyuter tizimlariga qarshi jinoyat sodir etuvchilar boshqa jinoyatchilarga qaraganda ancha yosh. NCA ma’lumotiga ko‘ra, 2015-yilda bunday ishlar bo‘yicha gumon qilinuvchilarning o‘rtacha yoshi 17 yoshni tashkil qilgan[21]. M.A. Prostoserdov ham xakerlar odatda yoshroq bo‘lib, texnik yo‘nalishdagi oliy o‘quv yurtlari, texnikum yoki kollejlarning talabalari yoki bitiruvchilari ekanini qayd etadi [17]. Yosh xakerlar uchun moliyaviy foyda har doim ham asosiy motiv emas, murakkab vazifani hal qilish va tengdoshlar oldida o‘zini ko‘rsatish istagi ham katta rol o‘ynaydi [21]. O‘zbekistonda ham yosh ishtirokchilar uchraydi: Buxoroda zararli APK(android package kit) fayllar orqali 60 dan ortiq fuqaroning mablag‘ini o‘g‘irlashda 20 yoshga to‘lmagan yigit va uning turli hududlardagi sheriklari ushlangan [32]. Ammo bitta holatdan umumiy xulosa chiqarib bo‘lmaydi.

Kiberfiribgar. Bu toifa xakerdan keskin farq qiladi. M.V. Talan va B.E. Shavaleev keltirgan Rossiya ma’lumotlariga ko‘ra, elektron to‘lov vositalari orqali firibgarlik sodir etganlarning 60 foizi 30–49 yoshda [19]. Ularning taxminan yarmi jinoyat sodir etgan

paytda sudlanganligi tugallanmagan yoki olib tashlanmagan shaxslar bo‘lgan, 30 foizga yaqin jinoyat esa retsidiv holatida sodir etilgan [19]. N.B. Osipyan fikricha, bunday shaxslar kuchli muloqot ko‘nikmalariga ega, texnik bilimi esa yuzaki bo‘ladi [33]. Uning asosiy quroli kompyuter emas, ijtimoiy ko‘nikmalar.

Drop. E.R. Leukfeldt va hammualliflari kiberjinoiy tarmoqlarda o‘g‘irlangan pul boshqa shaxslar hisobvaraqlariga o‘tkazilib, so‘ng naqdlashtirilishini ko‘rsatgan [20]. O‘zbekistonda ham bu sxema uchraydi. Soxta “Yagona darcha” ishida 26 nafar fuqaro nomiga rasmiylashtirilgan 293 ta karta orqali 456 kishidan 1 mlrd so‘mdan ortiq mablag' olingan [16]. Boshqa bir ishda fuqarolar bankda o‘z nomlariga 10 tadan karta ochib, ularni Rossiya fuqarosiga bergan va buning uchun har biri 300 dollar olgan. Ularga kartalar totalizator sayti uchun kerakligi aytilgan, jinoiy pul aylanmasidan esa ular bexabar bo‘lgan [34]. Demak, drop odatda jinoyatning asosiy ijrochisi emas, balki oson almashtiriladigan va qasdi ko‘pincha isbotlanmaydigan ishtirokchidir. Drop shaxsi haqida ijtimoiy-demografik ma’lumot topilmadi.

Shunday qilib, mavjud ma’lumotlar yagona portret o‘rniga yosh, odatda sudlanmagan, texnik bilimli xaker; kattaroq yoshli, ko‘pincha sudlangan, ijtimoiy ko‘nikmalarga tayanuvchi kiberfiribgar va tarmoqning quyi qatlamidagi drop o‘rtasida farqlashga asos beradi.

3.3. Qiyosiy-huquqiy tahlil: O‘zbekiston, Rossiya, Qozog‘iston

Uch davlat qonunchiligi eng ko‘p drop masalasida farq qiladi. Rossiya Federatsiyasida 2025-yil 24-iyundagi 176-FZ-son Federal qonun bilan Jinoyat kodeksining 187-moddasi 3–6-qismlar bilan to‘ldirildi va ular 2025-yil 5-iyuldan kuchga kirdi [9; 35]. Elektron to‘lov vositasini yoki unga kirish imkoniyatini g‘arazli maqsadda boshqa shaxsga berish va o‘z to‘lov vositasi bilan boshqa shaxs topshirig‘iga ko‘ra qonunga xilof operatsiyalar bajarish uchun 3 yilgacha, begona to‘lov vositalarini egallash yoki berish uchun 6 yilgacha ozodlikdan mahrum qilish nazarda tutilgan. Izohga ko‘ra, birinchi marta sodir etib, tergovga faol yordam bergan shaxs javobgarlikdan ozod qilinadi.

