O‘ZBEKISTON RESPUBLIKASIDA BANK KARTALARI FIRIBGARLIGINING ZAMONAVIY HOLATI VA ANTIFROD TIZIMINI TAKOMILLASHTIRISH YO‘LLARI

Jabborov Furqat Raximjon O‘g‘li
O‘zbekiston Respublikasi Huquqni muhofaza qilish akademiyasi magistranti

Annotatsiya
Mazkur maqolada O‘zbekiston Respublikasida bank kartalari bilan bog‘liq firibgarlikning zamonaviy holati rasmiy statistik ma’lumotlar asosida tahlil qilingan. Firibgarlikning asosiy turlari va ularning O‘zbekistondagi tarqalishi o‘rganilib, ijtimoiy muhandislikning ustuvor xususiyati empirik jihatdan asoslangan. Muallif tomonidan bank kartasi firibgarligi xavfini baholashning ko‘p qatlamli (gibrid) modeli va antifrod tizimini takomillashtirish bo‘yicha ilmiy-amaliy takliflar ishlab chiqilgan.

Kalit so‘zlar: bank kartasi firibgarligi, antifrod tizimi, phishing, ijtimoiy muhandislik, SIM-swap, mashinali o‘rganish, xulq-atvor tahlili, gibrid model.

Kirish

O‘zbekiston Respublikasida raqamli to‘lovlar infratuzilmasi jadal kengaymoqda: muomaladagi bank kartalari soni so‘nggi uch yil ichida ikki baravarga ko‘payib, 2025-yil oxiriga kelib 63 milliondan oshdi. Ayni paytda bank kartalari bilan bog‘liq firibgarlik ham keskin o‘sib bormoqda. Ushbu maqolada O‘zbekistondagi bank kartalari firibgarligining zamonaviy holati statistik ma’lumotlar asosida tahlil qilinib, antifrod tizimini takomillashtirish bo‘yicha ilmiy-amaliy yondashuvlar taklif etiladi.

Bank kartalari firibgarligining zamonaviy holati

Ichki ishlar vazirligi ma’lumotlariga ko‘ra, O‘zbekistonda kiberjinoyatlar soni so‘nggi besh yilda 68 baravardan ortiqqa ko‘paygan: 2019-yilda 863 ta jinoyat qayd etilgan bo‘lsa, 2024-yilda bu ko‘rsatkich 58 800 taga yetdi. Kiberjinoyatlarning umumiy jinoyatchilikdagi ulushi 2023-yildagi 6,2 foizdan 2024-yilda 44,4 foizga ko‘tarildi. 2021–2024 yillarda fuqarolarning 1,9 trillion so‘mdan ortiq mablag‘i talon-toroj qilingan.

Statistikaning eng muhim jihati — kiberjinoyatlarning 98 foizi aynan bank kartalari bilan bog‘liqligidir. Jinoyatlarning sodir etilish usullari quyidagicha taqsimlangan: 60 foizi — zararli havola va dasturlar orqali karta yoki qurilma boshqaruvini qo‘lga kiritish; 16 foizi — aldov bilan SMS-kod (OTP)ni qo‘lga kiritish; 11 foizi — onlayn savdo platformalaridagi firibgarliklar; 9 foizi — soxta investitsiya sxemalari; 4 foizi — onlayn-kredit firibgarligi. Ushbu taqsimot shuni ko‘rsatadiki, O‘zbekiston sharoitida eng katta tahdid texnik zaiflikdan emas, balki ijtimoiy muhandislikdan — fuqaroning o‘zini aldab, ma’lumotni ixtiyoriy ravishda topshirishga undash usulidan kelib chiqadi.

Bank kartasi firibgarligining asosiy turlari

Bank kartasi firibgarligining turlarini texnik, aralash va ijtimoiy-psixologik guruhlarga ajratish mumkin. Texnik usullarga skimming (magnit yo‘lakcha ma’lumotlarini nusxalash) va shimming (chip ma’lumotlarini ushlab qolish) kiradi. Ijtimoiy-psixologik usullarga phishing, vishing, smishing va boshqa ijtimoiy muhandislik shakllari kiradi. Aralash usullarga esa carding, SIM-swap (operatorni aldab telefon raqamini egallash) va ATO — hisob qaydnomasini to‘liq egallab olish kiradi. Muhim jihati shundaki, ushbu turlar bir-biridan ajralgan emas, balki zanjir bo‘lib amalga oshiriladi: phishing orqali

ma’lumot olish, SIM-swap orqali OTP-kodni ushlash va ATO orqali pulni yechib olish ketma-ketligi tipik jinoiy stsenariydir.

