RAQAMLI BANK XIZMATLARIDA KIBERXAVFSIZLIKNI TA’MINLASHNING DOLZARB MASALALARI

Shokirov Sardor Inotdullo o‘g‘li
Buxoro davlat universiteti o‘qituvchisi

Annotatsiya. *Mazkur maqolada raqamli bank xizmatlarida kiberxavfsizlikni ta’minlashning dolzarb masalalari tahlil qilinadi. Tadqiqotda mobil banking, internet-banking, elektron to‘lovlar, masofaviy identifikatsiya, onlayn kreditlash va API integratsiyalari bilan bog‘liq kiberxatarlar tizimlashtirilgan. Raqamli bank xizmatlarida kiberxavfsizlikni boshqarish modeli taklif qilinib, uning boshqaruv, profilaktika, aniqlash, javob qaytarish va tiklanish bosqichlari ishlab chiqildi. Shuningdek, banklar uchun antifrod tizimlari, ko‘p omilli autentifikatsiya, xavfsiz API boshqaruvi, kiberxavfsizlik auditi, xodimlar va mijozlarning kiberxavfsizlik bo‘yicha savodxonligini oshirishga doir amaliy takliflar berilgan.*

Kalit so‘zlar: *raqamli bank, kiberxavfsizlik, mobil banking, internet-banking, antifrod, phishing, biometrik identifikatsiya, ma’lumotlarni himoya qilish, elektron to‘lovlar, kiberxatar, moliyaviy firibgarlik, operatsion barqarorlik.*

KIRISH

Jahon iqtisodiyotida bank tizimining raqamlashtirilishi moliyaviy xizmatlar ko‘rsatish shakli, tezligi va mazmunini tubdan o‘zgartirmoqda. Bugungi kunda mijozlar mobil ilovalar, internet-banking, elektron hamyonlar, QR-kodli to‘lovlar, kontaktsiz to‘lov vositalari, masofaviy identifikatsiya hamda onlayn kreditlash xizmatlari orqali bank filialiga bormasdan turib turli moliyaviy operatsiyalarni amalga oshirmoqda. Bunday imkoniyatlar aholi va biznes uchun qulaylik yaratishi bilan bir qatorda, bank tizimida yangi turdagi texnologik va kiberxatarlarni ham yuzaga chiqarmoqda.

Raqamli bank xizmatlarining kengayishi bank mijozlari soni, tranzaksiyalar hajmi va qayta ishlanayotgan shaxsiy hamda moliyaviy ma’lumotlar miqdorining ortishiga olib keladi. Natijada bank axborot tizimlari kiberjinoyatchilar uchun jozibador nishonga aylanadi. Xususan, mijozlarning karta ma’lumotlarini qo‘lga kiritish, soxta mobil ilovalar yaratish, phishing xabarlari yuborish, bir martalik tasdiqlash kodlarini aldov yo‘li bilan olish, mobil qurilmalarga zararli dasturlar o‘rnatish, hisobvaraqlardan ruxsatsiz mablag‘ yechib olish kabi holatlar ko‘payishi mumkin.

O‘zbekistonda raqamli bank va to‘lov xizmatlari jadal rivojlanmoqda. Masofaviy bank xizmatlaridan foydalanuvchilar sonining ortishi, elektron hamyonlar, mobil ilovalar, QR va NFC to‘lovlarining kengayishi kiberxavfsizlikni bank faoliyatining ikkilamchi emas, balki strategik yo‘nalishiga aylantirmoqda. Shu bois banklarning texnologik rivojlanishi xavfsizlik standartlari, ma’lumotlarni himoya qilish, antifrod mexanizmlari va operatsion uzluksizlik bilan uyg‘un holda tashkil etilishi zarur.

Mavzuning dolzarbligi shundaki, raqamli bank xizmatlarida yuz beradigan kiberhodisalar nafaqat alohida mijozlar mablag‘lariga, balki banklarning obro‘si, mijozlar

ishonchi, to‘lov tizimlarining uzluksiz ishlashi va butun moliyaviy tizim barqarorligiga salbiy ta’sir ko‘rsatishi mumkin.

