KIBERXAVFSIZLIK MENEJMENTI MIJOZLAR ISHONCHINI BOSHQARISH VOSITASI SIFATIDA

Raimov Mirzohid Shuxrat o'g'li *- Qarshi davlat universiteti mustaqil izlanuvchisi,*
Markaziy bank Qashqadaryo viloyat bosh boshqarmasi
Kredit tashkilotlarining muammoli aktivlari bilan ishlash va moliyaviy tahlil qilish bo'limi boshlig'i
e-mail: Raimovmirzohid838@gmail.com
ORCID ID: 0009-0001-2053-5286

Annotatsiya. Tezisda kiberxavfsizlik texnik funksiya sifatida emas, balki mijozlar ishonchini boshqarish vositasi sifatida ko'rib chiqilgan. O'zbekistonda kiberjinoyatchilik ko'lami va uning bank xizmatlaridan foydalanishga ta'siri baholanib, 2026-yil 22-apreldan kuchga kirgan yangi me'yoriy talablar tizimlashtirilgan. Bankda kiberxavfsizlikni boshqarishning to'rt darajali modeli hamda ishonchni o'lchash ko'rsatkichlari taklif etilgan.

Kalit so'zlar: *kiberxavfsizlik, mijozlar ishonchi, bank menejmenti, masofaviy xizmatlar, firibgarlik, biometrik identifikatsiya, axborot xavfsizligi, moliyaviy inklyuziya.*

Kirish

Bank faoliyatining asosi ishonchdir. Mijoz o'z mablag'ini bankka topshirar ekan, u aslida moddiy mahsulot emas, balki va'dani sotib oladi. Bu va'da pulning saqlanishini, o'z vaqtida qaytarilishini va uchinchi shaxsga o'tib ketmasligini anglatadi. Raqamli kanallarga o'tish bilan bu ishonchning tabiati o'zgardi. Endi u nafaqat bankning to'lov qobiliyatiga, balki uning axborot tizimlarining himoyalanganligiga ham bog'liq bo'lib qoldi.

O'zbekistonda bu masala keskin tus olmoqda. So'nggi besh yil ichida kiberjinoyatchilik holatlari 68 barobar ko'paygan; faqat so'nggi 10 oyda 46 mingdan ortiq holat qayd etilib, ulardan ko'rilgan moddiy zarar 1,2 trln so'mdan

oshgan. Muallif hisob-kitobiga ko‘ra, bu bir holatga o‘rtacha 26,1 mln so‘m zarar va oyiga o‘rtacha 4 600 ta holat demakdir. Yillik ekvivalentda zarar taxminan 1,44 trln so‘mni tashkil etib, bu bank tizimining 2025-yildagi sof foydasining 10,7 foiziga teng miqdordir.

Muammoning boshqaruv jihati esa zararning o‘zidan ham jiddiyroq. Iqtisodiy tadqiqotlar va islohotlar markazining 2025-yilda o‘tkazgan so‘rovi natijalariga ko‘ra, respondentlarning 94 foizida faol bank kartasi mavjud, biroq ularning 35 foizi naqd pulni afzal ko‘rish sababi sifatida masofaviy xizmatlarga ishonmasligini ko‘rsatgan, 27 foizi esa faqat naqd puldan foydalanadi. Ya’ni texnologiya mavjud, mijoz esa undan foydalanishdan tiyilmoqda. Bu bevosita yo‘qotilgan daromad va moliyaviy inklyuziyaning cheklanishi demakdir.

Xalqaro amaliyot ham xuddi shu yo‘nalishga ishora qiladi. Ma’lumotlar buzilishidan ko‘riladigan zararning taxminan uchdan bir qismi (moliya sektorida 34 foizi) to‘g‘ridan-to‘g‘ri texnik xarajatlar emas, balki yo‘qotilgan biznes, ya’ni ketgan mijozlar va pasaygan obro‘ hissasiga to‘g‘ri keladi. Bu kiberxavfsizlikni IT-bo‘limining ichki masalasi emas, umumbank boshqaruv masalasi sifatida qarashni taqozo etadi.

