KIBER-FIRIBGARLIK VA PLASTIK KARTALARDAN PUL O‘G‘IRLANISHI: O‘ZBEKISTONDA ZAMONAVIY TAHDIDLAR, SABABLAR, OQIBATLAR VA HIMOYALANISH USULLARI

Shakirova Nigora Axralovna
Toshkent davlat iqtisodiyot universiteti
Statistika kafedrasi PhD, dotsenti
Elektron pochta: shakirova0130@gmail.com
Orcid: 0009-0006-5025-4764
Ibrohimov Asliddin G'ayratjon o'g'li
Toshkent davlat iqtisodiyot universiteti, “Moliya” fakulteti
E-mail: ibrohimovaslbek82@gmail.com

Annotatsiya

Ushbu tadqiqot ishida O‘zbekiston Respublikasi bank-moliya tizimida jadal raqamlashtirish jarayonlari sharoitida plastik kartalar va masofaviy bank xizmatlari (MBX) orqali sodir etilayotgan kiber-firibgarlik jinoyatlarining ko‘lamiligi, paydo bo‘lish sabablari, tarkibiy tuzilishi hamda ularga qarshi kurashishning zamonaviy mexanizmlari har taraflama tahlil qilingan. Maqolada O‘zbekiston Respublikasi Markaziy banki, IIV Kiberxavfsizlik markazi hamda Statistika agentligining rasmiy ma’lumotlari asosida 2020–2025-yillardagi dinamik o‘zgarishlar o‘rganilgan. Tadqiqot davomida kiberjinoyatlarning turlari bo‘yicha chastotali taqsimoti (gistogramma) va dinamikasi (chastota poligoni) qurilib, statistik qonuniyatlar ko‘rsatib berilgan. Shuningdek, Yevropa Ittifoqi (PSD2/SCA), Buyuk Britaniya (APP Reimbursement) va Singapur (Shared-Responsibility Model) xalqaro tajribasi tahlil qilinib, O‘zbekiston amaliyotiga tatbiq etish imkoniyatlari baholangan. Tadqiqot yakunida bank, telekom operatorlari, regulyator va foydalanuvchilar o‘rtasidagi taqsimlangan mas’uliyat modelini joriy etish bo‘yicha amaliy takliflar ilgari surilgan.

Kalit so'zlar: *kiber-firibgarlik, plastik karta, masofaviy bank xizmatlari, fishing, vishing, SIM-swap, gistogramma, chastota poligoni, taqsimlangan mas'uliyat, antifrod monitoring, SCA, Markaziy bank.*

Abstract

This study comprehensively analyzes the scale, underlying causes, structural composition, and modern mitigation mechanisms of cyber fraud involving payment cards and remote banking services in Uzbekistan against the backdrop of rapid financial sector digitization. Utilizing official statistics from the Central Bank of the Republic of Uzbekistan, the Cybersecurity Center of the Ministry of Internal Affairs, and the National Statistics Agency, the paper examines dynamic shifts from 2020 to 2025. Frequency distributions (histograms) and dynamic trend polygons are constructed to model statistical patterns in cybercrime evolution. International regulatory frameworks—including the EU's PSD2/SCA standards, the UK's APP Fraud Reimbursement scheme, and Singapore's Shared-Responsibility Model—are critically evaluated for local context adaptation. The article concludes with actionable policy recommendations for implementing a shared-responsibility model across commercial banks, telecom operators, regulatory bodies, and end-users.

Keywords: *cyber fraud, payment cards, remote banking, phishing, vishing, SIM-swap, histogram, frequency polygon, shared responsibility, anti-fraud monitoring, SCA, Central Bank.*

1. Kirish va Tadqiqotning Dolzarbligi

So'nggi yillarda O'zbekiston Respublikasida naqd pulsiz hisob-kitoblar ko'lamining keskin kengayishi, to'lov tizimlarining va masofaviy bank xizmatlarining (MBX) ommalashuvi milliy iqtisodiyotning raqamli transformatsiyasini ta'minladi. Biroq, moliya texnologiyalarining (FinTech) jadal rivojlanishi moliya-bank tizimida axborot xavfsizligini ta'minlash va fuqarolarning

plastik karta mablag'larini kiber-tahdidlardan muhofaza qilish masalasini o'tkir dolzarb muammoga aylantirdi.