Qozog‘istonda Jinoyat kodeksining 232-1-moddasi 2025-yil 16-sentabrdan kuchga kirgan [10; 36]. U o‘z bank hisobvarag‘iga kirish imkonini qonunga xilof ravishda berganlik

uchun 3 yilgacha, uchinchi shaxslar manfaatida to‘lov va o‘tkazmalarni amalga oshirganlik uchun 5 yilgacha, bunday kirish imkoniyatini egallagan tashkilotchilar uchun 7 yilgacha ozodlikdan mahrum qilishni nazarda tutadi. Bu yerda ham ixtiyoriy xabar bergan va faol yordam ko‘rsatgan shaxs ozod qilinadi [36].

O‘zbekistonda esa 2026-yil 15-noyabr holatiga drop uchun alohida norma yo‘q. PQ-153-son qarorning 5-bandi “a” kichik bandida bunday shaxslar uchun ma’muriy va jinoiy javobgarlik belgilash taklifi ma’qullangan [8]. Tegishli qonun loyihalari 2026-yil 22-iyulda Qonunchilik palatasi tomonidan qabul qilinib, Senatga yuborilgan. Iyul oyida e’lon qilingan ma’lumotlarga ko‘ra, loyihada masofaviy davlat xizmatlaridagi shaxsiy akkauntlar va SIM-kartalarni g‘arazli maqsadda boshqa shaxsga berganlik uchun ma’muriy javobgarlik nazarda tutilgan, bank kartasi yoki hisobvarag‘ini berish esa alohida tilga olinmagan [37; 38]. Bank kartasi bo‘yicha bu holatni huquqiy bo‘shliq deb baholash mumkin.

Ikkinchi muammo javobgarlik yoshi bilan bog‘liq va u kiberjinoyatlarga xos. Jinoyat kodeksining 17-moddasiga ko‘ra, o‘g‘rilik uchun javobgarlik 14 yoshdan, firibgarlik va XX[1] bob jinoyatlari uchun esa 16 yoshdan boshlanadi [3]. Kartadagi pulni masofadan egallashning o‘zi usuliga qarab ikki xil baholanishi mumkin: jabrlanuvchini aldab olingan bo‘lsa, 168-modda 3-qism “v” bandi, axborot tizimiga ruxsatsiz kirib olingan bo‘lsa, 169-modda 3-qism “b” bandi qo‘llanadi. Natijada 15 yoshli shaxsning javobgarligi qilmishning qaysi moddaga kvalifikatsiya qilinishiga bog‘liq bo‘lib qoladi, amaliyotda esa bu chegara doim ham aniq emas.

Uchinchi masala jazoni og‘irlashtiruvchi holatlarga tegishli. Jinoyat kodeksining 56-moddasida axborot texnologiyalaridan foydalanib jinoyat sodir etish og‘irlashtiruvchi holat sifatida ko‘rsatilmagan, bu belgi faqat 167–169-moddalarda 3-bo‘limida tegishli bandlar sifatida mavjud [3]. PQ-153-son qarorning 5-bandi “d” kichik bandida uni javobgarlik va jazoni og‘irlashtiruvchi holat sifatida belgilash taklifi ma’qullangan [8], biroq bu hali kodeksga kiritilmagan. Natijada boshqa jinoyatlar internet orqali sodir etilganda bu holat jazo tayinlashda og‘irlashtiruvchi holat sifatida hisobga olinmaydi.

4. Muhokama

Kiberjinoyatchilikda firibgarlik va o‘g‘rilik ustunligining sabablaridan biri, jamiyatta

jabrlanuvchini aldash uchun yuqori texnik malaka talab etilmaydi, drop kartalar esa pul evaziga topiladi [34]. XX¹ bob bo‘yicha qarorlarda kripto-aktivlar ishlarining ustunligi esa, ehtimol, shu yo‘nalishdagi faol aniqlash amaliyotini aks ettiradi.

