



RAQAMLI MOLIYA TIZIMIDA XAVFSIZLIKNI TA'MINLASH: BANKLAR VA IIO HAMKORLIGINING STRATEGIK MODEL

*IIV Akademiyasi Raqamli texnologiyalar
va axborot xavfsizligi kafedrası boshlig'i,
Matematika va fizika fanlar nomzodi podpolkovnik
Iminov Abdurasul Abdulatipovich
IIB Akademiyasi 3-o'quv kursi 325-guruh kursanti
Botiraliyev Asliddin Xurshid o'g'li*

Annotatsiya: *Mazkur maqolada raqamli iqtisodiyot sharoitida moliya-bank tizimidagi kiberjinoyatchilikka qarshi kurashish mexanizmlari tahlil qilinadi. Tadqiqotning asosiy maqsadi banklar va huquqni muhofaza qiluvchi organlar o'rtasida axborot almashinuvi va tezkor harakat qilishning integratsiyalashgan strategik modelini ishlab chiqishdan iborat. Maqolada kiber-firdovgarlikning zamonaviy usullari va ularning oldini olishda davlat-xususiy sheriklik tamoyillarining o'rnı yoritilgan.*

Kalit so'zlar: *raqamli moliya, kiberxavfsizlik, bank tizimi, IIO, kiberjinoyat, antifrod tizimi, strategik model, blokcheyn, biometriya.*

KIRISH

2026-yilga kelib, jahon iqtisodiyoti to'liq raqamli transformatsiya bosqichiga kirdi. O'zbekiston Respublikasida ham bank-moliya xizmatlarining 90% dan ortig'i masofaviy shaklga o'tkazildi. Biroq, texnologik taraqqiyot bilan bir qatorda kiberjinoyatchilikning ham yangi, murakkab turlari shakllanmoqda. Bugungi kunda moliya tizimidagi xavfsizlik nafaqat iqtisodiy barqarorlik, balki milliy xavfsizlikning ajralmas qismi hisoblanadi.

Raqamli moliya tizimida xavfsizlikni ta'minlashda banklarning texnik imkoniyatlari va Ichki ishlar organlarining huquqiy vakolatlari o'rtasidagi "uzilish" (gap) kiberjinoyatchilarga qo'l kelmoqda. Shu sababli, ushbu ikki tuzilma o'rtasidagi hamkorlikni yangi bosqichga olib chiqish — strategik zaruriyatdir.

I BOB. RAQAMLI MOLIYA TIZIMIDAGI ZAMONAVIY TAHDIDLAR TAHLILI

Raqamli moliya tizimidagi tahdidlar doimiy ravishda evolyutsiya qilib bormoqda. Hozirgi kunda quyidagi asosiy xavflar ustuvorlik qilmoqda:

1. Ijtimoiy muhandislik (Social Engineering): 2025-2026 yillar statistikasiga ko'ra, bank kartalaridan mablag'larni o'g'irlashning 70% dan ortig'i aynan fuqarolarning ishonchiga kirish orqali amalga oshirilgan.



2. Deepfake texnologiyalari: Firibgarlar bank xodimi yoki mijozning ovozi va qiyofasini sun'iy intellekt yordamida soxtalashtirib, tranzaksiyalarni tasdiqlatishga erishmoqda.

3. Phishing va zararli dasturlar: Bank ilovalarining soxta nusxalarini tarqatish orqali shaxsiy ma'lumotlarni o'g'irlash.

4. Kriptovalyuta orqali mablag'larni legallashtirish: O'g'irlangan pullarni zanjirli tranzaksiyalar orqali kiber-hamyonlarga o'tkazish va izini yo'qotish.

II BOB. BANKLAR VA IIO HAMKORLIGIDAGI MAVJUD MUAMMOLAR

Hozirgi kunda hamkorlik asosan "so'rov-javob" mexanizmiga asoslangan. Bu esa quyidagi kamchiliklarni keltirib chiqarmoqda:

- Vaqt yo'qotilishi: Firibgarlik sodir etilganidan so'ng bankdan ma'lumot olish uchun IIO so'rovi bir necha soatdan bir necha kungacha vaqt olishi mumkin. Bu vaqt ichida pullar bir necha "qo'llardan" o'tib, naqdlashtirib ulguriladi.

- Ma'lumotlar bazasining integratsiyalashmaganligi: Banklarning "Antifrod" (firibgarlikka qarshi) tizimlari IIOning kiberjinoyatchilar haqidagi bazasi bilan real vaqt rejimida bog'lanmagan.