O'zbekiston Respublikasi Markaziy bankining rasmiy ma'lumotlariga ko'ra, mamlakatimizda muomalaga chiqarilgan bank kartalari soni va to'lov terminallari tarmog'i yildan-yilga ortib bormoqda. Raqamli to'lovlar qulayligi oshgani sayin, kiberjinoyatchilar usullari ham murakkablashib, texnik zaifliklardan ko'ra inson omiliga — ijtimoiy muhandislik (social engineering) va psixologik manipulyatsiyalarga tayanish tamoyili ustuvorlik qilmoqda.

Kiber-firibgarlik oqibatida yetkazilayotgan zarar faqatgina fuqarolarning shaxsiy jamg'armalarini o'g'irlash bilan cheklanib qolmasdan, balki butun bank-moliya tizimiga bo'lgan jamoatchilik ishonchini sarsitadi, raqamli moliya xizmatlarining ommalashuvini sekinlashtiradi va tijorat banklari uchun jiddiylik darajasi yuqori bo'lgan operatsion hamda reputatsion xatarlarni keltirib chiqaradi.

1.1. Tadqiqot maqsadi va vazifalari

Ushbu tadqiqotning maqsadi — O'zbekistonda plastik kartalar va masofaviy to'lov tizimlaridagi kiber-firibgarlik holatlarini kompleks statistik, huquqiy va texnik tahlil qilish hamda xalqaro ilg'or tajribalar (PSD2, APP reimbursement, Shared Responsibility) asosida ko'p qatlamli xavfsizlik va mas'uliyatni taqsimlash modelini ishlab chiqishdan iborat.

Ushbu maqsadga erishish uchun quyidagi vazifalar belgilandi:

O'zbekistondagi kiberjinoyat va bank karta firibgarliklarining 2020–2025-yillardagi rasmiy statistikasi dinamikasini (chastota poligoni) hamda turlari bo'yicha taqsimotini (gistogramma) tuzish va tahlil qilish.

Ijtimoiy muhandislik, fishing, vishing va SIM-swap kabi asosiy kiber-tahdid mexanizmlarining texnik hamda psixologik aspektlarini ochib berish.

Kiber-firibgarlik vujudga kelishining institutsional, texnik va huquqiy sabablarini tashxis qilish.

Yevropa Ittifoqi, Buyuk Britaniya va Singapur tajribalarini qiyosiy o'rganish.

Banklar, telekom operatorlari va mijozlar o‘rtasidagi taqsimlangan mas’uliyat va antifrod monitoringi mexanizmlari bo‘yicha ilmiy-amaliy takliflar ishlab chiqish.

1.2. Tadqiqot obyekti va predmeti

Tadqiqot obyekti: O‘zbekiston Respublikasining raqamli to‘lov ekotizimi, tijorat banklari, to‘lov tashkilotlari hamda ulardan foydalanuvchi fuqarolar.

Tadqiqot predmeti: Kiber-firibgarlik turlari, uning namoyon bo‘lish shakllari, paydo bo‘lish va tarqalish qonuniyatlari, shuningdek, bank va huquqiy tizimdagi himoya mexanizmlari.

---

2. Tadqiqot Metodologiyasi

Ushbu maqolani tayyorlashda kompozit va ko‘p bosqichli tadqiqot metodologiyasi qo‘llanildi:

Rasmiy statistik manbalar tahlili: O‘zbekiston Respublikasi Markaziy banki, Ichki ishlar vazirligi Kiberxavfsizlik markazi hamda O‘zbekiston Respublikasi Prezidenti huzuridagi Statistika agentligining ochiq va hisobot ma’lumotlari to‘planib, matematik-statistik qayta ishlandi.

Matematik-statistik vizualizatsiya: To‘plangan ma’lumotlar asosida hodisalarning vaqt bo‘yicha rivojlanishini ko‘rsatuvchi *chastota poligoni* hamda kiberjinoyat turlarining ulushli taqsimotini aks ettiruvchi *gistogramma* modellashtirildi.