Davlat darajasida bu muammoga javob allaqachon shakllantirilgan. O‘zbekiston Respublikasi Prezidentining 2026-yil 10-martdagi PF-38-son Farmoni bilan 2026–2030-yillarga mo‘ljallangan Kiberxavfsizlik strategiyasi tasdiqlandi, unda banklar, to‘lov tizimlari operatorlari hamda to‘lov va kredit tashkilotlariga qo‘yiladigan kibertahdidlarga qarshi turish talablarini belgilash, onlayn bankingda xavfsizlikni oshirish va mijozlarni firibgarlikdan himoya qilish alohida vazifalar sifatida ko‘rsatilgan. Bundan oldin, 2023-yil 31-maydagi PQ-167-son Qaror bilan muhim axborot infratuzilmasi obyektlari, jumladan bank-moliya tizimi, uchun davlat reyestri yuritish, mutaxassislarni sertifikatlashtirish va muntazam monitoring o‘tkazish tartibi joriy etilgan edi. Bu me’yoriy asos kiberxavfsizlikni bank boshqaruv tizimiga integratsiya qilish zaruratini tasdiqlaydi, biroq buning aniq amaliy mexanizmi hali ishlab chiqilmagan.

Tezisning maqsadi kiberxavfsizlik menejmentini mijozlar ishonchini

boshqarish vositasi sifatida asoslash va uni bank boshqaruv tizimiga integratsiya qilish bo‘yicha takliflar ishlab chiqishdan iborat.

Asosiy qism

Kiberxavfsizlik va mijozlar ishonchi o‘rtasidagi bog‘liqlik bir tomonlama emas. Uni ikkita alohida kanal orqali tushunish mumkin.

Birinchi kanal – bevosita ta’sir. Firibgarlik holati sodir bo‘lganda mijoz nafaqat mablag‘ini yo‘qotadi, balki bankka bo‘lgan munosabatini ham o‘zgartiradi. Muhimi shundaki, bu ta’sir bitta mijoz bilan cheklanmaydi: zamonaviy sharoitda bunday holat ijtimoiy tarmoqlar orqali tez tarqaladi va bankning butun mijozlar bazasiga ta’sir qiladi. Shu bois firibgarlik holatiga javob berish tezligi bank uchun texnik emas, obro‘ masalasidir.

Ikkinchi kanal – bilvosita ta’sir. Mijoz shaxsan zarar ko‘rmagan bo‘lsa ham, umumiy axborot muhiti uning xulq-atvorini o‘zgartiradi. Yuqorida keltirilgan 35 foizlik ko‘rsatkich aynan shu bilvosita ta’sirning natijasidir: bu odamlarning aksariyati shaxsan firibgarlikka duch kelmagan, biroq ular masofaviy xizmatni xavfli deb hisoblaydi. Bu ta’sirni faqat texnik chora bilan bartaraf etib bo‘lmaydi, bu yerda kommunikatsiya va moliyaviy savodxonlik ishga tushadi.

Shu tariqa kiberxavfsizlik menejmenti ikkita vazifani bir vaqtda hal qilishi kerak: hodisalarning sodir bo‘lish ehtimolini kamaytirish va mijozda himoyalanganlik hissini shakllantirish. Bu vazifalar bir-biriga bog‘liq, ammo bir xil emas: bank texnik jihatdan mukammal himoyalangan bo‘lib, ayni paytda mijoz nazarida xavfli ko‘rinishi mumkin va aksincha.

Vaziyatning miqdoriy ko‘rsatkichlari 1-jadvalda umumlashtirilgan.

