BANK KARTALARI ORQALI FIRIBGARLIK: KRIMINOLOGIK TAHLIL

(O‘ZBEKISTON MISOLIDA)

Avazbek Sayfiddinov

Toshkent davlat yuridik universiteti Jinoiy-odil sudlov fakulteti Tadqiqot markazi kichik ilmiy xodimi

avazbeksayfiddinov23@gmail.com

Annotatsiya. Ushbu maqolada bank kartalari orqali sodir etilayotgan firibgarlik jinoyatlarining kriminologik xususiyatlari, sodir etilish mexanizmi, jinoyatchi va jabrlanuvchi shaxsining o‘ziga xos jihatlari, shuningdek mazkur jinoyatlarning oldini olishning huquqiy va tashkiliy mexanizmlari tahlil qilinadi. O‘zbekiston Respublikasida bank kartalari orqali firibgarlikning jinoyat-huquqiy asoslari, xususan, Jinoyat kodeksining 168-moddasi, “To‘lovlar va to‘lov tizimlari to‘g‘risida”gi Qonun hamda kiberxavfsizlik sohasidagi normalar qiyosiy-huquqiy jihatdan o‘rganiladi. Bank kartalari bilan bog‘liq firibgarlikning asosiy usullari, jumladan fishing, ijtimoiy muhandislik, SMS-kodlarni qo‘lga kiritish, zararli ilovalar, onlayn savdo va jabrlanuvchi nomiga onlayn kredit rasmiylashtirish kabi usullar kriminologik nuqtai nazardan yoritiladi. Shuningdek, Yevropa Ittifoqining kuchli mijoz autentifikatsiyasi hamda Buyuk Britaniyaning APP-firibgarligidan jabrlangan shaxsga mablag‘larni qaytarish mexanizmi O‘zbekiston amaliyoti bilan taqqoslanadi. Tadqiqot natijasida bank kartalari orqali firibgarlikning oldini olish faqat fuqarolarning ehtiyotkorligini oshirish bilan cheklanmasligi, balki banklar, to‘lov tashkilotlari, telekommunikatsiya operatorlari va huquqni muhofaza qiluvchi organlar o‘rtasidagi tezkor axborot almashinuvi, antifrod monitoringi va mablag‘larni zudlik bilan bloklash mexanizmlarini kuchaytirish zarurligi asoslantiriladi.

Keywords: bank kartasi, firibgarlik, kiberfiribgarlik, kriminologik tahlil, ijtimoiy muhandislik, fishing, OTP-kod, antifrod tizimi, elektron to‘lovlar, raqamli dalillar, bank xavfsizligi, jinoyat profilaktikasi.

Kirish.

Raqamli iqtisodiyotning jadal rivojlanishi bank xizmatlaridan foydalanish imkoniyatlarini kengaytirib, naqd pulsiz to‘lovlarni kundalik iqtisodiy munosabatlarning asosiy vositalaridan biriga aylantirmoqda. Biroq moliyaviy operatsiyalarning raqamli shaklga o‘tishi jinoyatchilikning yangi usullarini ham yuzaga keltirmoqda. Bank kartalari bilan bog‘liq firibgarlik shular jumlasidan bo‘lib, uning xavfliligi nafaqat yetkazilgan moddiy zararda, balki jinoyatning tezkorligi, anonimligi, transmilliyligi va jabrlanuvchini psixologik manipulyatsiya qilish imkoniyatida namoyon bo‘ladi.

O‘zbekistonda muammoning ko‘lami ayniqsa jiddiy tus olgan. Ichki ishlar vazirligi ma’lumotlariga ko‘ra, 2019-yilda axborot texnologiyalaridan foydalanib 18 turdagi 863 ta jinoyat qayd etilgan bo‘lsa, 2024-yilda 62 turdagi 58 800 ta kiberjinoyat qayd etilgan. 2024-yilda kiberjinoyatlarning umumiy jinoyatchilikdagi ulushi 44,4 foizga yetgan, ularning 98 foizini bank kartalari bilan bog‘liq kibero‘g‘rilik va kiberfiribgarlik tashkil etgan.[1] 2026-yil mart oyida taqdim etilgan ma’lumotlarga ko‘ra, 2025-yilda sodir etilgan firibgarlik jinoyatlarining 82 foizi kibermakonda sodir etilgan.[2] Mazkur ko‘rsatkichlar bank kartalari orqali firibgarlikni oddiy maishiy yoki internet firibgarligi sifatida emas, balki mustaqil kriminologik muammo sifatida o‘rganishni talab etadi. Tadqiqotning maqsadi - bank kartalari orqali firibgarlikning kriminologik tavsifini aniqlash, uning asosiy determinantalari va sodir etilish usullarini tahlil qilish hamda O‘zbekiston sharoitida samarali profilaktika mexanizmlarini asoslash.

