



RAQAMLI IQTISODIYOTDA MOLİYAVIY XAVFSIZLIKKA YANGI TAHDIDLAR.

Ilmiy rahbar: Yuldasheva Umida Asanaliyevna

TDIU, “Xalqaro moliya” kafedrası DSc., professor

E-mail: umida_yu@mail.ru

Boboqulova Durdona Abdusami qizi

TDIU, Moliya fakulteti talabasi

E-mail: abdosamiyevnadurdona04@gmail.com

Annotatsiya: Maqolada raqamli iqtisodiyot sharoitida moliyaviy xavfsizlikka ta'sir etayotgan yangi tahdidlar, jumladan, raqamli firibgarlik, kiberhujumlar, ma'lumotlar sizib chiqishi, sun'iy intellektdan foydalanilgan hujumlar hamda uchinchi tomon texnologik provayderlariga bog'liqlik tahlil qilinadi. Xalqaro tadqiqotlar va O'zbekiston Respublikasi Markaziy bankining rasmiy ma'lumotlari asosida xavflarning iqtisodiy oqibatlari umumlashtirilib, moliyaviy tashkilotlar kiberbarqarorligini kuchaytirish bo'yicha amaliy takliflar ishlab chiqiladi.

Kalit so'zlar: raqamli iqtisodiyot, moliyaviy xavfsizlik, kiberxavfsizlik, raqamli firibgarlik, antifrod, sun'iy intellekt, fintech, ma'lumotlar xavfsizligi, kiberbarqarorlik.

Kirish

Raqamli transformatsiya bank xizmatlari, mobil to'lovlar, masofaviy identifikatsiya va fintech platformalarining ommalashuvini tezlashtirdi. Ushbu jarayon tranzaksiyalar tezligi va xizmatlar qulayligini oshirayotgan bo'lsa-da, moliyaviy qiymatning raqamli kanallar orqali yaratilishi hamda uzatilishi yangi xavflarni yuzaga keltirmoqda. Moliyaviy xavfsizlik endilikda kapital va likvidlik bilan bir qatorda mijoz identifikatori, to'lov ma'lumotlari, algoritmlar, API interfeyslari, bulutli infratuzilma va tashqi xizmatlarning uzluksizligini ham qamrab oladi.



O'zbekistonda ham masofaviy bank xizmatlari foydalanuvchilari soni millionlab mijozlarni qamrab olmoqda. Markaziy bank ma'lumotlarida 2025-yil 1-oktabr holatiga Xalq bankida 8,19 mln, O'zsanoatqurilishbankda 6,01 mln va Ipoteka-bankda 4,74 mln masofaviy xizmat foydalanuvchisi qayd etilgan [3]. Shu sababli raqamli moliyaviy xavfsizlikni mustahkamlash banklar, to'lov tashkilotlari va davlat nazorati uchun strategik vazifadir.

Mavzuga oid adabiyotlar sharhi

Raqamli moliyaviy xavfsizlik bo'yicha ilmiy qarashlar axborot tizimlarini texnik himoyalash masalasidan moliyaviy barqarorlik, operatsion uzluksizlik va tizimli riskni birgalikda boshqarish yondashuviga tomon rivojlanmoqda. Xorijiy adabiyotlarda banklar va moliyaviy infratuzilmalarning o'zaro bog'liqligi sababli bitta kiberhodisa ko'plab tashkilotlar faoliyatiga ta'sir ko'rsatishi mumkinligi ta'kidlanadi.

Ross Anderson "Security Engineering" asarida xavfsizlikni faqat texnik vositalar bilan cheklemasdan, tizim loyihasi, inson xulqi, tashkiliy jarayonlar va foydalanish qulayligi bilan bog'liq muammo sifatida talqin qiladi. Uning yondashuvi banklarda himoya choralari ishlab chiqishda texnologik nazorat bilan birga foydalanuvchi xatolari va firibgarlarning xatti-harakatlarini ham hisobga olish lozimligini ko'rsatadi [4].