NCA ma’lumotiga ko‘ra, Buyuk Britaniyada bunday jinoyatchilar qo‘lga tushish xavfini past deb biladi [21]. Toshkentdagi past fosh etilish [30] bizda ham shunday idrok shakllanishi mumkinligini taxmin qilishga imkon beradi, ammo bu alohida o‘rganilmagan.

Portret bo‘yicha natijalar D.R. Do‘smatov taklif etgan 16–35 yoshli, sudlanmagan shaxs obrazi [25] xakerga yaqin, ammo kiberfiribgarga to‘liq mos kelmasligini ko‘rsatadi: Rossiya ma’lumotlariga ko‘ra, bu toifaning katta qismi 30–49 yoshda va ularning salmoqli qismi ilgari sudlangan [19]. Agar bu farq O‘zbekiston ma’lumotlarida ham tasdiqlansa, profilaktika ikki yo‘nalishda qurilishi kerak: yosh xakerlar uchun ta’lim muassasalari orqali erta profilaktika, kiberfiribgarlar uchun esa retsidivning oldini olish. “Huquqbuzarliklar profilaktikasi to‘g‘risida”gi qonunda esa kiberjinoyatlarga xos profilaktika choralari alohida nazarda tutilmagan [4].

Drop masalasida Qozog‘iston tajribasidan foydalanish mumkin. U yerda yangi modda kiritilgunga qadar droplar odatda guvoh sifatida, qasdi isbotlangandagina firibgarlik ishtirokchisi sifatida javobgarlikka tortilgan [36]. O‘zbekistonda ham alohida tarkib bo‘lmagani sababli dropni faqat qasdi isbotlangan holda firibgarlik yoki o‘g‘rilikda ishtirokchi sifatida javobgarlikka tortish mumkin. Pul o‘tkazuvchilar kiberjinoiy tarmoqning muhim bo‘g‘ini bo‘lgani uchun [20] aynan shu bo‘g‘inga ta’sir qilish butun sxemani qimmatlashtiradi. PQ-153-son qarorda droplar reyestrini yuritish ham nazarda tutilgan [8]. Bizning fikrimizcha, faqat ma’muriy javobgarlik yetarli emas, chunki drop tarmoqning almashtiriladigan qatlami bo‘lib, jarima uni ishtirok etishdan qaytarmaydi.

Loyihadagi xavfsizlik talablarini bajarmagan bank firibgarlik zararini qoplashi to‘g‘risidagi norma [37] esa rutin faoliyat nazariyasidagi himoya elementiga ta’sir qiluvchi vaziyatli profilaktika chorasidir [29].

Javobgarlik yoshi masalasida D.R. Do‘smatov ayrim kiberjinoyatlar uchun yoshni 14 ga tushirishni taklif etadi [25]. Bu taklifga qisman qo‘shilish mumkin. 168 va 169-moddalar o‘rtasidagi nomuvofiqlikni bartaraf etish kerak, biroq O‘zbekistonda voyaga yetmagan

kiberjinoyatchilar haqida ma’lumot deyarli uchramaydi, XX¹ bob uchun yoshni umumiy pasaytirish yetarlicha asoslanmagan. Avval Oliy sud Plenumi darajasida ikki band o‘rtasidagi chegarani aniqlashtirish, 14–16 yoshlilar uchun esa profilaktikani kuchaytirish maqbulroq. PQ-153-son qarorda voyaga yetmaganlarning bank kartalari bo‘yicha alohida talablar ishlab chiqish ham nazarda tutilgan [8].

Tadqiqotning cheklovlari ham bor: portret bo‘yicha empirik ma’lumotlar asosan Rossiya, Buyuk Britaniya va Niderlandiyaga tegishli, statistika IIV rahbarlarining OAVdagi bayonotlaridan olingan, sud portalidagi hujjatlar esa anonimlashtirilgani sababli ulardan sudlanuvchilarning ijtimoiy-demografik belgilarini aniqlab bo‘lmadi [26].