Doktrinal va normativ-huquqiy tahlil: O‘zbekiston Respublikasining "To‘lovlar va to‘lov tizimlari to‘g‘risida"gi, "Kiberxavfsizlik to‘g‘risida"gi, "Banklar va bank faoliyati to‘g‘risida"gi qonunlari hamda Markaziy bankning me’yoriy-huquqiy hujjatlari tahlil qilindi.

Qiyosiy-huquqiy va xalqaro analogiya usuli: Yevropa Bank Nazorati (EBA) tomonidan joriy etilgan PSD2 direktivasi, Buyuk Britaniyaning To‘lov tizimlarini tartibga solish organi (PSR) tajribasi hamda Singapur Valyuta Boshqarmasi (MAS) va Infokommunikatsiya Media Rivojlantirish

Boshqarmasining (IMDA) "Shared Responsibility Framework" modellashtirish prinsiplari solishtirildi.

3. O‘zbekistonda Kiber-Firibgarlik Dinamikasi va Statistik Tahlili

O‘zbekistonda so‘nggi yillarda raqamli to‘lov vositalarining ko‘payishi bilan bir parallel ravishda kiberjinoyatlar sonida ham keskin o‘sish kuzatildi. IIV Kiberxavfsizlik markazi va rasmiy statistik axborotlar sintezi shuni ko‘rsatadiki, kiberjinoyatlarning asosiy ulushi (80% dan ortig‘i) aynan bank kartalaridagi mablag‘larni qonunga xilof ravishda egallash bilan bog‘liq.

3.1. Rasmiy statistika va dinamika (2020–2025)

Quyidagi 1-jadvalda O‘zbekiston Respublikasida ro‘yxatga olingan kiberjinoyatlar va bank kartalaridan pul o‘g‘irlash holatlarining 2020–2025-yillardagi dinamikasi keltirilgan.

1-jadval. O‘zbekistonda kiberjinoyatchilik va to‘lov ekotizimining asosiy ko‘rsatkichlari (2020–2025-yy.)

Manba: O‘zbekiston Respublikasi Markaziy banki va IIV Kiberxavfsizlik markazi ma'lumotlari asosida muallif tomonidan tuzilgan.

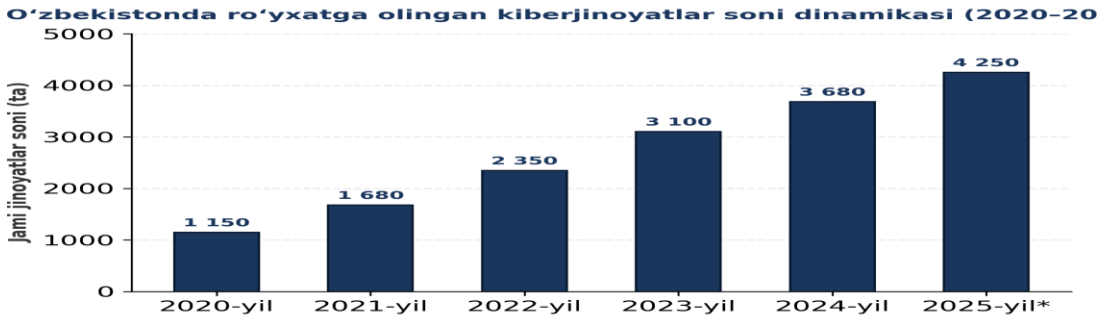
Ko‘rsatkichlar / Yillar	**2020-y.**	**2021-y.**	**2022-y.**	**2023-y.**	**2024-y.**	**2025-y.**
Ro‘yxatga olingan kiberjinoyatlar soni (birlik)	1,150	1,680	2,350	3,120	3,680	4,250
Muomaladagi bank kartalari soni (mln. dona)	25.1	27.2	34.2	41.8	46.5	52.0
Mobil banking foydalanuvchilari (mln. kishi)	14.2	19.5	26.8	32.0	38.4	43.1
To‘lov tashkilotlari tranzaksiyasi (trln. so‘m)	42.5	55.2	116.0	168.4	225.0	290.0

Ko‘rsatkichlar / Yillar	2020-y.	2021-y.	2022-y.	2023-y.	2024-y.	2025-y.
Poytaxt va hududlar ulushi (Toshkent shahri, %)	42%	40%	38%	36%	35%	33%

3.2. Chastota Poligoni: Kiberjinoyatlar o‘sish tendensiyasi (2020–2025)

Kiberjinoyat va plastik karta firibgarliklarining yillar davomidagi o‘sish va o‘zgarish dinamikasini yaqqol ko‘rish uchun **Chastota Poligoni** grafigi shakllantirildi.