- Kadrlar yetishmovchiligi: Banklarda huquqiy bilimga ega kiber-mutaxassislar, IIOda esa moliya texnologiyalarini (FinTech) mukammal tushunadigan tergovchilar tanqisligi sezilmoqda.

III BOB. STRATEGIK HAMKORLIK MODEL: INTEGRATSIYALASHGAN TIZIM

Maqolada taklif etilayotgan "Bank-IIO-Mijoz" strategik modeli uchta asosiy ustunga tayanadi:

1. "Cyber-Shield" Yagona axborot platformasi

Banklar va IIO Kiberjinoyatchilikka qarshi kurashish markazi o'rtasida real vaqt rejimida (Real-time) ma'lumot almashish imkonini beruvchi platforma. Agar biror bankda shubhali tranzaksiya bloklansa, bu haqda ma'lumot avtomatik tarzda IIO tizimida aks etadi.

2. Sun'iy Intellekt asosidagi preventiv monitoring

Banklarning antifrod tizimlariga IIO tomonidan taqdim etilgan "qora ro'yxat"dagi shaxslar, shubhali qurilmalar (IMEI kodlar) va IP-manzillar integratsiya qilinadi. SI tizimi jinoyat sodir etilishidan avval uni profilaktika qilish imkonini beradi.

3. Tezkor bloklash mexanizmi (Kill Switch)

Jabrlanuvchi IIOga xabar bergan zahoti, prokuror sanksiyasini kutmasdan (keyinchalik rasmiylashtirish sharti bilan), o'g'irlangan mablag'larni keyingi barcha zanjirlar bo'ylab vaqtincha muzlatib qo'yish huquqini beruvchi huquqiy-texnik mexanizm.



IV BOB. HUQUQIY VA TEXNIK ASPEKTLAR

Strategik modelni amaliyotga tatbiq etish uchun quyidagi qadamlar qo'yilishi lozim:

- Qonunchilikni takomillashtirish: "Bank siri to'g'risida"gi qonunga kiberjinoyatlarni tergov qilish jarayonida ma'lumotlarni tezkor almashishga oid o'zgartirishlar kiritish.

- Blokcheyn texnologiyasi: Tranzaksiyalar tarixini o'zgartirib bo'lmaydigan zanjir ko'rinishida saqlash, bu sud jarayonida inkor etib bo'lmas dalil bo'lib xizmat qiladi.

- Biometrik autentifikatsiya: Barcha moliya amaliyotlarini faqat Face-ID yoki barmoq izi orqali emas, balki "tiriklik testi" (liveness detection) orqali tasdiqlashni majburiy etib belgilash.

V BOB. XALQARO TAJRIBA VA UNI O'ZBEKISTONDA QO'LLASH

Singapur va Janubiy Koreya tajribasi shuni ko'rsatadiki, banklar va politsiya o'rtasidagi "Shared Cyber Defense" (Birgalikdagi kiber-mudofaa) markazlari kiber-firibgarlikni 45% ga kamaytirishga xizmat qilgan. O'zbekistonda ham Markaziy bank huzurida "Moliya kiber-insidentlariga javob berish markazi" (CERT-Fin) faoliyatini IIO bilan yanada jipslashtirish lozim.

XULOSA

Raqamli moliya tizimida xavfsizlikni ta'minlash faqatgina texnik masala emas, balki kompleks strategik yondashuvni talab etadi. Banklar va IIO o'rtasidagi hamkorlikning taklif etilayotgan modeli quyidagi natijalarni beradi:

1. Kiberjinoyatlarni fosh etish tezkorligi 5-10 barobarga oshadi.
2. Mijozlarning raqamli bank tizimiga bo'lgan ishonchi ortadi.
3. Iqtisodiyotdagi "yashirin" pul aylanmalarining oldi olinadi.

Xulosa qilib aytganda, kiber-xavfsizlik sohasidagi davlat-xususiy sherikligi raqamli O'zbekiston barqarorligining kafolatidir.

FOYDALANILGAN ADABIYOTLAR RO'YXATI:

1. O'zbekiston Respublikasining "Kiberxavfsizlik to'g'risida"gi Qonuni, 2022.
2. Mirziyoyev Sh.M. "Yangi O'zbekiston strategiyasi". - T.: "O'zbekiston", 2021.
3. Gulyamov S.S. "Raqamli iqtisodiyotda huquqiy masalalar". - T., 2023.
4. International Monetary Fund (IMF). "Cyber Resilience in the Financial Sector", 2024.
5. World Bank Report. "Digital Financial Services and Security Challenges", 2025.
6. Markaziy Bank rasmiy sayti - Statistika ma'lumotlari.