Kriminologik nuqtai nazardan bank kartalari orqali firibgarlikni bank kartasi yoki u bilan bog‘langan raqamli to‘lov vositalari orqali aldash, ishonchni suiiste’mol qilish yoki ijtimoiy muhandislik usullaridan foydalanib jabrlanuvchining pul mablag‘larini egallashga qaratilgan qasddan sodir etiladigan jinoyat faoliyati sifatida tavsiflash mumkin. O‘zbekiston Respublikasi Jinoyat kodeksining 168-moddasida firibgarlik aldash yoki ishonchni suiiste’mol qilish yo‘li bilan o‘zganing mulkini yoki mulkka bo‘lgan huquqni qo‘lga kiritish sifatida belgilangan. Axborot tizimidan, shu jumladan axborot texnologiyalaridan foydalanib sodir etilgan firibgarlik esa kvalifikatsiyalangan holat sifatida nazarda tutilgan.[3] Demak, bank kartalari orqali sodir etiladigan firibgarlikning muhim qismi amaldagi jinoyat-huquqiy model doirasida 168-modda bilan qamrab olinadi. Biroq kriminologik jihatdan mazkur jinoyatni faqat karta rekvizitlarini noqonuniy egallash bilan izohlash noto‘g‘ri. Zamonaviy firibgar ko‘pincha kartaning o‘zini

emas, balki jabrlanuvchining qaror qabul qilish jarayonini nazorat qilishga intiladi. U bank xodimi, davlat organi vakili yoki savdo platformasi xodimi sifatida namoyon bo‘lib, qo‘rquv, shoshilinchlik yoki manfaatdorlikni kuchaytiradi va jabrlanuvchini kerakli ma’lumotni o‘z ixtiyori bilan taqdim etishga undaydi.

2024-yil ma’lumotlariga ko‘ra, kiberjinoyatlarning 60 foizi zararli havolalar va dasturlar orqali bank kartasi yoki mobil qurilma ustidan nazoratni qo‘lga kiritish, 16 foizi esa aldov yo‘li bilan SMS-kod va akkauntlarni boshqarish imkonini beruvchi ma’lumotlarni olish orqali sodir etilgan.[4] Bu ko‘rsatkichlar bank kartalari bilan bog‘liq jinoyatlarda texnik vosita bilan inson omilining o‘zaro bog‘liqligini ko‘rsatadi.

Kriminologik jihatdan jinoyatchining shaxsida texnik ko‘nikmalar bilan bir qatorda psixologik manipulyatsiya qobiliyati ham muhim. Jinoyat sodir etishda telefon raqamlari, soxta profillar, fishing sahifalari, zararli APK-fayllar va boshqa vositalar bir-birini to‘ldiruvchi elementlar sifatida ishlatilishi mumkin. Ayrim holatlarda jinoyatning alohida bosqichlari turli shaxslar o‘rtasida taqsimlanib, bir shaxs jabrlanuvchi bilan aloqa qilsa, boshqasi mablag‘larni qabul qilish va uchinchi shaxs ularni chiqarib yuborish bilan shug‘ullanishi mumkin.

Birinchi guruh - fishing va soxta to‘lov sahifalari. Jabrlanuvchiga bank, davlat organi yoki mashhur savdo platformasi nomidan havola yuborilib, karta raqami, amal qilish muddati, CVV kodi yoki tasdiqlash kodi kiritilishi so‘raladi.

Ikkinchi guruh - ijtimoiy muhandislikka asoslangan telefon firibgarligi. Jinoyatchi o‘zini bank xodimi sifatida tanishtirib, “hisobingizdan shubhali operatsiya qilindi”, “kartangiz bloklanadi” kabi vajlar bilan jabrlanuvchini psixologik bosim ostiga qo‘yadi.

Uchinchi guruh - zararli dastur yoki mobil ilovalar orqali qurilmani nazorat qilish. Bunday holatda jabrlanuvchi soxta ilovani o‘rnatishi natijasida telefon yoki bank ilovasi bilan bog‘liq ma’lumotlar jinoyatchilar qo‘liga o‘tishi mumkin.