Iñaki Aldasoro, Leonardo Gambacorta, Paolo Giudici va Thomas Leach moliya sektoridagi operatsion hamda kiberxavflarni o'rgangan tadqiqotida banklardagi operatsion yo'qotishlar hodisa turi va hududlar bo'yicha sezilarli farqlanishini ko'rsatadi. Mualliflarning xulosalari riskni yagona ko'rsatkich bilan emas, hodisalar turi, zarar miqdori va aniqlanish muddatini hisobga olgan holda baholash zarurligini asoslaydi [5].

Md Hamid Uddin, Sabur Mollah va Md Hakim Ali 43 mamlakat banklari ma'lumotlari asosida CyberTech xarajatlari bilan bank barqarorligi o'rtasidagi munosabatni tahlil qilgan. Ularning fikricha, texnologiyaga investitsiya kiritish kiberxavflarga qarshi kurashishda zarur, biroq xarajatlarning haddan tashqari ortishi



bank barqarorligiga salbiy ta'sir qilishi mumkin. Demak, raqamli xavfsizlik xarajatlari samaradorlik va riskni hisobga olgan holda rejalashtirilishi kerak [6].

Financial Stability Board tomonidan ishlab chiqilgan FIRE (Format for Incident Reporting Exchange) tashabbusi kiber va operatsion hodisalar to'g'risidagi axborotni standartlashtirilgan shaklda almashishga qaratilgan. Bu yondashuv kiberhodisalarni faqat alohida bank muammosi sifatida emas, moliyaviy tizim barqarorligiga ta'sir qiluvchi omil sifatida kuzatish imkonini beradi [7].

Ushbu tadqiqotlar uchta muhim ilmiy xulosani beradi: birinchidan, kiberxavfsizlik texnik himoyadan kengroq institutsional masaladir; ikkinchidan, raqamli infratuzilmaning o'zaro bog'liqligi xavflarning tizimli tus olishiga olib keladi; uchinchidan, xavfsizlikka sarflanadigan mablag'lar riskka mutanosib va natijadorlik mezonlari asosida boshqarilishi lozim.

O'zbekiston olimlarining raqamli bank xizmatlari va kiberxavfsizlikka oid ishlari ham mavzuning milliy sharoitdagi dolzarbligini ko'rsatadi. Zokir Mamadiyarov va Doniyor Karshievning "Cybersecurity in Digital Banking: Safeguarding Customer Trust in Uzbekistan" maqolasida raqamli bank xizmatlarining kengayishi mijozlar ishonchini himoyalash masalasini birinchi o'ringa olib chiqishi qayd etiladi. Mualliflar ma'lumotlar buzilishi, firibgarlik va shaxsni o'g'irlash kabi tahdidlarni raqamli bank xizmatlari uchun muhim xavf sifatida ko'rib chiqadi [8].

Anvar Mengniyozovning 2026-yilda e'lon qilingan "Bank xizmatlarining raqamli transformatsiyasi va kiberxavfsizlikni ta'minlash muammolari" tadqiqotida O'zbekiston bank tizimida raqamli xizmatlar va moliyaviy ekotizimlar rivojlanishi bilan kiberxavfsizlikka qo'yiladigan talablar ortishi tahlil qilingan. Muallif raqamli transformatsiya yo'nalishlarini kiberxavfsizlik kontekstida tizimlashtiradi va bank tizimining barqaror faoliyatini ta'minlash masalasini alohida ko'rsatadi [9].

Madinabonu Mamatxonovanning 2026-yilda chop etilgan raqamli to'lov tizimlaridagi xavfsizlik mexanizmlariga bag'ishlangan maqolasida O'zbekiston to'lov tizimlarining 2020–2024-yillardagi rivojlanishi, firibgarlik ko'rsatkichlari va



xavfsizlik choralarini qiyosiy tahlil qilishga e'tibor qaratilgan. Tadqiqot raqamli to'lovlarning o'sishi bilan birga profilaktik va tashkiliy himoya mexanizmlarini kuchaytirish zarurligini ilgari suradi [10].