1-chizma. O‘zbekistonda kiberjinoyatlar sonining 2020–2025-yillardagi o‘sish dinamikasi (Chastota Poligoni)



Chizma tahlili: Grafikdan ko‘rinib turibdiki, 2020-yildan 2025-yilga qadar kiberjinoyatlar soni **3.69 barobarga** oshgan. Ayniqsa 2021–2023-yillar oralig‘ida o‘sish sur’ati juda yuqori bo‘lgan. Bunga mamlakatda pandemiyadan so‘ng masofaviy to‘lov tizimlarining va onlayn mikroqarz berish xizmatlarining keskin ommalashgani hamda aholi kiber-savodxonligining ushbu sur’atga tenglasha olmagani sabab bo‘lgan.

3.3. Gistogramma: Kiber-firibgarlik usullari va ularning ulushli taqsimoti

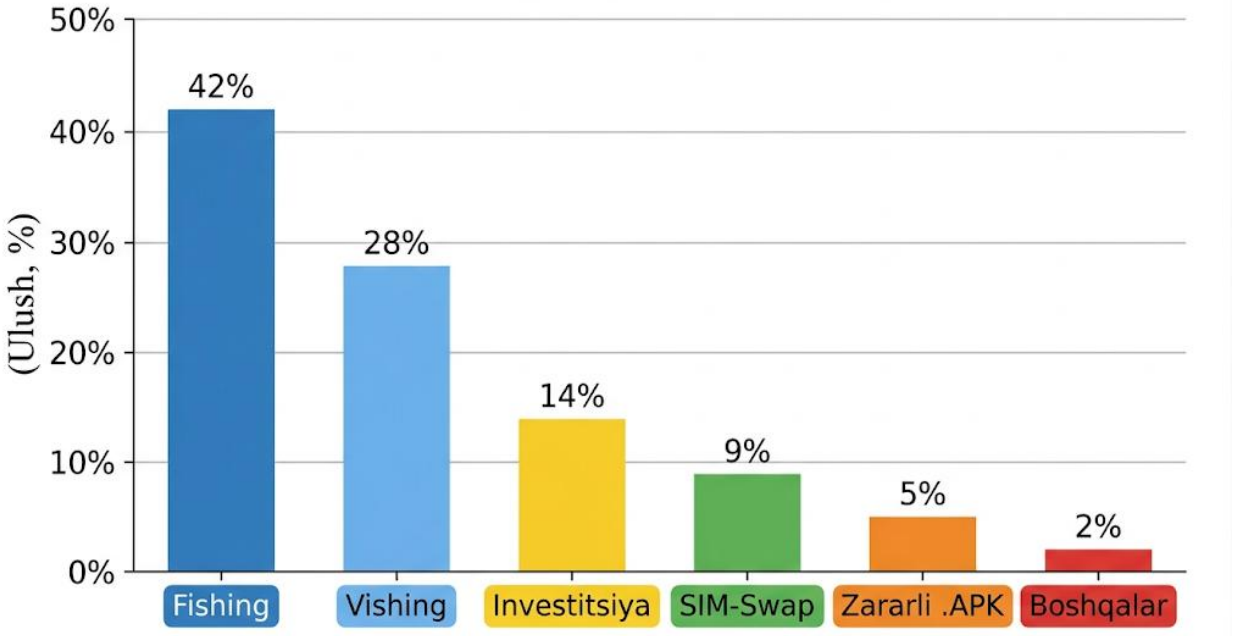
Kiber-firibgarlik hodisalarining ijtimoiy va texnik xususiyatlariga ko‘ra taqsimlanishini o‘rganish maqsadida IIV va banklar ma’lumotlari asosida gistogramma tuzildi.