Antifrod tizimining hozirgi holati va cheklovlari

O‘zbekiston Respublikasida 2025–2026 yillarda antifrod tizimlarini joriy etish bo‘yicha bir qator normativ hujjatlar qabul qilindi. Markaziy bankning yangi nizomlari antifrod tizimini uch darajaga — session antifrod, tranzaksion antifrod va uyali aloqa darajasidagi nazoratga — ajratadi. Shu bilan birga, mavjud tizimlarning bir qator cheklovlari saqlanib qolmoqda: ular asosan qoidalarga asoslangan yondashuvga tayanadi, mashinali o‘rganish modellari hali keng joriy etilmagan; banklararo ma’lumot almashinuvi cheklangan; eng muhimi — ijtimoiy muhandislik holatlarida operatsiya haqiqiy foydalanuvchining o‘z qurilmasidan amalga oshirilgani uchun an’anaviy antifrod samarasiz qoladi.

Antifrod tizimini takomillashtirish bo‘yicha mualliflik takliflari

Aniqlangan cheklovlardan kelib chiqib, bank kartasi firibgarligi xavfini baholashning ko‘p qatlamli (gibrid) modeli taklif etiladi. Ushbu modelda operatsiya ketma-ket uch qatlamdan o‘tadi: birinchi qatlam — qoidalarga asoslangan tezkor filtr; ikkinchi qatlam — mashinali o‘rganish modeli (operatsiyaga risk-ball beradi); uchinchi qatlam — ijtimoiy muhandislikka yo‘naltirilgan xulq-atvor tahlili. Aynan uchinchi qatlam O‘zbekiston sharoiti uchun kalit ahamiyatga ega, chunki u texnik emas, balki xatti-harakat indikatorlarini — parallel telefon sessiyasi, operatsiyaning ikkilanib kechishi, yangi qabul qiluvchiga birinchi yirik o‘tkazma kabilarni — baholaydi.

Bundan tashqari, quyidagi takliflar ilgari suriladi: Markaziy bank huzurida banklararo yagona antifrod axborot almashinuvi platformasini tashkil etish; antifrod modelining samaradorligini baholashda oddiy “aniqlik” o‘rniga precision, recall va F1-ball kabi nomutanosib ma’lumotlarga sezgir mezonlardan foydalanish; sun’iy intellekt qo‘llanilganda “tushuntiriladigan SI” (explainable AI) prinsipiga rioya qilish; xorijiy tajriba (Singapur, Buyuk Britaniya) asosida mobil operatorlarni javobgarlik zanjiriga kiritish.

Xulosa

O‘zbekiston Respublikasida bank kartalari firibgarligi eksponensial sur’atda o‘sayotgan jiddiy muammoga aylangan. Statistik tahlil shuni ko‘rsatadiki, eng katta tahdid — texnik zaiflik emas, balki inson omili va ijtimoiy muhandislikdir. Shu sababli antifrod tizimini takomillashtirish faqat texnik emas, balki xulq-atvor tahlilini ham qamrab oluvchi kompleks yondashuvni talab etadi. Taklif etilgan ko‘p qatlamli gibrid model va unga hamroh tashkiliy choralar O‘zbekistonning o‘ziga xos sharoitini hisobga olgan holda ishlab chiqilgan bo‘lib, ularning joriy etilishi bank kartalari firibgarligining ko‘lamini kamaytirishga xizmat qilishi mumkin.

Foydalanilgan adabiyotlar

1. O‘zbekiston Respublikasi tijorat banklarining axborot xavfsizligi va kiberxavfsizligiga doir minimal talablar to‘g‘risidagi nizom. O‘zR Adliya vazirligi, 18.08.2025, ro‘yxat raqami 3669. // URL: https://lex.uz/uz/docs/-7689673
2. Masofadan moliyaviy xizmatlar ko‘rsatishda axborot va kiberxavfsizlikni ta’minlash hamda firibgarlikning oldini olish bo‘yicha minimal talablar to‘g‘risidagi nizom (2026-yil yanvar). // URL: https://lex.uz/pdffile/-8007760

3. “O‘zbekistonda kiberjinoyatlar umumiy jinoyatlarning salkam yarmini tashkil qilyapti” // Gazeta.uz, 05.11.2025. URL: https://www.gazeta.uz/oz/2025/11/05/cybercrime/
4. Bahnsen A.C., Aouada D., Stojanovic A., Ottersten B. Feature Engineering Strategies for Credit Card Fraud Detection // Expert Systems with Applications. – 2016. – Vol. 51. – P. 134–142.
5. Abdallah A., Maarof M.A., Zainal A. Fraud Detection System: A Survey // Journal of Network and Computer Applications. – 2016. – Vol. 68. – P. 90–113.
6. Monetary Authority of Singapore. Combatting Scams — Shared Responsibility Framework (SRF). – MAS, 2024. // URL: https://www.mas.gov.sg/regulation/combatting-scams
7. Rasulev A.X. Moliyaviy kiberjinoyatlarga qarshi kurashning huquqiy asoslari. – Toshkent: TDYuU nashriyoti, 2021. – 220 b.