Mahalliy ishlarning amaliy ahamiyati shundaki, ular O'zbekiston bank va to'lov tizimining o'ziga xos jihatlarini, jumladan, mijozlar ishonchi, raqamli to'lovlar o'sishi va institutsional himoya choralarini yoritadi. Shu bilan birga, raqamli firibgarlik, sun'iy intellektga asoslangan hujumlar, uchinchi tomon provayderlari, API zaifliklari va tizimli kiberxavflarni yagona moliyaviy xavfsizlik arxitekturasida birlashtirib tahlil qilishga ehtiyoj mavjud.

Mazkur maqolaning ilmiy yondashuvi xalqaro tadqiqotlar va O'zbekistonning rasmiy statistik ko'rsatkichlarini birlashtirib, tahdidlarni o'zaro bog'liq tizim sifatida ko'rib chiqishdan iborat. Bu yondashuv xavflarni faqat alohida hodisalar bo'yicha sanab o'tishdan farqli ravishda, ularning moliyaviy yo'qotishlar, xizmatlar uzluksizligi va mijozlar ishonchiga birgalikdagi ta'sirini ochib berishga qaratilgan.

Tadqiqot metodologiyasi

Tadqiqotda tizimli va qiyosiy tahlil, statistik ma'lumotlarni guruhlash, mantiqiy umumlashtirish, induksiya va deduksiya usullaridan foydalanildi. Xalqaro manbalar sifatida WEF, IBM, Financial Stability Board hamda ilmiy maqolalar; milliy manbalar sifatida O'zbekiston Respublikasi Markaziy banki hisobotlari va tegishli normativ-huquqiy hujjatlar olindi [1–3; 7].

Tahlil uch bosqichda amalga oshirildi: birinchi bosqichda tahdidlar texnologik manbasi va moliyaviy oqibatiga ko'ra tasniflandi; ikkinchi bosqichda rasmiy ko'rsatkichlar yordamida xavflarning amaliy miqyosi tavsiflandi; uchinchi bosqichda O'zbekiston sharoitida xavflarni kamaytirishga qaratilgan institutsional va texnologik choralar shakllantirildi.

Tahlil va natijalar

Raqamli moliyaviy xavfsizlikka tahdidlarning asosiy shakllari.



Raqamli iqtisodiyotda moliyaviy xavfsizlikka tahdidlar texnologik zaifliklar, inson xatolari, algoritmik xatolar, ma'lumotlar konsentratsiyasi va tashqi provayderlarga bog'liqlik kesishgan nuqtada yuzaga keladi. Shu sababli xavfni faqat hujum ehtimoli bilan emas, balki moliyaviy operatsiyalarning maxfiyligi, yaxlitligi, mavjudligi va uzluksizligiga ta'siri bilan baholash maqsadga muvofiq.

1-jadval.

Raqamli iqtisodiyotda moliyaviy xavfsizlikka asosiy yangi tahdidlar¹

Tahdid turi	Asosiy mexanizm	Moliyaviy oqibat	Ustuvor himoya chorasi
AI yordamidagi hujumlar	Deepfake, avtomatlashtirilgan fishing, zaifliklarni tez aniqlash	Hisobni egallash, firibgarlik	AI nazorati, kuchli identifikatsiya
Raqamli firibgarlik	Phishing, smishing, vishing, ijtimoiy muhandislik	Mijoz mablag'lari yo'qotilishi	Real vaqt antifrod monitoringi
Ma'lumotlar buzilishi	Noqonuniy kirish, login ma'lumotlari o'g'irlanishi	Jarima, kompensatsiya, obro'ga zarar	Shifrlash, kirish huquqini cheklash
Bulut va uchinchi tomon riski	Provayderdagi uzilish yoki zaiflik	Xizmatlar to'xtashi, zanjirli ta'sir	Provayder auditi, zaxira rejasi
API va platforma riski	Autentifikatsiya zaifligi, API manipulyatsiyasi	Ma'lumot sizishi, tranzaksiya buzilishi	API xavfsizligi, tokenizatsiya