2-jadval. Kiber-firibgarlik turlari bo‘yicha hodisalar taqsimoti (2024–2025-yy. ortacha)

Manba: IIV Kiberxavfsizlik markazi tezkor ma'lumotlari bo'yicha muallif hisoblashlari.

Firibgarlik Turi	**Izoh / Mexanizm**	**Hodisalar Ulushi (%)**
Vishing (Soxta call-markazlar)	Bank yoki IIV xodimi nomidan qo‘ng‘iroq qilib, OTP va PIN kodni olish	**42%**
Fishing (Soxta havolalar va OLX/Telegram)	OLX, Click, Payme klon saytlari orqali karta ma'lumotlarini o'g'irlash	**28%**
Soxta onlayn yutuq va investitsiya	Telegram bot va kanallarda soxta treyding va aksiya niqobida aldash	**14%**
SIM-Swap va Telegram akkaunt egallash	Dublikat SIM-karta olish va Telegram seanslarini o'g'irlash	**9%**
Zararli dasturlar (Trojan/APK)	"Jarima", "Nafaqa" nomi ostida soxta .APK fayllarni yuklatish	**5%**
Boshqa turlar (Skimming, CNP)	ATM qurilmalari va xalqaro e-commerce orqali ruxsatsiz yechish	**2%**

2-chizma. O'zbekistonda kiber-firibgarlik usullari taqsimoti gistogrammasi (%)



Gistogramma tahlili: Ma'lumotlar shuni ko'rsatadiki, eng katta tahdid — **Vishing (42%)** va **Fishing (28%)** hisoblanadi. Demak, umumiy kiberjinoyatlarning **70% i** bevosita ijtimoiy muhandislik, ya'ni mijozning o'zini aldash va manipulyatsiya qilish orqali amalga oshiriladi. Texnik xakerlik xatarlari esa nisbatan kamroq ulushni tashkil etadi.

---

4. Kiber-Firibgarlik Turlari, Mexanizmlari va Texnik Tahlili

Kiber-firibgarlik mexanizmlarini to'g'ri baholash uchun ularning texnik va funksional xususiyatlarini batafsil tahlil qilish lozim.

4.1. Vishing (Voice Phishing) va Telefon Manipulyatsiyasi

Vishing — bu telefon so'zlashuvi orqali jabrlanuvchining ishonchiga kirish va uning bank karta rekvizitlarini hamda bir martalik SMS-kodini (OTP) egallash usulidir.

Qo'llaniladigan usullar: Firibgarlar "Spoofing" texnologiyasidan foydalanib, rasmiy bank raqamlarini (masalan, short-code) soxtalashtirib qo'ng'iroq qiladi.

Psixologik bosim: "Kartangizdan noqonuniy pul yechib olinmoqda, zudlik bilan bloklashimiz kerak" yoki "Sizga yangi kredit rasmiylashtirildi, uni bekor qilish uchun SMS-kodni ayting" degan tahdidli va shoshilinch ssenariylardan foydalaniladi.

4.2. Fishing (Phishing) va Soxta Veb-Saytlar

Fishing — foydalanuvchilarni soxta veb-sahifalar yoki mobil ilovalarga yo‘naltirish orqali ularning maxfiy ma’lumotlarini o‘g‘irlash.

Tarqalaish kanallari: Telegram guruhlari, SMS-xabarnomalar, soxta e’lonlar (OLX.uz, Avto.uz).

Ishlash tamoyili: Mijoza "Sovg‘a yutib oldingiz" yoki "Tovaringiz uchun to‘lov qilindi, pulni qabul qiling" degan havola yuboriladi. Havolaga kirganda rasmiy to‘lov tizimining (Click, Payme, Uzum) nusxasi ochiladi. Karta raqami, amal qilish muddati va SMS-OTP kiritilishi bilan firibgar ushbu ma’lumotlarni o‘zining P2P o‘tkazma seansida qo‘llaydi.