1-jadval

Kiberxavfsizlik va mijozlar ishonchi bilan bog‘liq ko‘rsatkichlar[1]

Ko‘rsatkich	Qiymat	Davr
Kiberjinoyatchilik holatlarining o‘sishi	68 barobar	so‘nggi 5 yil

[1]“O‘zbekistonda bank ilovalari uchun yangi qoidalar joriy etilmoqda. 22-apreldan nimalar o‘zgaradi?” (Gazeta.uz, 2026-yil 8-aprel); “O‘zbekistonliklar qaysi bank xizmatlaridan mamnun va qaysilaridan norozi? Tahlil” (Spot.uz,

Ko‘rsatkich	Qiymat	Davr
Qayd etilgan holatlar soni	46 000 dan ortiq	so‘nggi 10 oy
Ko‘rilgan moddiy zarar	1,2 trln so‘mdan ortiq	so‘nggi 10 oy
Bir holatga to‘g‘ri keluvchi o‘rtacha zarar	*26,1 mln so‘m*	*hisob-kitob*
Oyiga o‘rtacha holatlar soni	*4 600 ta*	*hisob-kitob*
Zararning yillik ekvivalenti	*1,44 trln so‘m*	*hisob-kitob*
Zararning bank sektori sof foydasiga nisbati	*10,7 %*	*hisob-kitob*
Faol bank kartasiga ega respondentlar	94 %	2025-y. so‘rovi
Masofaviy xizmatlarga ishonmasligi sababli naqd pulni afzal ko‘ruvchilar	35 %	2025-y. so‘rovi
Faqat naqd puldan foydalanuvchilar	27 %	2025-y. so‘rovi

Vaziyatga javoban Markaziy bank tomonidan masofaviy moliyaviy xizmatlar uchun axborot va kiberxavfsizlik talablari belgilandi. Ular 2026-yil 22-apreldan kuchga kirdi va bank ilovalari arxitekturasiga bevosita ta’sir qiladi (2-jadval).

2-jadval

2026-yil 22-apreldan joriy etilgan asosiy talablar[2]

Yo‘nalish	Talab mazmuni
Biometrik identifikatsiya	Qurilmaga kirish, karta biriktirish va parolni o‘zgartirish kabi muhim amallarda biometrik tasdiqlash majburiy;

2025-yil 21-iyun); “Birinchi yarim yillikda banklar qariyb 11 trln so‘m sof foyda oldi” (Bankers.uz, 2026-yil 22-iyul) ma’lumotlari asosida muallif tomonidan tuzilgan va hisoblangan.

[2]“O‘zbekistonda bank ilovalari uchun yangi qoidalar joriy etilmoqda. 22-apreldan nimalar o‘zgaradi?» (Gazeta.uz, 2026-yil 8-aprel) ma’lumotlari asosida muallif tomonidan tuzilgan.

Yo‘nalish	Talab mazmuni
	faqat SMS-kod yetarli emas
Telefon raqamini tekshirish	Ilova telefon raqamining karta egasi yoki uning yaqin qarindoshiga tegishliligini JShShIR bo‘yicha tekshirishi shart
Seanslarni boshqarish	Ilovada ulangan qurilmalar, IP-manzillar va kirish vaqti ko‘rsatilishi hamda faol seansni to‘xtatish imkoniyati bo‘lishi kerak
Qo‘ng‘iroq va masofaviy kirishdan himoya	Telefon yoki video qo‘ng‘iroq davomida ilova funksiyalari bloklanadi; masofadan boshqarish dasturlari aniqlanganda kirish cheklanadi
Bir martalik parol talablari	Kod kamida 6 belgidan iborat, harf va raqamlardan tashkil topgan, amal qilish muddati 59 soniya; uch marta xato kiritilganda 15 daqiqaga bloklanadi
P2P o‘tkazmalar	Kartadan kartaga o‘tkazma faqat mobil ilova orqali amalga oshiriladi; oluvchi ma’lumotlari qisman yashiriladi
Onlayn kreditlash	Kredit byurosida bir JShShIR bo‘yicha bir vaqtda faqat bitta so‘rov ko‘rib chiqiladi; mablag‘ berishdan oldin biometrik tasdiqlash takrorlanadi