To‘rtinchi guruh - onlayn savdo va soxta investitsiya takliflari. Jinoyatchi mavjud bo‘lmagan mahsulotni sotish, oldindan to‘lov olish yoki yuqori daromad va’dasi bilan mablag‘larni o‘zlashtirishga erishadi.

Beshinchi guruh - jabrlanuvchi nomiga onlayn kredit rasmiylashtirish. Bunda shaxsga doir ma’lumotlar, bank ilovasi yoki identifikatsiya vositalaridan noqonuniy foydalanilib, kredit mablag‘i jinoyatchi nazoratidagi hisobvaraqqa yo‘naltiriladi.

Shunday qilib, zamonaviy bank kartalari orqali firibgarlik “karta ma’lumotlarini o‘g‘irlash” modelidan “jabrlanuvchini mablag‘ni o‘zi o‘tkazishga ishontirish” modeliga ham siljimoqda. Bu esa profilaktika choralarini texnik xavfsizlik bilan bir qatorda psixologik va xulq-atvor xavflarini ham hisobga olgan holda tashkil etishni talab qiladi.

Bank kartalari orqali firibgarlikda jinoyatchi shaxsini faqat “kompyuter mutaxassisi” sifatida tasavvur qilish ilmiy jihatdan yetarli emas. Jinoyatning ayrim shakllarida yuqori texnik bilim talab qilinsa, ijtimoiy muhandislikka asoslangan holatlarda kommunikativ va psixologik manipulyatsiya ko‘nikmalari ustunlik qiladi. Shu sababli jinoyatchilarni texnik tayyorgarligi, jinoyatdagi funksiyasi va guruhdagi roliga ko‘ra farqlash maqsadga muvofiq. Jabrlanuvchi masalasida ham “raqamli savodxonligi past shaxs” degan soddalashtirilgan yondashuvdan voz kechish lozim. Firibgarlarning ishonchli brendlar va davlat organlari nomidan foydalanishi, shoshilinch qaror qabul qilishga majburlashi va psixologik bosimni kuchaytirishi natijasida texnik bilimga ega foydalanuvchi ham jinoyat qurboniga aylanishi mumkin.

Shu nuqtai nazardan, viktimologik profilaktika foydalanuvchini ayblashga emas, balki uning zaif vaziyatlarini kamaytirishga qaratilishi kerak. Bank interfeyslarida xavf haqida aniq ogohlantirish, yirik yoki noodatiy tranzaksiyalarda qo‘shimcha tekshiruv, yangi oluvchiga pul yuborishda kechikish va tezkor bloklash imkoniyati jabrlanuvchining xatosi oqibatlarini kamaytirishi mumkin.

Bank kartalari orqali firibgarlikka qarshi kurashning bevosita jinoyat-huquqiy asosi Jinoyat kodeksining 168-moddasidir.[3] Shu bilan birga, to‘lov munosabatlarini tartibga soluvchi 2019-yil 1-noyabrdagi O‘RQ-578-son “To‘lovlar va to‘lov tizimlari to‘g‘risida”gi Qonun bank va to‘lov tizimlarining faoliyat yuritishi uchun huquqiy asos yaratadi.[5] Kiberxavfsizlik bilan bog‘liq munosabatlar esa 2022-yil 15-apreldagi O‘RQ-764-son “Kiberxavfsizlik to‘g‘risida”gi Qonun bilan tartibga solinadi.[6] Amaldagi tizimning asosiy muammolaridan biri - jinoyat sodir etilgandan keyingi javob choralariga nisbatan jinoyat sodir etilishidan oldingi risklarni boshqarish mexanizmlarining yetarli darajada tizimlashtirilmaganidir. Bank kartasidan noqonuniy mablag‘ yechilganidan keyin jinoyatchini aniqlash muhim bo‘lsa-da, dastlabki daqiqalarda tranzaksiyani bloklash ko‘pincha ancha samarali profilaktik natija beradi.

Shu sababli bank va to‘lov tashkilotlarining shubhali tranzaksiyalarni aniqlash, vaqtincha to‘xtatish, mijoz murojaatini tezkor ko‘rib chiqish, elektron

dalillarni saqlash va mablag‘larni qaytarish bo‘yicha aniq algoritmlarini huquqiy jihatdan takomillashtirish zarur.