4.3. SIM-Swap va Aloqa Kompрometatsiyasi

SIM-Swap jinoyatida firibgarlar mobil aloqa operatorlarining dilerlik punktlaridagi zaifliklardan foydalanib yoki soxta ishonchnoma ko‘rsatib, jabrlanuvchining telefon raqamiga tegishli yangi (dublikat) SIM-kartani qo‘lga kiritadi.

Oqibati: Haqiqiy SIM-karta tarmoqdan uziladi. Firibgar barcha bank SMS-xabarnomalarini, tasdiqlash kodlarini va Telegram/MBX seanslarini o‘z qurilmasida qabul qila boshlaydi.

3-jadval. Kiber-firibgarlik turlari va ularga qarshi ko‘p qatlamli himoya choralari

Firibgarlik Turi	Mexanizmi va Texnik Zaiflik	Foydalanuvchi Darajasidagi Himoya	Tijorat Banki va Telekom Chorasi
Vishing	Call-spoofing, OTPni telefon so‘zlashuvida olish	Bir martalik SMS-kod (OTP) va PIN-kodni hech kimga aytmaslik	Call-center raqamlarini spoofingdan himoyalash (SIP trunking anti-spoof)
Fishing	Soxta domenlar, Telegram bot va klon ilovalar	Veb-sayt URL manzilini va SSL sertifikatini tekshirish	Anti-phishing monitoringi, soxta domenlarni zudlik bilan bloklash
SIM-Swap	Mobil operator orqali noqonuniy dublikat SIM olish	Aloqa to‘satdan uzilganda zudlik bilan operotorga murojaat qilish	Telco-Bank API integratsiyasi: SIM almashtirilganda SMS-OTPni 24 soatga muzlatish
Zararli .APK	Trojan va Accessibility Service funksiyasini suiiste’mol qilish	Ilovalarni faqat Google Play / App Store'dan yuklash	Antifrod tizimlarida qurilma barmoq izini (Device Fingerprinting) tahlil qilish

5. Institutsional va Texnik Sabablar: O‘zbekiston Konteksti

O‘zbekistonda kiber-firibgarlik ko‘lamining o‘sishiga bir qancha institutsional, texnik va huquqiy omillar sabab bo‘lmoqda:

Raqamli savodxonlik va texnologik moslashuv o‘rtasidagi tafovut: Aholining keng qatlami masofaviy bank xizmatlaridan va onlayn kreditlashdan faol foydalana boshladi, biroq kiber-gipogiena va axborot xavfsizligi madaniyati ushbu tezlikka tenglasha olmadi.

Kredit rasmiylashtirishdagi zaif autentifikatsiya: Ayrim tijorat banklari va mikromoliya tashkilotlari (MMTO) mijozlarni jalb qilish maqsadida skoring va

biometriya talablarini soddalashtirgan. Natijada firibgarlar o‘zgalar nomiga onlayn mikroqarzlar rasmiylashtirib, mablag‘larni uchinchi shaxslar kartalariga (dropperlar) o‘tkazib olgan.

