TIJORAT BANKLARIDA AXBOROT TEXNOLOGIYALARI RISKLARINI BAHOLASH

Yashin Boltayev

E-mail: yashinboltaev@gmail.com

Tel: +99897 305 03 07

ORCID: 0009-0005-5345-2734

Kirish

So‘nggi yillarda O‘zbekiston bank tizimi raqamli xizmatlar hisobiga sezilarli darajada o‘zgardi: mobil ilova va internet-banking orqali xizmat ko‘rsatish endi qo‘shimcha imkoniyat emas, balki asosiy kanalga aylandi. Bu jarayon banklarga ko‘plab afzalliklar bergani rost, ammo shu bilan birga yangi turdagi zaifliklarni ham yuzaga chiqardi. Axborot texnologiyalari (AT) risklarini qanday aniqlash va ularni qanday ustuvorlashtirish masalasi shu sababli endi nazariy emas, amaliy ahamiyatga ega mavzuga aylandi.

Tahlil

Bank xizmatlarining katta qismi bugungi kunda mobil ilova, internet-banking va boshqa masofaviy kanallar orqali ko‘rsatilmoqda. Bu holat bankka aniq foyda keltiradi jumladan xizmat tezlashadi, xarajat kamayadi, mijoz qamrovi kengayadi. Ammo shu bilan bir qatorda oldin unchalik sezilmagan bir muammo endi kattaroq ko‘lamda namoyon bo‘lyapti: axborot texnologiyalari tizimidagi har qanday nosozlik yoki hujum endi bir emas, minglab, hattoki millionlab mijozga bir vaqtning o‘zida ta'sir qilishi mumkin. Shu boisdan AT risklarini to‘g'ri baholash tijorat banklari uchun endi ixtiyoriy emas, majburiy vazifaga aylandi.

Vaziyatning naqadar jiddiy ekanini raqamlar orqali ko‘rish mumkin. Ichki _____ vazirligi Kiberjinoyatlar markazi ma'lumotiga ko‘ra, 2019-yildan 2024-yilgacha O‘zbekistonda qayd etilgan kiberjinoyatlar soni 68 baravardan ortiq oshgan, shundan 98 foizi aynan bank kartalari orqali sodir etilgan**[1]**. Bunday statistika shuni ko‘rsatadiki, kiberxavflar endi umumiy, mavhum tushuncha emas

ular bevosita bank sektoriga, aniqrog'i har bir bankning kundalik operatsion faoliyatiga tegishli masala.

O‘zbekiston Respublikasi Markaziy banki tomonidan bu boradagi javob ham keskinlashib bormoqda: 2025-yilda kuchga kirgan, tijorat banklarining axborot xavfsizligi va kiberxavfsizligiga doir minimal talablarini belgilovchi nizom**[2]** endi har bir bankdan alohida kiberxavfsizlik xizmatini tashkil etishni talab qiladi. Bu to‘g'ri qadam, ammo yetarli emas. Chunki nizom asosan "nima qilinishi kerak" degan minimal ro‘yxatni beradi, "qanday baholash kerak" degan savolga esa har bir bank o‘zi javob topishi kerak bo‘ladi.

Aynan shu o‘rinda risklarni baholashning amaliy uslubiyoti kerak bo‘ladi. Xalqaro amaliyotda buning uchun ehtimollik-ta'sir (probability-impact) yondashuvi keng qo‘llaniladi: har bir AT risk turi ikki mezon bo‘yicha yuzaga kelish ehtimoli va bankka ta'sir kuchi baholanadi, so‘ngra ikkalasi birgalikda risk darajasini beradi. Bu usul murakkab emas, aksincha, uni har qanday bank, hatto katta IT bo‘limi bo‘lmagan kichik bankda ham qo‘llash mumkin. Ammo nazariy sxema qanchalik sodda bo‘lsa ham, uni real raqamlar bilan to‘ldirmasdan turib amaliy qiymati bo‘lmaydi.

Quyida shu fikrni tasdiqlaydigan aniq misol keltirilgan: kiberjinoyatchilarning bank kartalariga nisbatan qo‘llagan usullari taqsimoti. Bu ma'lumot risklarni baholashda "qaysi yo‘nalishga birinchi navbatda kuch tashlash kerak" degan savolga aniq javob beradi.

Bank kartalari orqali sodir etilgan kiberjinoyatlarning usullari bo‘yicha taqsimoti (2024-yil)

Usul	**Ulushi**
Zararli havola/dastur orqali karta yoki qurilma nazoratini qo‘lga kiritish	60%
Turli aldov usullari bilan SMS-tasdiqlash kodini qo‘lga kiritish	16%
Turli firibgarlik sxemalari orqali mablag'larni jalb qilish	9%

Boshqa usullar	15%
Jami	100%

Manba: Ichki ishlar vazirligi Kiberjinoyatlar markazi ma'lumotlari asosida muallif tomonidan guruhlangan [1].

Ko‘rinib turibdiki, xavflarning katta qismi deyarli to‘rtdan uch ulushi mijoz qurilmasi yoki hisob raqamiga bevosita ta'sir ko‘rsatishga qaratilgan. Demak, agar bank o‘z risk-reyestrida cheklangan resursni qayerga yo‘naltirishni tanlashi kerak bo‘lsa, javob aniq: avvalambor antifrod tizimi va mijozlarni autentifikatsiya qilish mexanizmlari kuchaytirilishi kerak, faqat shundan keyin boshqa, nisbatan kamroq ehtimollikdagi risklarga navbat yetadi.

Baholash natijalarini tartibli tarzda tahlil qilish uchun ISO/IEC 27001:2022 standartida[3] tavsiya etilgan uslubiyot foydali bo‘ladi: u xavflarni aniqlash, ularni baholash va kamaytirish choralarini rejalashtirishni bir tizimga birlashtiradi. O‘zbekiston banklari uchun bu standartni to‘liq nusxa ko‘chirishning hech qanday zarurati yo‘q, aksincha, uning mantiqiy sxemasini olib, milliy sharoitga moslashtirish kifoya qiladi.

Xulosa

Tijorat banklarida AT risklarini baholash endi bir marta o‘tkaziladigan tekshiruv emas, muntazam va tizimli jarayon bo‘lishi kerak. Har bir bank o‘z ichki risk-reyestrini yuritishi, uni kamida yiliga bir marta yangilab borishi va real statistikaga tayangan holda eng yuqori darajadagi risklarga — avvalambor antifrod va autentifikatsiya sohasiga — ustuvor e'tibor qaratishi maqsadga muvofiq.

Foydalanilgan adabiyotlar

1. Ichki ishlar vazirligi Kiberjinoyatlar markazi ma'lumotlari. 2024-yilda O‘zbekistonda kiberjinoyatchilar fuqarolardan 603 milliard so‘mni talon-taroj qilgan, uch yilda bu 1,9 trln so‘mga yetgan // Spot.uz. — 2025. — 29-may [Elektron resurs]. — URL: https://www.spot.uz/oz/2025/05/29/cybercrime

2. O‘zbekiston Respublikasi Markaziy banki boshqaruvining 2025-yil 18-avgustdagi qarori. Tijorat banklarining axborot xavfsizligi va kiberxavfsizligiga doir minimal talablar to‘g'risidagi nizomni tasdiqlash haqida (ro‘yxat raqami 3669) [Elektron resurs]. — URL: https://lex.uz/docs/-7689673
3. International Organization for Standardization. ISO/IEC 27001:2022 — Information security, cybersecurity and privacy protection — Information security management systems — Requirements. — Geneva: ISO, 2022 [Elektron resurs]. — URL: https://www.iso.org/standard/27001