Yevropa Ittifoqida PSD2 doirasida Strong Customer Authentication (SCA) - kuchli mijoz autentifikatsiyasi joriy etilgan bo‘lib, ayrim elektron to‘lovlarda mijozni bir nechta mustaqil autentifikatsiya elementlari asosida tasdiqlash talab qilinadi.[7] Mazkur mexanizm karta va hisob ma’lumotlarini oddiy o‘g‘irlashga asoslangan ayrim firibgarlik turlarini kamaytirishda samarali bo‘lsa-da, EBA va ECBning 2025-yilgi hisobotida firibgarlarning foydalanuvchini bevosita manipulyatsiya qilishga ko‘proq o‘tayotgani qayd etilgan.[8] Bu tajriba O‘zbekiston uchun muhim xulosani beradi: autentifikatsiya foydalanuvchining shaxsini aniqlashi mumkin, biroq uning qarori firibgar ta’sirida qabul qilingan-qilinmaganini o‘zi bilan o‘zi aniqlay olmaydi. Shu sababli biometrik autentifikatsiya bilan bir qatorda qurilma identifikatsiyasi, tranzaksiya xulq-atvori tahlili va riskka asoslangan antifrod monitoringini rivojlantirish zarur.

Buyuk Britaniyada esa Authorised Push Payment (APP) firibgarligidan jabrlangan shaxslarni himoya qilishga qaratilgan kompensatsiya mexanizmi joriy etilgan. 2024-yil 7-oktabrdan boshlab tegishli holatlarda to‘lov xizmatlari provayderlari jabrlanuvchining yo‘qotilgan mablag‘larini qaytarish majburiyatiga ega bo‘ldi.[9] Mazkur model banklarni nafaqat firibgarlikdan keyingi nizoni hal qilishga, balki firibgarlikni oldindan aniqlashga ham rag‘batlantiradi. O‘zbekiston sharoitida ushbu modelni to‘liq ko‘chirish emas, balki bank, to‘lov tashkiloti va mijozning ehtiyotkorlik darajasini hisobga oluvchi mutanosib kompensatsiya tizimini ishlab chiqish maqsadga muvofiq. Agar bank tizimida tranzaksiyaning g‘ayrioddiyligi yaqqol ko‘rinib turgan bo‘lsa va bank tegishli chorani ko‘rmagan bo‘lsa, bankning javobgarligi masalasi alohida baholanishi mumkin.

Kiberfiribgarlikning transmilliyligi xalqaro hamkorlikni ham talab qiladi. Budapest Convention elektron dalillarni olish, saqlash va davlatlar o‘rtasida hamkorlik qilish uchun muhim huquqiy mexanizmlarni belgilaydi.[10] Uning Ikkinchi Qo‘shimcha protokoli elektron dalillarga transchegaraviy kirish va xizmat ko‘rsatuvchi provayderlar bilan hamkorlikni kuchaytirishga qaratilgan.[11] Bu O‘zbekiston uchun muhim, chunki jinoyatchi, jabrlanuvchi, server, bank hisobi va raqamli dalil turli yurisdiksiyalarda joylashishi mumkin.

Birinchidan, banklar, to‘lov tashkilotlari, telekommunikatsiya operatorlari va huquqni muhofaza qiluvchi organlar o‘rtasida kiberfiribgarlik indikatorlari bo‘yicha tezkor axborot almashinuvi tizimini shakllantirish zarur. Bunda shubhali

telefon raqamlari, hisobvaraqlar, qurilmalar, fishing domenlari va boshqa indikatorlar bo‘yicha avtomatlashtirilgan ma’lumot almashinuvi yo‘lga qo‘yilishi mumkin.

Ikkinchidan, banklarda real vaqt rejimida ishlaydigan antifrod tizimlarini takomillashtirish lozim. Tizim mijozning odatiy tranzaksiyalaridan keskin farq qiluvchi operatsiyalarni, yangi qurilma orqali kirishni, yangi oluvchiga katta miqdordagi pul o‘tkazilishini va boshqa xavf indikatorlarini kompleks baholashi kerak.

Uchinchidan, jabrlanuvchining firibgarlikni aniqlagan zahoti tranzaksiyani bloklash imkoniyatini soddalashtirish kerak. Mijozning murojaati bir vaqtning o‘zida bank, to‘lov tashkiloti va huquqni muhofaza qiluvchi organga yetib boradigan yagona tezkor mexanizm sifatida shakllantirilishi mumkin.