5. Xulosa

Birinchidan, O‘zbekistonda kiberjinoyatchilikning asosiy qismini XX¹ bob jinoyatlari emas, axborot texnologiyalari yordamida sodir etiladigan firibgarlik va o‘g‘rilik tashkil etadi. Ikkinchidan, xorijiy ma’lumotlar xaker, kiberfiribgar va drop yoshi, sudlanganligi va motivi bo‘yicha farq qilishini ko‘rsatadi. Uchinchidan, milliy qonunchilik bu farqni qisman hisobga oladi: dropning javobgarligi belgilanmagan, 17-moddadagi yosh chegarasi usulga qarab turlicha ishlaydi, 56-modda esa axborot texnologiyalaridan foydalanishni og‘irlashtiruvchi holat sifatida nazarda tutmaydi.

Natijalardan kelib chiqib, quyidagi takliflarni ilgari suramiz.

1) Jinoyat kodeksining atamalarning huquqiy ma’nosiga bag‘ishlangan bo‘limiga “axborot texnologiyalaridan foydalanib sodir etilgan jinoyat” tushunchasini kiritish va uni “Kiberxavfsizlik to‘g‘risida”gi qonundagi ta’rif bilan muvofiqlashtirish [3; 5].

2) Drop uchun tabaqalashtirilgan javobgarlik belgilash va unga bank kartasi hamda hisobvarag‘ini berishni ham kiritish. Birinchi marta va g‘arazsiz sodir etilgan holatlar uchun ma’muriy, g‘arazli yoki takroriy holatlar uchun jinoiy javobgarlik nazarda tutilishi, Rossiya va Qozog‘iston tajribasidagi kabi tergovga faol yordam bergan shaxs javobgarlikdan ozod qilinishi lozim [9; 10].

3) Oliy sud Plenumi qarori bilan 168-modda 3-qism “v” bandi va 169-modda 3-qism “b” bandini farqlash mezonlarini aniqlashtirish hamda 14–16 yoshlilar orasida kiberjinoyatlar profilaktikasini kuchaytirish [3].

4) 56-moddaga “jinoyatni axborot texnologiyalaridan foydalanib sodir etish” holatini qo‘shish. Bu holat axborot texnologiyalaridan foydalanish malakalovchi belgi sifatida nazarda tutilmagan jinoyatlarga nisbatan qo‘llanishi kerak [3; 8].

Foydalanilgan adabiyotlar ro‘yxati

Normativ-huquqiy hujjatlar

1. Kiberjinoyatchilikka qarshi Birlashgan Millatlar Tashkilotining konvensiyasi: BMT Bosh Assambleyasining 2024-yil 24-dekabrdagi 79/243-son rezolyutsiyasi bilan qabul qilingan. URL: https://www.unodc.org/unodc/en/cybercrime/convention/home.html

2. Kiberjinoyatchilik to‘g‘risidagi konvensiya: Budapesht, 2001-yil 23-noyabr // Yevropa Kengashi shartnomalari seriyasi. № 185.

3. O‘zbekiston Respublikasining Jinoyat kodeksi: 1994-yil 22-sentabrda tasdiqlangan // Qonunchilik ma’lumotlari milliy bazasi. URL: https://lex.uz/docs/-111453.

4. “Huquqbuzarliklar profilaktikasi to‘g‘risida”: O‘zbekiston Respublikasining 2014-yil 14-maydagi O‘RQ-371-son Qonuni // Qonunchilik ma’lumotlari milliy bazasi. URL: https://lex.uz.

5. “Kiberxavfsizlik to‘g‘risida”: O‘zbekiston Respublikasining 2022-yil 15-apreldagi O‘RQ-764-son Qonuni // Qonunchilik ma’lumotlari milliy bazasi. URL: https://lex.uz.

6. “O‘zbekiston Respublikasining ayrim qonun hujjatlariga korrupsiyaga qarshi kurashish samaradorligini oshirishga, korrupsiyaga oid jinoyatlar uchun javobgarlik muqarrarligini ta’minlashga qaratilgan qo‘shimcha va o‘zgartirishlar kiritish to‘g‘risida”: O‘zbekiston Respublikasining 2026-yil 22-iyundagi O‘RQ-1155-son Qonuni // Qonunchilik ma’lumotlari milliy bazasi. URL: https://www.lex.uz/uz/docs/-8282286.