Yangi talablarning boshqaruv nuqtai nazaridan muhim jihati shundaki, ular xavfsizlik va qulaylik o‘rtasidagi muvozanatni ongli ravishda xavfsizlik tomoniga siljitadi. Qo‘shimcha biometrik tasdiqlash, qisqartirilgan parol muddati va qo‘ng‘iroq paytida ilovaning bloklanishi mijoz uchun qo‘shimcha qadamlar demakdir. Shu bois bank oldida yangi vazifa paydo bo‘ladi: ushbu cheklovlarni mijozga to‘siq sifatida emas, uning manfaatidagi himoya sifatida tushuntirish. Aks holda talablarning bajarilishi ishonchni oshirish o‘rniga foydalanuvchi tajribasini

yomonlashtirishi mumkin.

Bankda kiberxavfsizlikni boshqarish to‘rtta darajani qamrab olishi lozim. Ularning har biri o‘z mas’uliyat doirasiga va o‘lchanadigan natijasiga ega (3-jadval).

3-jadval

Bankda kiberxavfsizlikni boshqarishning to‘rt darajali modeli[3]

Daraja	Mazmuni	Mas’ul	O‘lchanadigan natija
Strategik	Kiberxavfsizlik siyosatini tasdiqlash, risk ishtahasini belgilash, byudjet ajratish	Kuzatuv kengashi va uning risk qo‘mitasi	Kengashga taqdim etilgan kiberxavfsizlik hisobotlari soni va davriyligi
Texnik	Himoya vositalarini joriy etish, zaifliklarni aniqlash, tizimlarni yangilash	Axborot xavfsizligi bo‘limi	Aniqlangan zaifliklarni bartaraf etish muddati; muvaffaqiyatli hujumlar soni
Operatsion	Hodisalarga javob berish, mijoz murojaatini ko‘rib chiqish, mablag‘ni qaytarish tartibi	Mijozlarga xizmat ko‘rsatish va monitoring xizmati	Hodisaga javob berish o‘rtacha vaqti; hal qilingan murojaatlar ulushi
Kommunikatsion	Mijozlarni ogohlantirish,	Marketing va jamoatchilik bilan	Ogohlantirish kampaniyalari

[3]Muallif ishlanmasi.

Daraja	Mazmuni	Mas'ul	O‘lchanadigan natija
	moliyaviy savodxonlikni oshirish, inqiroz kommunikatsiyasi	aloqalar xizmati	qamrovi; masofaviy xizmatlarga ishonch darajasi

Amaliyotda ko‘pincha ikkinchi daraja — texnik daraja yaxshi yo‘lga qo‘yilgan bo‘ladi, birinchi va to‘rtinchi darajalar esa zaif qoladi. Kuzatuv kengashi kiberxavfsizlik masalasini faqat hodisa yuz berganda ko‘rib chiqadi, mijozlar bilan kommunikatsiya esa umumiy ogohlantirish xabarlari bilan cheklanadi. Aynan shu ikki bo‘shliq mijozda «bank himoyalanmagan» degan tasavvur shakllanishiga olib keladi, garchi texnik jihatdan vaziyat qoniqarli bo‘lsa ham.

Modelning to‘rtinchi darajasi alohida izoh talab qiladi. Mijozlar ishonchi o‘lchanadigan kattalik bo‘lib, uni bank muntazam so‘rovlar orqali kuzatib borishi mumkin. Masofaviy xizmatlardan foydalanishdan tiyilayotgan mijozlar ulushi, ilovadan foydalanishni to‘xtatganlar soni va firibgarlik bo‘yicha murojaatlarning dinamikasi — bularning barchasi ishonch darajasining bilvosita ko‘rsatkichlari hisoblanadi va boshqaruv hisobotiga kiritilishi lozim.