To‘rtinchidan, boshqa shaxslarning bank hisobvaraqlaridan noqonuniy mablag‘larni qabul qilish va tranzit qilish holatlarini aniqlash bo‘yicha risk indikatorlarini kuchaytirish lozim. Qisqa vaqt ichida ko‘plab shaxslardan mablag‘ qabul qilish, ularni tezda boshqa hisobvaraqlarga o‘tkazish kabi xatti-harakatlar antifrod monitoringining predmeti bo‘lishi kerak.

Beshinchidan, aholining moliyaviy va kiberxavfsizlik savodxonligini real ssenariylar asosida oshirish zarur. “OTP-kodni bermang” kabi umumiy tavsiyadan tashqari, bank xodimi nomidan qo‘ng‘iroq qilinganda nima qilish, soxta havolani qanday aniqlash va mablag‘ noqonuniy yechilganda qaysi ketma-ketlikda harakat qilish kabi amaliy ko‘nikmalar o‘rgatilishi kerak.

Xulosa. Bank kartalari orqali firibgarlik O‘zbekistonda raqamli iqtisodiyotning rivojlanishi bilan birga kuchayib borayotgan murakkab kriminologik hodisadir. Uning o‘ziga xosligi jinoyatchining ko‘pincha masofadan turib harakat qilishi, jabrlanuvchining o‘zini tranzaksiyani tasdiqlashga undashi va mablag‘larning juda qisqa vaqtda boshqa hisobvaraqlarga o‘tkazilishi bilan belgilanadi.

Tahlil shuni ko‘rsatadiki, jinoyatga qarshi kurashni faqat jazo choralarini kuchaytirish bilan cheklash yetarli emas. Jinoyat sodir etilishidan oldingi bosqichda riskni aniqlash, shubhali tranzaksiyani vaqtincha to‘xtatish, mablag‘larni saqlab qolish va raqamli dalillarni tezkor mustahkamlash samaraliroq yondashuvdir.

Tadqiqot natijasida quyidagi takliflar ilgari suriladi: banklar va huquqni muhofaza qiluvchi organlar o‘rtasida yagona tezkor axborot almashinuvi tizimini

yaratish; shubhali tranzaksiyalarni real vaqt rejimida aniqlash va qisqa muddatga kechiktirishning huquqiy mexanizmini ishlab chiqish; jabrlanuvchi mablag‘larini qaytarish bo‘yicha mutanosib kompensatsiya tizimini joriy etish; “tranzit” hisobvaraqlarni aniqlashning antifrod mezonlarini kuchaytirish; elektron dalillarni tezkor saqlash va xalqaro almashish mexanizmlarini rivojlantirish; aholining kiberhuquqiy savodxonligini amaliy ssenariylar asosida oshirish.

Shunday qilib, O‘zbekiston uchun eng maqbul model - jinoiy-huquqiy javobgarlik, bank xavfsizligi, antifrod texnologiyalari, tezkor tashkiliy hamkorlik va viktimologik profilaktikani birlashtiruvchi kompleks tizimdir. Bunday model bank kartalari orqali firibgarlikni sodir etilgan jinoyat sifatida qayd etishdan ko‘ra, uni sodir etilishidan oldin aniqlash va to‘xtatishga ustuvor ahamiyat beradi.

ADABIYOTLAR

1. O‘zbekiston Respublikasining Jinoyat kodeksi. 168-modda - Firibgarlik.

2. O‘zbekiston Respublikasining 2019-yil 1-noyabrdagi O‘RQ-578-son “To‘lovlar va to‘lov tizimlari to‘g‘risida”gi Qonuni.

3. O‘zbekiston Respublikasining 2022-yil 15-apreldagi O‘RQ-764-son “Kiberxavfsizlik to‘g‘risida”gi Qonuni.

4. O‘zbekiston Respublikasi Ichki ishlar vazirligi. Kiberxavfsizlik markazi ma’lumotlari va kiberjinoyatchilik statistikasi, 2019–2024-yillar.

5. O‘zbekiston Respublikasi Prezidenti rasmiy veb-sayti. “Uyushgan jinoyatchilik va kiberjinoyatlarga qarshi kurashish takomillashtiriladi”. 12.03.2026.

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

7. European Banking Authority, European Central Bank. Joint EBA-ECB Report on Payment Fraud. 2025.

8. Payment Systems Regulator. Annual Report and Accounts 2024/25. United Kingdom.

9. Council of Europe. Convention on Cybercrime (Budapest Convention), ETS No. 185.

10. Council of Europe. Second Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence, CETS No. 224. 2022.

11. United Nations Office on Drugs and Crime. Materials on cybercrime, electronic evidence and international cooperation.