Tadqiqotning maqsadi — O‘zbekistonda raqamli bank xizmatlarida uchraydigan asosiy kiberxatarlarni aniqlash, amaldagi himoya mexanizmlarini baholash va bank tizimida kiberxavfsizlikni takomillashtirish bo‘yicha ilmiy-amaliy takliflar ishlab chiqishdan iborat.

Tadqiqot obyekti — tijorat banklari, to‘lov tashkilotlari va raqamli moliyaviy xizmatlar ekotizimi.

Tadqiqot predmeti — raqamli bank xizmatlarida axborot xavfsizligi, kiberxatarlarni boshqarish, antifrod tizimlari, mijoz ma’lumotlarini himoya qilish hamda operatsion barqarorlikni ta’minlash mexanizmlari.

Tadqiqotning ilmiy yangiligi quyidagilarda namoyon bo‘ladi:

- raqamli bank xizmatlaridagi kiberxatarlar tashkiliy, texnik va ijtimoiy omillar asosida tizimlashtirildi;
- raqamli bank xavfsizligini boshqarishning “boshqaruv–profilaktika–aniqlash–javob qaytarish–tiklanish” modeli taklif qilindi;
- antifrod tizimlari, biometrik autentifikatsiya va mijozlarning kiberxavfsizlik savodxonligini o‘zaro bog‘liq holda rivojlantirish zarurligi asoslandi;
- banklar uchun kiberxatarlarni baholashning amaliy yo‘nalishlari ishlab chiqildi.

Tadqiqot metodologiyasi. Mazkur tadqiqotda ilmiy bilishning bir qator umumiy va maxsus usullaridan foydalanildi. Xususan, kontent tahlil usuli orqali O‘zbekiston Respublikasining kiberxavfsizlik, shaxsga doir ma’lumotlar, bank faoliyati va to‘lov tizimlariga oid qonunchilik hujjatlari o‘rganildi. Markaziy bankning yillik hisobotlari, to‘lov tizimlari bo‘yicha statistik ma’lumotlari, CERT-CBU faoliyatiga oid rasmiy axborotlar tahlil qilindi.

Qiyosiy tahlil usuli yordamida O‘zbekiston bank tizimidagi kiberxavfsizlik amaliyoti NIST Cybersecurity Framework 2.0, ISO/IEC 27001:2022, PCI DSS v4.0.1 hamda Bazel qo‘mitasining operatsion barqarorlik tamoyillari bilan solishtirildi. Tizimli yondashuv asosida raqamli bank ekotizimidagi banklar, to‘lov tashkilotlari, fintech kompaniyalari, mobil aloqa operatorlari, mijozlar, davlat organlari va xalqaro to‘lov tizimlari o‘rtasidagi o‘zaro bog‘liqlik baholandi.

Shuningdek, risklarga yo‘naltirilgan yondashuv asosida kiberxatarlarning kelib chiqish manbasi, yuzaga kelish ehtimoli, ehtimoliy zarar darajasi va oldini olish choralariga doir tahliliy matritsa tuzildi. Tadqiqot natijalari ochiq statistik ma’lumotlar va normativ manbalar asosida shakllantirilgan bo‘lib, empirik so‘rovnoma natijalariga asoslanmagan.

O‘zbekistonda raqamli to‘lov infratuzilmasining kengayishi bank xizmatlarining ommaviyligi ortib borayotganini ko‘rsatadi. Bunda masofaviy bank xizmatlari, bank kartalari, to‘lov terminallari, mobil ilovalar va elektron hamyonlar bank-moliya tizimining muhim tarkibiy qismiga aylanmoqda.

Quyidagi ko‘rsatkichlar raqamli bank xizmatlarining kengayib borayotganini ko‘rsatsa-da, ularning ortishi bilan birga hujum yuzasi ham kengayadi. Chunki bankning mobil ilovasi, internet-banking portali, API interfeyslari, kartalarni boshqarish tizimi, ichki

ma’lumotlar bazasi, call-markazlari va uchinchi tomon servislarining har biri kiberxatar manbai bo‘lishi mumkin.