7. “O‘zbekiston Respublikasining Kiberxavfsizlik strategiyasini belgilash va kiberjinoyatchilikning oldini olish tizimini takomillashtirish to‘g‘risida”: O‘zbekiston Respublikasi Prezidentining 2026-yil 10-martdagi PF-38-son Farmoni // Qonunchilik ma’lumotlari milliy bazasi. URL: https://lex.uz/uz/docs/-8079286.

8. “Axborot texnologiyalari yordamida sodir etiladigan jinoyatlarga qarshi kurashish faoliyatini yanada kuchaytirishga qaratilgan chora-tadbirlar to‘g‘risida”: O‘zbekiston Respublikasi Prezidentining 2025-yil 30-apreldagi PQ-153-son Qarori // Qonunchilik

ma’lumotlari milliy bazasi. URL: https://lex.uz/uz/docs/-7511145.

9. О внесении изменений в статью 187 Уголовного кодекса Российской Федерации: Федеральный закон от 24.06.2025 № 176-ФЗ // КонсультантПлюс. URL: https://www.consultant.ru/document/cons_doc_LAW_508353/.

10. Уголовный кодекс Республики Казахстан от 03.07.2014 № 226-V ЗРК. Ст. 232-1 // Информационно-правовая система нормативных правовых актов Республики Казахстан «Әділет». URL: https://adilet.zan.kz/rus/docs/K1400000226.

Ilmiy adabiyotlar va boshqa manbalar

11. The UN Convention against Cybercrime – the guarantor of a secure digital space // O‘zbekiston milliy axborot agentligi (UzA). URL: https://uza.uz/en/posts/the-un-convention-against-cybercrime-the-guarantor-of-a-secure-digital-space_776279.

12. 2025-yil boshidan buyon o‘zbekistonliklar kiberjinoyatlardan 1 trln 890 mlrd so‘m zarar ko‘rdi — IIV // Gazeta.uz. 2025. 24-dekabr. URL: https://www.gazeta.uz/oz/2025/12/24/cybercrime/.

13. O‘zbekistonda 10 mingdan ortiq shubhali kartalar bloklandi, 1,72 trln so‘m saqlab qolindi // Spot.uz. 2026. 16-iyun. URL: https://www.spot.uz/oz/2026/06/16/cybersecurity/.

14. 2026-yil O‘zbekistonda kiberjinoyatlar oqibatida fuqarolarga 1 trln so‘mdan ortiq zarar yetkazildi // Spot.uz. 2026. 12-oktabr. URL: https://www.spot.uz/oz/2026/10/12/cybercrime/.

15. IIV: joriy yilda 17 ming 483 kiberjinoyat fosh etildi // O‘zbekiston milliy axborot agentligi (UzA). 2026. 13-oktabr. URL: https://uza.uz/oz/posts/iiv-joriy-yilda-17-ming-483-kiberjinoyat-fosh-etildi_921369.

16. Soxta Yagona portal orqali 1 mlrd so‘mdan ortiq pul o‘g‘irlagan guruh ushlandi // Spot.uz. 2026. 17-iyul. URL: https://www.spot.uz/oz/2026/07/17/cyber-fraud/.

17. Простосердов М.А. Экономические преступления, совершаемые в киберпространстве, и меры противодействия им: дис. … канд. юрид. наук: 12.00.08. М., 2016. 232 с.

18. Гайфутдинов Р.Р. К вопросу о типологии личности компьютерных преступников с учетом характера и мотивации их криминальной деятельности //

Вопросы российского и международного права. 2017. Т. 7, № 4А. С. 245–256.

19. Талан М.В., Шавалеев Б.Э. Криминологический анализ личности мошенника в сфере неправомерного использования электронных средств платежа // Вестник Санкт-Петербургского университета. Право. 2023. Т. 14, вып. 1. С. 108–122.

20. Leukfeldt E.R., Kleemans E.R., Stol W.P. A typology of cybercriminal networks: from low-tech all-rounders to high-tech specialists // Crime, Law and Social Change. 2017. Vol. 67, No. 1. P. 21–37.