Ransomware va Tizimni shifrlash, Operatsion uzilish, Zaxira nusxasi,
model riski noto'g'ri noto'g'ri model
algoritmik qaror kredit/frod qarori validatsiyasi

Jadvaldan ko'rinadiki, tahdidlar alohida-alohida emas, balki ketma-ket rivojlanishi mumkin. Masalan, fishing orqali olingan identifikatsiya ma'lumotlari mobil bank hisobini egallashga, keyin esa pul mablag'larini boshqa hisobvaraqlarga o'tkazishga olib kelishi mumkin. Uchinchi tomon dasturiy ta'minotidagi zaiflik esa bir vaqtning o'zida bir nechta moliyaviy tashkilotlarga ta'sir ko'rsatishi ehtimolini oshiradi.

Kiberhujumlarning iqtisodiy qiymati

IBM ma'lumotlariga ko'ra, 2024-yilda moliyaviy sektorida bitta ma'lumotlar buzilishining o'rtacha qiymati 6,08 mln AQSh dollarini tashkil etgan va bu global o'rtacha ko'rsatkichdan yuqori bo'lgan [11]. IBMning 2026-yilgi hisobotida esa barcha tarmoqlar bo'yicha global o'rtacha zarar 4,99 mln dollar deb baholangan [2]. Bu ko'rsatkichlarni bevosita taqqoslashda tadqiqot yillari va qamrab olingan tarmoqlar farqini hisobga olish zarur.

Kiberhodisa bevosita moliyaviy yo'qotishdan tashqari, xizmatlarning vaqtincha to'xtashi, mijozlarning ishonchi pasayishi, huquqiy xarajatlar va operatsion tiklash xarajatlarini ham keltirib chiqaradi. Shu bois kiberxavfsizlikka investitsiya faqat IT xarajati emas, balki ehtimoliy zararlarni cheklash va biznes uzluksizligini ta'minlash vositasi sifatida qaralishi kerak.

Sun'iy intellekt: himoya vositasi va yangi xavf Manbai.

Sun'iy intellekt moliyaviy xavfsizlikka ikki tomonlama ta'sir ko'rsatadi. Bir tomondan, u katta hajmdagi tranzaksiyalarni real vaqt rejimida tahlil qilish, noodatiy xatti-harakatlarni aniqlash, zararli faoliyatni tasniflash va hodisalarga javob berish tezligini oshirish imkonini beradi. Ikkinchi tomondan, hujumchilar AI yordamida ishonarli fishing xabarlarini, soxta ovoz va videolar, avtomatlashtirilgan zararli kod hamda zaifliklarni aniqlash vositalarini yaratishi mumkin.



WEFning 2026-yilgi hisobotida respondentlarning 87 foizi AI bilan bog'liq zaifliklarni tez o'sayotgan kiberxavf deb ko'rsatgan [1]. Bu raqam barcha hujumlarning 87 foizi AI orqali amalga oshirilganini anglatmaydi; u so'rov ishtirokchilarining xavf dinamikasiga bergan bahosini ifodalaydi. Shuning uchun AI xavfsizligini texnik himoya bilan birga ma'lumotlar boshqaruvi, modelga kirish huquqi, maxfiylik va inson nazorati bilan bog'lash lozim.

Moliyaviy tashkilotlarda AI modelidan foydalanishdan oldin ma'lumotlar sifati va qonuniyligi tekshirilishi, model muntazam validatsiya qilinishi, qarorlar izohlanishi va model natijalarini inson tomonidan qayta ko'rib chiqish mexanizmi belgilanishi zarur. Ayniqsa, mijozning biometrik ma'lumotlari, kredit tarixi va tranzaksion xulqi qayta ishlanganda ma'lumotlardan foydalanish maqsadi va kirish vakolatlari qat'iy chegaralanishi kerak.