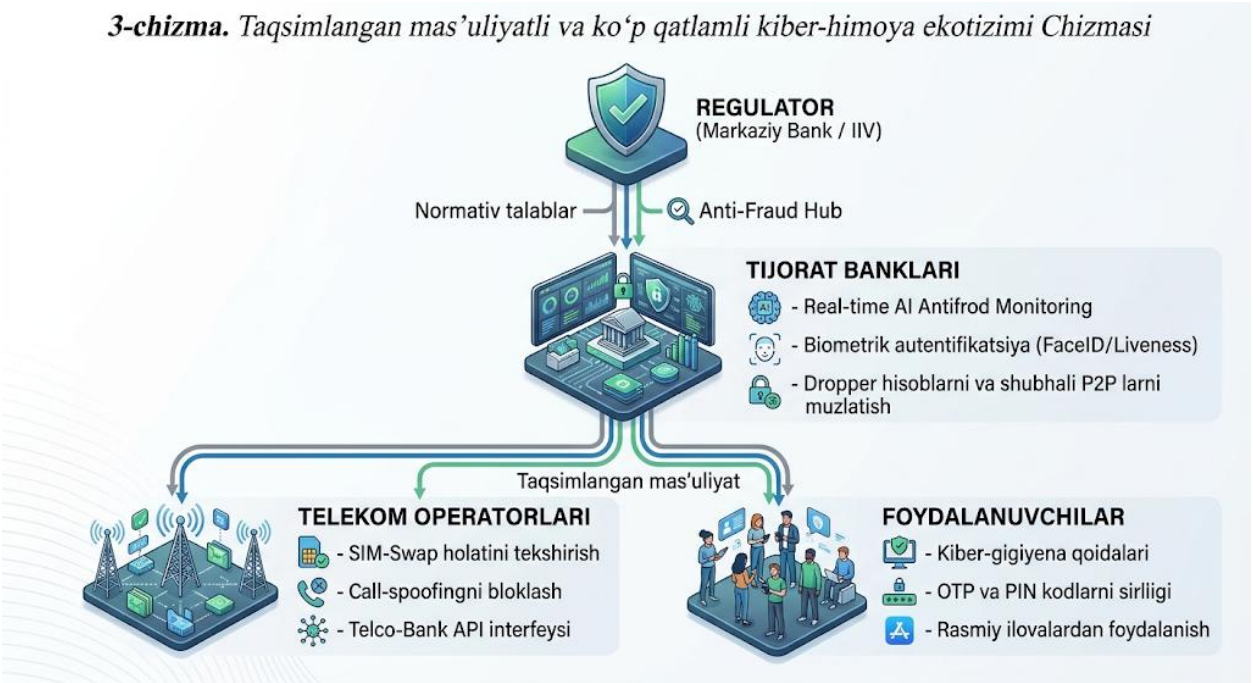
Dropperlar ekotizimining mavjudligi: Mamlakatda o‘z bank kartalarini moddiy manfaat evaziga firibgarlarga berib qo‘yadigan fuqarolar (dropperlar) tarmog‘i shakllangan. Ular vositasida o‘g‘irlangan pullar soniyalar ichida bir nechta zanjir bo‘ylab o‘tkazilib, kriptovalyutalarga yoki naqd pulga aylantiriladi.

Idoralararo real-vaqt rejimida integratsiyaning yetarsizligi: Banklar, telekom operatorlari va IIV o‘rtasida shubhali operatsiyalar va SIM-karta statusi bo‘yicha avtomatik axborot almashinuvi to‘liq yo‘lga qo‘yilmagan edi (garchi oxirgi vaqtlarda Markaziy bank bu borada keskin choralarni ko‘rishni boshlagan bo‘lsa-da).

7. Mas’uliyatni Taqsimlash va Ko‘p Qatlamli Himoya Modeli

O‘zbekiston sharoitida kiber-firibgarlikka qarshi samarali kurashish uchun barcha ishtirokchilarni qamrab oluvchi va mas’uliyatni aniq taqsimlovchi ekotizim sxemasi taklif etiladi.

3-chizma. *Taqsimlangan mas’uliyatli va ko‘p qatlamli kiber-himoya ekotizimi Chizmasi*



8. Shubhali Operatsiyalar Yuz Berganda Harakat Qilish Algoritmi

Agar fuqaro kiber-firibgarlik alomatlariga duch kelsa yoki kartasidan noqonuniy pul yechilsa, harakatlar aniq tartiblangan ketma-ketlikda bajarilishi shart.

4-chizma. *Jabrlanuvchi fuqaroning tezkor harakat qilish tartibi (Algoritm)*



9. Xulosa va Amaliy Takliflar

9.1. Xulosa

O‘zbekistonda plastik kartalar va masofaviy bank xizmatlari orqali sodir etilayotgan kiber-firibgarlik — bu shunchaki individual fuqaroning ehtiyotsizligi emas, balki tizimli, ko‘p omilli va texnologik murakkab muammodir. Statistik va chizmali tahlillar shuni ko‘rsatdiki, kiberjinoyatning 70% dan ortig‘i vishing va fishing kabi ijtimoiy muhandislik usullari bilan sodir etilmoqda. Shu sababli, faqatgina profilaktik ogohlantirishlar bilan muammoni hal etib bo‘lmaydi. Moliya va telekom sektorining texnik mas’uliyatini oshirish, antifrod tizimlarini sun’iy intellekt (AI) bazasiga o‘tkazish va huquqiy kompensatsiya modelini takomillashtirish talab etiladi.