1-jadval

O‘zbekistonda raqamli bank va to‘lov infratuzilmasining ayrim ko‘rsatkichlari

Ko‘rsatkich	2025-yil 1-yanvar holati
Muomaladagi bank kartalari soni	62,0 mln dona
To‘lov terminallari soni	426 ming dona
To‘lov terminallari orqali amalga oshirilgan to‘lovlar hajmi	326,7 trln so‘m
Bankomat va infokiosklar soni	29,9 mingdan ortiq
Masofaviy bank xizmatlari foydalanuvchilari	52,9 mln
Shundan jismoniy shaxslar	51,4 mln
Shundan biznes subyektlari	1,5 mln
Mobil ilovalar orqali jismoniy shaxslarning onlayn tranzaksiyalari	396,7 trln so‘m
To‘lov tashkilotlari soni	44 ta
To‘lov tashkilotlari orqali tranzaksiyalar hajmi	333 trln so‘m
Raqamli identifikatsiyadan o‘tgan mijozlar soni	12,2 mln

Manba: O‘zbekiston Respublikasi Markaziy bankining 2024-yil yakunlari bo‘yicha yillik hisobotidan tuzildi.

Masofaviy bank xizmatlari foydalanuvchilari haqidagi statistika individual shaxslar sonini emas, balki bank tizimlarida qayd etilgan foydalanuvchi hisoblari yig‘indisini ifodalashi mumkin. Shunga qaramay, ushbu ko‘rsatkich raqamli bank tizimiga bo‘lgan talabning yuqori ekanini va uning himoyasiga qo‘yiladigan talablar oshib borayotganini anglatadi.

O‘zbekistonda kiberxavfsizlikni ta’minlashning normativ-huquqiy asoslari bosqichma-bosqich shakllanmoqda. “Kiberxavfsizlik to‘g‘risida”gi Qonun davlat organlari, xo‘jalik yurituvchi subyektlar va boshqa ishtirokchilarning mazkur sohadagi vakolatlari hamda majburiyatlarini belgilaydi. Ushbu qonun muhim axborot infratuzilmasi obyektlarining xavfsizligini ta’minlash, kiberhodisalarning oldini olish, aniqlash va oqibatlarini bartaraf etish bo‘yicha umumiy talablarni shakllantiradi.

“Shaxsga doir ma’lumotlar to‘g‘risida”gi Qonun banklar uchun alohida ahamiyat kasb etadi. Chunki banklar mijozlarning shaxsiy ma’lumotlari, biometrik identifikatsiya ma’lumotlari, hisobvaraqlar, kredit tarixi, tranzaksiyalar va aloqa ma’lumotlarini qayta ishlaydi. Ushbu ma’lumotlarning qonuniy, maqsadli va xavfsiz qayta ishlanishi mijozlar ishonchining asosiy shartidir.

Markaziy bank huzuridagi CERT-CBU markazi banklar, kredit va to‘lov tashkilotlari, to‘lov tizimi operatorlarining kiberxavfsizligini muvofiqlashtirishda muhim

o‘rin egallaydi. Markazning asosiy vazifalari qatoriga muhim axborot infratuzilmasi obyektlarini aniqlash, axborot tizimlarini ekspertizadan o‘tkazish, kiberhodisalarni monitoring qilish, ularning oqibatlarini bartaraf etishni kuzatish hamda profilaktik chora-tadbirlar bo‘yicha tavsiyalar ishlab chiqish kiradi.

2024-yilda Markaziy bank tomonidan to‘lov tizimi operatorlari va to‘lov xizmati provayderlari uchun axborot xavfsizligi hamda kiberxavfsizlikni ta’minlashga oid nizom ishlab chiqilib, amaliyotga joriy etildi. Bundan tashqari, onlayn mikroqarzlar bilan bog‘liq firibgarlikning oldini olish maqsadida qo‘shimcha identifikatsiyadan o‘tmagan arizalar bo‘yicha vaqtinchalik cheklovlar joriy qilingan.

Raqamli bank ilovalarida yangi qurilmadan kirish, parolni tiklash va yangi ro‘yxatdan o‘tish jarayonlarida Face ID mexanizmlarining joriy qilinishi ham karta firibgarligini kamaytirishga xizmat qilmoqda. Biroq biometrik identifikatsiya xavfsizlikning yagona vositasi emas, balki ko‘p qatlamli himoya tizimining tarkibiy qismi sifatida qaralishi lozim.