O'zbekistonda raqamli moliyaviy xizmatlar va xavfsizlik

O'zbekiston bank tizimida masofaviy xizmatlardan foydalanishning kengligi xavfsizlik choralarini keng miqyosda tashkil etishni talab etadi. Markaziy bank statistikasi bo'yicha 2025-yil 1-oktabrda Xalq bankida 8,19 mln, O'zsanoatqurilishbankda 6,01 mln, Ipoteka-bankda 4,74 mln masofaviy bank xizmatlari foydalanuvchisi qayd etilgan [3]. Ushbu raqamlar faol foydalanuvchilar sonini emas, rasmiy statistikada qayd etilgan foydalanuvchilar ko'rsatkichini anglatishi mumkin; shu sababli ularni mijozlarning noyob soni sifatida talqin qilishda manba metodologiyasi e'tiborga olinishi lozim.

2-jadval.

O'zbekistonda raqamli moliyaviy xizmatlar va xavfsizlik indikatorlari²

Ko'rsatkich	Qiymat	Davr/manba	
Xalq banki masofaviy bank xizmatlari foydalanuvchilari	8,19 mln	2025-yil	1-oktabr, Markaziy bank



O'zsanoatqurilishbank foydalanuvchilari	6,01 mln	2025-yil Markaziy bank	1-oktabr,
Ipoteka-bank foydalanuvchilari	4,74 mln	2025-yil Markaziy bank	1-oktabr,
Onlayn kredit firibgarligi holatlarida qaytarilgan mablag'	304,1 mlrd so'm	2025-yil, Markaziy bank	
Qaytarish bilan bog'liq holatlar	28 138 ta	2025-yil, Markaziy bank	
Kartalar firibgarligi bo'yicha bloklangan mablag'	9,5 mlrd so'm	Markaziy bank yillik hisoboti	

Markaziy bankning 2025-yilgi hisobotida onlayn kredit firibgarligining oldini olish doirasida qo'shimcha identifikatsiyadan o'tmagan holatlarda mablag'larni vaqtincha cheklash mexanizmi qo'llangani va 28 138 ta holatda jami 304,1 mlrd so'm mablag' kredit tashkilotlari hisobvaraqlariga qaytarilgani qayd etilgan [12]. Bank kartalari bilan bog'liq firibgarlik murojaatlari bo'yicha 9,5 mlrd so'm mablag' bloklangani ham muammoning amaliy ahamiyatini ko'rsatadi.

Raqamli firibgarlik va antifrod mexanizmlari.

Raqamli firibgarlik phishing, smishing, vishing, soxta mobil ilovalar, SIM-swap, hisobni egallash va deepfake kabi usullarning birlashuvi orqali murakkablashmoqda. Hujumchilar ko'pincha himoya tizimini texnik jihatdan buzishdan ko'ra, mijozni aldash va uning o'zidan maxfiy ma'lumotlarni olishga urinadi. Shu sababli foydalanuvchilarni xabardor qilish va tranzaksiyalarni xulq-atvor asosida tekshirish texnik nazorat bilan bir xil ahamiyatga ega.

Antifrod tizimi mijozning odatiy tranzaksiya profilini shakllantirib, yangi qurilma, noodatiy geografik joylashuv, summa keskin o'zgarishi, yangi oluvchiga pul yuborish yoki qisqa vaqt ichida bir nechta hisobga o'tkazmalar kabi belgilarni birgalikda baholashi kerak. Bitta belgi asosida operatsiyani avtomatik bloklash



noto'g'ri ijobiy natijalarni oshirishi mumkin; shu sababli risk balli, qo'shimcha tekshiruv va mijozni tasdiqlash bosqichlari uyg'unlashtirilishi maqsadga muvofiq.