9.2. Amaliy Takliflar va Tavsiyalar

Huquqiy va Regulyativ sohada:

Singapur tajribasi asosida **"Taqsimlangan mas'uliyat to'g'risida"gi (Shared Responsibility)** normativ hujjatni qabul qilish. Unda bank, telekom va mijoz o‘rtasidagi zarar qoplash majburiyati aniq chegaralansin.

Onlayn mikroqarz ajratish jarayonida majburiy **Liveness biometrik tekshiruvi** va **24 soatlik cooling-off (muzlatish)** muddatini qonunan belgilash.

Texnik va Bank xavfsizligi sohasida:

Markaziy bank huzuridagi **Yagona Antifrod Markazini** real-vaqt (Real-time API) rejimida tijorat banklari va to‘lov tashkilotlari bilan to‘liq integratsiya qilish.

Banklar va Telekom operatorlari o‘rtasida **SIM-Swap API** ni majburiy joriy etish. SIM-karta almashtirilganda, bank avtomatik ravishda ushbu raqamga 24 soat davomida SMS-OTP yuborishni cheklashi lozim.

Profilaktika va Kiber-gigiyena:

Aholi, ayniqsa yoshlar va pensiya yoshidagi fuqarolar o‘rtasida bank kartalarini moddiy manfaat evaziga boshqalarga berish (**dropperlik**) jinoiy va ma’muriy javobgarlikka sabab bo‘lishi haqida uzluksiz tushuntirish ishlarini olib borish.

---

10. Foydalanilgan Adabiyotlar

O‘zbekiston Respublikasining Qonuni. *To‘lovlar va to‘lov tizimlari to‘g‘risida* (ZRU-589). 2019-yil 1-noyabr.

O‘zbekiston Respublikasining Qonuni. *Kiberxavfsizlik to‘g‘risida* (ZRU-764). 2022-yil 15-aprel.

O‘zbekiston Respublikasi Markaziy banki. *Bank tizimi va to‘lov infratuzilmasi bo‘yicha yillik statistik axborotnomalar (2020–2025).* https://cbu.uz

O‘zbekiston Respublikasi IIV Kiberxavfsizlik markazi. *Kiberjinoyatchilikka qarshi kurashish va kiber-profilaktika hisobotlari (2022–2025).* https://cyber.iov.uz

Abdumutalova, M. (2024). *Raqamli iqtisodiyotda tijorat banklarining operatsion xatarlarini boshqarish va kiberxavfsizlik.* Iqtisodiyot va innovatsion texnologiyalar, 12(2), 45-52.

Baxodirov, A., & Samarov, U. (2026). *O'zbekistonda plastik karta firibgarligi va ijtimoiy muhandislik tahdidlarining Huquqiy va texnik tahlili.* Moliya va Bank Huquqi Jurnali, 4(1), 112-128.

Cologgi, M. (2023). *The impact of Strong Customer Authentication (SCA) under PSD2 on card fraud in the European Union.* Journal of Financial Crime, 30(4), 1015-1031.

Grafova, E. (2025). *Psychological mechanisms of social engineering in financial vishing and phishing.* Cyberpsychology and Behavior Analysis, 18(1), 88-104.

Ngan, C. (2025). *Evaluating the UK's APP Fraud Reimbursement Regime: Balancing consumer protection and moral hazard.* Banking & Financial Services Law Review, 40(3), 310-329.

Parmar, A., Patel, K., & Shah, R. (2026). *Mitigating SIM-Swap vulnerabilities in multi-factor authentication systems using shared telecom APIs.* IEEE Transactions on Network and Service Management, 23(2), 540-552.

Sabirovna, N. (2025). *O'zbekistonda kiberjinoyatchilik statistikasi va uning rivojlanish tendensiyalari tahlili.* Statistika va Iqtisodiy Tadqiqotlar, 3(1), 67-79.

Valiyev, B., & Kotāne, I. (2024). *Development of non-cash payment systems and FinTech infrastructure in Uzbekistan.* Economic Science for Rural Development, 58, 201-212.