Xulosa va takliflar

Keltirilgan materiallar asosida quyidagi xulosalarga kelish mumkin.

1. Raqamli kanallarga o‘tish bilan bank ishonchining tabiati o‘zgardi: u endi nafaqat bankning to‘lov qobiliyatiga, balki uning axborot tizimlari himoyalanganligiga ham bog‘liq.

2. O‘zbekistonda kiberjinoyatchilik ko‘lami tez o‘smoqda: so‘nggi besh yilda holatlar soni 68 barobar ortgan, so‘nggi 10 oyda 46 mingdan ortiq holat qayd etilib, zarar 1,2 trln so‘mdan oshgan; bu bank tizimi yillik sof foydasining o‘ndan bir qismiga teng miqdor.

3. Kiberxavfsizlikning bank uchun asosiy iqtisodiy oqibati to‘g‘ridan-to‘g‘ri yo‘qotish emas, balki mijozning raqamli kanaldan voz kechishidir:

respondentlarning 94 foizida karta bo‘lgani holda, 35 foizi masofaviy xizmatlarga ishonmasligini bildirgan.

4. 2026-yil 22-apreldan joriy etilgan talablar xavfsizlik va qulaylik muvozanatini xavfsizlik tomoniga siljitdi, bu esa bankdan ushbu cheklovlarni mijozga to‘g‘ri tushuntirishni talab qiladi.

5. Kiberxavfsizlikni boshqarish to‘rtta darajani — strategik, texnik, operatsion va kommunikatsion — qamrab olishi lozim; amaliyotda ko‘pincha faqat texnik daraja yetarli darajada ishlab chiqilgan.

Shu asosda quyidagi takliflar ilgari suriladi:

1. Kiberxavfsizlik hisobotini kuzatuv kengashiga taqdim etishning majburiy davriyligini belgilash va uni kengash risk qo‘mitasining doimiy kun tartibiga kiritish.

2. Mijozlar ishonchi darajasini muntazam so‘rovlar orqali o‘lchash va uni bank boshqaruvining hisobot ko‘rsatkichlariga kiritish.

3. Firibgarlik holatiga javob berish vaqtini alohida ko‘rsatkich sifatida belgilash va uni mijozlarga xizmat ko‘rsatish sifatini baholash tizimiga bog‘lash.

4. Yangi xavfsizlik talablarini joriy etishda mijozlar uchun tushuntirish kampaniyasini o‘tkazish, cheklovlarni to‘siq emas, himoya sifatida taqdim etish.

5. Moliyaviy savodxonlikni oshirish dasturlarini bankning marketing faoliyati bilan birlashtirish va ularning qamrovini o‘lchanadigan ko‘rsatkich sifatida belgilash.

Foydalanilgan adabiyotlar

1. O‘zbekistonda bank ilovalari uchun yangi qoidalar joriy etilmoqda. 22-apreldan nimalar o‘zgaradi? // Gazeta.uz. – 2026-yil 8-aprel.
2. O‘zbekistonliklar qaysi bank xizmatlaridan mamnun va qaysilaridan norozi? Tahlil // Spot.uz. – 2025-yil 21-iyun.
3. Cost of a Data Breach Report 2025. – Armonk: IBM Security, 2025.
4. Financial Services Data Breach Cost 2025 // DataBreachCost.com. – databreachcost.com/industry/financial-services

5. Supervisory priorities 2026–2028 // European Central Bank Banking Supervision. – 2025. – bankingsupervision.europa.eu
6. Birinchi yarim yillikda banklar qariyb 11 trln so‘m sof foyda oldi // Bankers.uz. – 2026-yil 22-iyul. – bankers.uz/news/3355
7. Banklar faollik indeksi: 2026-yil I chorak yakunlari bo‘yicha reyting yangilandi // Iqtisodiy tadqiqotlar va islohotlar markazi. – 2026. – review.uz