Markaziy bankning 2025-yil 30-apreldagi PQ-153-son qaror bo'yicha axborotida banklar, to'lov tizimi operatorlari va to'lov tashkilotlari uchun kiberjinoyatlarning oldini olish, mijozlar moliyaviy xavfsizligini ta'minlash, tranzaksiyalarni monitoring qilish va shubhali operatsiyalarni aniqlash bo'yicha qo'shimcha vazifalar belgilangan [13]. Bu choralarning samaradorligi banklararo axborot almashinuvi, tezkor javob berish va mijozlarni qo'shimcha tekshirish jarayonlariga bog'liq.

Bulutli texnologiyalar va uchinchi tomon riski.

Banklar bulutli hisoblash, dasturiy ta'minot, identifikatsiya, API va to'lov protsessingining ayrim qismlarini tashqi provayderlarga topshirishi mumkin. Bunday yondashuv xarajatlarni optimallashtiradi, biroq riskni bank chegarasidan tashqariga olib chiqadi. Agar umumiy provayderda uzilish yuz bersa, unga bog'langan bir nechta tashkilotlarning xizmatlari bir vaqtda to'xtashi mumkin.

Uchinchi tomon riskini baholashda provayderning moliyaviy holati bilan cheklanmasdan, kiberxavfsizlik standartlari, ma'lumotlarni joylashtirish siyosati, hodisaga javob berish rejasi, zaxira nusxalash, xizmatni tiklash va shartnoma tugaganidan keyin ma'lumotlarni qaytarish yoki o'chirish mexanizmlari tekshirilishi lozim. Kritik xizmatlar uchun muqobil provayderga o'tish yoki ichki tizimga qaytish rejasi — exit strategy — oldindan ishlab chiqilishi zarur.

Financial Stability Boardning FIRE tashabbusi kiber va operatsion hodisalar bo'yicha ma'lumot almashinuvini standartlashtirishga qaratilgan [7]. O'zbekiston sharoitida ham banklar, to'lov tashkilotlari, telekommunikatsiya operatorlari va vakolatli davlat organlari o'rtasida hodisalar to'g'risidagi axborotni xavfsiz hamda tezkor almashish mexanizmlarini takomillashtirish muhim.

Moliyaviy xavfsizlikni boshqarishning takomillashtirilgan modeli.

Tadqiqot natijalari asosida raqamli iqtisodiyot sharoitida moliyaviy xavfsizlikni boshqarishning besh pog'onali modeli taklif etiladi. Model xavflarni



faqat sodir bo'lgandan keyin bartaraf etishga emas, balki ularni oldindan aniqlash, zararni cheklash va xizmatlarni tiklashga yo'naltirilgan.

3-jadval

Raqamli iqtisodiyot sharoitida moliyaviy xavfsizlikni boshqarishning besh pog'onali modeli³

Pog'ona	Mazmuni	Asosiy amaliy choralar
1. Identifikatsiya	Mijoz va qurilmani ishonchli aniqlash	Ko'p omilli va riskka asoslangan autentifikatsiya, biometrik tekshiruv
2. Real vaqt antifrod	Tranzaksiyalarni uzluksiz baholash	Xulq-atvor tahlili, risk balli, shubhali operatsiyalarni tekshirish
3. Ma'lumot va algoritmlar himoyasi	Ma'lumotlar hamda AI modellarini himoyalash	Shifrlash, tokenizatsiya, minimal kirish huquqi, model validatsiyasi
4. Kiberbarqarorlik	Xizmatlarning uzluksizligini saqlash	Tarmoq segmentatsiyasi, zaxira nusxalari, tiklash sinovlari, incident response
5. Ekotizim hamkorligi	Tashkilotlararo muvofiqlashtirish	Banklar, Markaziy bank, to'lov tashkilotlari va provayderlar axborot almashinuvi

Birinchi pog'onada mijozni autentifikatsiya qilish darajasi operatsiya xavfiga mos bo'lishi lozim. Odatdagi kichik to'lovlar bilan noodatiy katta miqdordagi yoki yangi oluvchiga yuboriladigan to'lovlar bir xil tekshiruvdan o'tmasligi kerak.