21. National Crime Agency. Intelligence Assessment: Pathways into Cyber Crime. London: NCA, 2017. 18 p.

22. Bekkers L.M.J., Moneva A., Leukfeldt E.R. Distinct group, distinct traits? A comparison of risk factors across cybercrime offenders, traditional offenders and non-offenders // Psychiatry, Psychology and Law. 2025. DOI: 10.1080/13218719.2025.2546311.

23. Расулев А.К. Противодействие преступлениям в сфере информационных технологий и безопасности в Республике Узбекистан на современном этапе // Бизнес в законе. Экономико-юридический журнал. 2017. № 1. С. 46–53.

24. Murodov B.B., Xushvaqtova N.A. Axborot texnologiyalari sohasida sodir etiladigan jinoyatlarni tergov qilishda jamoatchilik bilan hamkorlik // Yuridik fanlar axborotnomasi. 2022. № 3. B. 65–75.

25. Do‘smatov D.R. Kiberjinoyatchilikka qarshi kurashning jinoyat-huquqiy va kriminologik jihatlari: yurid. fan. bo‘yicha falsafa doktori (PhD) dis. avtoref. Toshkent: TDYU, 2026.

26. Public.sud.uz: jinoyat ishlari bo‘yicha sudlar qarorlari. URL: https://public.sud.uz/report/CRIMINAL.

27. Усиление борьбы с организованной преступностью обсудили у президента // Gazeta.uz. 2026. 12 марта. URL: https://www.gazeta.uz/ru/2026/03/12/combatting-crime/.

28. Бугаев В.А., Чайка А.В. Факторы преступности в сфере компьютерных технологий // Учёные записки Крымского федерального университета им. В.И. Вернадского. Юридические науки. 2019. Т. 5 (71), № 4. С. 139–145.

29. Leukfeldt E.R., Yar M. Applying Routine Activity Theory to Cybercrime: A Theoretical and Empirical Analysis // Deviant Behavior. 2016. Vol. 37, No. 3. P. 263–280.

30. “Qani natija?” Prezident IIVning kiberjinoyatchilikka qarshi kurashish bo‘yicha faoliyatini tanqid qildi // Gazeta.uz. 2026. 27-yanvar. URL: https://www.gazeta.uz/oz/2026/01/27/cyber-crimes/.

31. “Kiberjinoyatlarning 40 foizdan ortig‘i Toshkent shahriga to‘g‘ri kelyapti” — poytaxt IIBB // Gazeta.uz. 2025. 6-noyabr. URL: https://www.gazeta.uz/oz/2025/11/06/kiberjinoyat/.

32. Buxoroda 60 dan ortiq fuqaroning pullarini APK fayllar orqali o‘g‘irlagan shaxslar ushlandi // Spot.uz. 2026. 29-sentabr. URL: https://www.spot.uz/oz/2026/09/29/cybercrime-in-bukhara/.

33. Осипян Н.Б. К вопросу об учете психологических особенностей личности киберпреступника для целей предупредительной деятельности // Виктимология. 2024. Т. 11, № 3. С. 425–433.

34. G‘ijduvon hokimidan MSK raisigacha – kiberfiribgarlar kimlarni qanday chuv tushirgan? // Kun.uz. 2026. 11-iyul. URL: https://kun.uz/news/2026/07/11/gijduvon-hokimidan-msk-raisigacha-kiberfiribgarlar-kimlarni-qanday-chuv-tushirgan-17f887.

35. Уголовный кодекс дополнили нормами об ответственности для дропперов // Гарант.ру. 2025. 25 июня. URL: https://www.garant.ru/news/1824569/.

36. Дропперов будут привлекать к уголовной ответственности // Uchet.kz. 2025. 16 сентября. URL: https://uchet.kz/news/dropperov-budut-privlekat-k-ugolovnoy-otvetstvennosti/.

37. Kiberjinoyatlarga qarshi kurashga oid ikkita qonun loyihasi Senatga yuborildi // Spot.uz. 2026. 22-iyul. URL: https://www.spot.uz/oz/2026/07/22/combating-cybercrime.

38. Akkaunt va SIM-kartani boshqaga berganlik uchun javobgarlik joriy etilishi mumkin // Sputnik O‘zbekiston. 2026. 22-iyul. URL: https://oz.sputniknews.uz/20260722/akkaunt-sim-karta-javobgarlik-qonun-loyiha-59189148.html.