Ikkinchi pog'onada real vaqt monitoringi mijoz xatti-harakati, qurilma, tarmoq va tranzaksiya parametrlarini birgalikda baholashi zarur.

Uchinchi pog'ona ma'lumotlarni shifrlash, tokenizatsiya, kirish vakolatlarini minimallashtirish hamda AI modellarini validatsiya qilishni qamrab oladi. To'rtinchi pog'ona zaxira nusxalari, biznes uzluksizligi va favqulodda tiklash rejalarini muntazam sinovdan o'tkazishni nazarda tutadi. Beshinchi pog'ona esa kiberhodisalar haqida axborot almashish, umumiy tahdidlarni aniqlash va birgalikdagi javob choralari muvofiqlashtirishga qaratiladi.

Modelni joriy etishda natijadorlik ko'rsatkichlari ham belgilanishi lozim. Jumladan, firibgarlikni aniqlashgacha bo'lgan vaqt, oldi olingan zarar miqdori, noto'g'ri bloklangan tranzaksiyalar ulushi, hodisadan keyin xizmatni tiklash vaqti, zaxira nusxalarini tiklash sinovlari natijasi va uchinchi tomon risklarini baholash qamrovi doimiy monitoring qilinishi mumkin.

Amaliy takliflar

Birinchidan, banklar va to'lov tashkilotlarida real vaqt rejimida ishlaydigan markazlashgan antifrod mexanizmlarini rivojlantirish zarur. Ikkinchidan, yuqori riskli operatsiyalar uchun qo'shimcha autentifikatsiya va mijoz bilan mustaqil aloqa kanali orqali tasdiqlash amaliyotini kengaytirish lozim. Uchinchidan, AI tizimlari uchun model boshqaruvi, validatsiya, ma'lumotlar maxfiyligi va inson nazorati talablari ichki siyosatlarida aniq belgilanishi kerak.

To'rtinchidan, bulutli xizmatlar va boshqa texnologik provayderlar bo'yicha yagona risk reyestri yuritilib, muhim xizmatlar uchun muqobil ishlash rejasi ishlab chiqilishi maqsadga muvofiq. Beshinchidan, banklar va vakolatli organlar o'rtasida kiberhodisalar bo'yicha standartlashtirilgan axborot almashinuvi yo'lga qo'yilishi lozim. Oltinchidan, mijozlarning raqamli savodxonligini oshirish va firibgarlik usullari haqida muntazam ogohlantirish tizimi texnik choralarni to'ldirishi kerak.

Xulosa

Tadqiqot natijalari raqamli iqtisodiyotda moliyaviy xavfsizlik an'anaviy bank risklaridan tashqariga chiqib, kiberxavfsizlik, ma'lumotlar himoyasi,



algoritmik risk, uchinchi tomon provayderlariga bog‘liqlik va raqamli firibgarlikni yagona boshqaruv tizimida birlashtirishni talab etishini ko‘rsatdi. Raqamli xizmatlarning kengayishi moliyaviy xizmatlardan foydalanish qulayligini oshiradi, biroq texnologik o‘zaro bog‘liqlik kuchaygani sari bitta zaiflikning ta’siri ham kengayishi mumkin.

Xalqaro tadqiqotlar kiberhodisalar katta iqtisodiy yo‘qotishlarga sabab bo‘lishi va texnologik himoya xarajatlarini riskka mos ravishda rejalashtirish zarurligini ko‘rsatadi [5; 6; 11]. AI texnologiyalari firibgarlikni aniqlash va hodisalarga javob berishni tezlashtirishi bilan birga, soxta identifikatsiya, fishing va ma’lumotlardan noqonuniy foydalanish xavfini ham kuchaytiradi [1; 2].

O‘zbekiston misolida masofaviy bank xizmatlari foydalanuvchilarining ko‘pligi hamda 2025-yilda onlayn kredit firibgarligi bilan bog‘liq holatlarda 304,1 mlrd so‘m mablag‘ qaytarilgani raqamli moliyaviy xavfsizlikning amaliy ahamiyatini ko‘rsatadi [3; 12]. Biroq qaytarilgan va bloklangan mablag‘lar umumiy firibgarlik hajmini to‘liq ifodalamasligi sababli, kelgusida hodisalarni standart tasniflash va statistik hisobini takomillashtirish lozim.

Moliyaviy xavfsizlik siyosatining ustuvor yo‘nalishi hodisadan keyin javob berish modelidan xavfni real vaqt rejimida aniqlash va zararni cheklash modeliga o‘tishdir. Buning uchun riskka asoslangan autentifikatsiya, markazlashgan antifrod, AI tizimlarini boshqarish, kiberbarqarorlik sinovlari, uchinchi tomon riskini baholash va idoralararo tezkor axborot almashinuvi birgalikda rivojlantirilishi zarur.

Taklif etilgan besh pog‘onali model identifikatsiyadan tortib ekotizim hamkorligigacha bo‘lgan nazoratlarni birlashtiradi. Uning amaliy natijadorligi firibgarlikni aniqlash vaqti, oldi olingan zarar, noto‘g‘ri bloklashlar ulushi hamda xizmatni tiklash tezligi kabi ko‘rsatkichlar orqali baholanishi mumkin. Mazkur yondashuv raqamli transformatsiya sur‘atini pasaytirmasdan moliyaviy tizim ishonchliligi va barqarorligini mustahkamlashga xizmat qiladi.

FOYDALANILGAN ADABIYOTLAR RO‘YXATI



1. World Economic Forum. Global Cybersecurity Outlook 2026. Geneva: WEF, 2026.
2. IBM Security. Cost of a Data Breach Report 2026: AI-powered adversaries and the enterprise risk challenge. IBM, 2026.
3. O‘zbekiston Respublikasi Markaziy banki. Number of customers applied remote banking systems as of October 1, 2025. Toshkent, 2025.
4. Anderson, R. Security Engineering: A Guide to Building Dependable Distributed Systems. 3rd ed. Wiley, 2020. <https://doi.org/10.1002/9781119644682>
5. Aldasoro, I., Gambacorta, L., Giudici, P., Leach, T. Operational and cyber risks in the financial sector. CEPR Discussion Paper DP14418, 2020. <https://cepr.org/publications/dp14418>
6. Uddin, M. H., Mollah, S., Ali, M. H. Does cyber tech spending matter for bank stability? International Review of Financial Analysis, 2020. <https://doi.org/10.1016/j.irfa.2020.101587>
7. Financial Stability Board. Format for Incident Reporting Exchange (FIRE): Final report. 15 April 2025.
8. Mamadiyarov, Z., Karshiev, D. Cybersecurity in Digital Banking: Safeguarding Customer Trust in Uzbekistan. American Journal of Corporate Management, 1(2), 2024.
9. Mengniyozov, A. Bank xizmatlarining raqamli transformatsiyasi va kiberxavfsizlikni ta’minlash muammolari. Iqtisodiy taraqqiyot va tahlil, 4(2), 2026, 129–139. <https://doi.org/10.60078/2992-877X-2026-vol4-iss2-pp129-139>
10. Mamatxonova, M. Security Assurance Mechanisms in Digital Payment Systems in Uzbekistan. Raqamli gumanitar tadqiqotlar, 2026, 27–31. <https://doi.org/10.5281/zenodo.23202502>
11. IBM Security. Cost of a Data Breach 2024: Financial Industry. IBM, 2024.
12. O‘zbekiston Respublikasi Markaziy banki. Annual Report 2025. IV bo‘lim: National Payment System, Banking Information Technologies and Cybersecurity. Toshkent, 2026.



13. O'zbekiston Respublikasi Markaziy banki. 2025-yil 30-apreldagi PQ-153-son qaror bo'yicha axborot: axborot texnologiyalari yordamida sodir etiladigan jinoyatlarga qarshi kurashish choralari.