Tadqiqot natijasida raqamli bank xizmatlarida kiberxavfsizlikni boshqarishning besh bosqichli modeli taklif qilinadi.

2-jadval

Raqamli bank xizmatlarida kiberxavfsizlikni boshqarish modeli

Bosqich	Asosiy mazmuni	Bank uchun amaliy chora
1. Boshqaruv	Xavfsizlik siyosati, javobgarlik va risk-appetitni belgilash	Kuzatuv kengashi darajasida kiberxavfsizlik siyosatini tasdiqlash
2. Profilaktika	Hujum yuzasini kamaytirish va zaifliklarning oldini olish	MFA, biometrik himoya, shifrlash, segmentatsiya, xodimlarni o‘qitish
3. Aniqlash	Shubhali hodisalarni erta aniqlash	SIEM, SOC, antifrod, tranzaksiya monitoringi, loglarni tahlil qilish
4. Javob qaytarish	Hodisani cheklash va zarar miqdorini kamaytirish	Incident response rejasi, kartani bloklash, mijozni xabardor qilish
5. Tiklanish	Xizmatlarni qayta ishga tushirish va saboqlarni tizimlashtirish	Zaxira nusxalar, avariya tiklash rejasi, post-incident tahlil

Ushbu model NIST Cybersecurity Framework 2.0 dagi “Govern, Identify, Protect, Detect, Respond, Recover” funksiyalariga mos keladi. Modelning ustunligi shundaki, unda xavfsizlik faqat hujum sodir bo‘lgandan keyingi reaktsiya sifatida emas, balki bank strategiyasi va kundalik operatsion faoliyatining ajralmas qismi sifatida talqin qilinadi.

Bank tizimida kiberxavfsizlikni boshqarish bo‘yicha kuzatuv kengashi, boshqaruv organi, risk-menejment bo‘linmasi, axborot texnologiyalari bo‘limi, ichki audit xizmati va kiberxavfsizlik bo‘linmasining vazifalari aniq belgilanishi lozim. Ayniqsa, xavfsizlik uchun javobgarlik faqat IT bo‘limi zimmasiga yuklanmasligi, balki butun bank miqyosida taqsimlangan boshqaruv tizimi shakllantirilishi kerak.

Muhokama

Raqamli bank xizmatlarida kiberxavfsizlikni ta’minlash bo‘yicha xalqaro amaliyot banklar uchun uch asosiy xulosani beradi. Birinchidan, kiberxavfsizlik texnik masala bo‘lish bilan birga, korporativ boshqaruv va operatsion risklarni boshqarish masalasi hamdir. Ikkinchidan, banklar kiberhodisa yuz berishini istisno holat deb emas, balki ehtimoli mavjud operatsion xavf sifatida qabul qilishi zarur. Uchinchidan, xavfsizlikni ta’minlashning eng samarali shakli ko‘p qatlamli himoya hisoblanadi.

Bazel qo‘mitasining operatsion barqarorlik tamoyillarida banklar axborot-kommunikatsiya texnologiyalari va kiberxavfsizlik bo‘yicha hujjatlashtirilgan siyosatga ega bo‘lishi, unda boshqaruv, javobgarlik, kirishni boshqarish, muhim axborot aktivlarini himoya qilish, monitoring, hodisaga javob qaytarish, biznes uzluksizligi va avariya tiklash mexanizmlari belgilanishi lozimligi ta’kidlanadi .

Raqamli bank xizmatlarida xavfsizlikni ta’minlash jarayonida ko‘p omilli autentifikatsiya muhim ahamiyat kasb etadi. Mijozning faqat parol bilan tizimga kirishi yetarli emas. Tizimga kirishda parol, biometrik belgi, ishonchli qurilma, bir martalik kod yoki xulq-atvor tahliliga asoslangan qo‘shimcha tekshiruvlardan foydalanish maqsadga muvofiq. Ayniqsa, yangi qurilmadan kirish, yirik miqdordagi mablag‘ o‘tkazish, parolni tiklash, karta bog‘lash va kredit rasmiylashtirish kabi yuqori xatarli operatsiyalar kuchaytirilgan tekshiruvni talab etadi.

Shu bilan birga, mobil ilovalar va API interfeyslarining himoyasi ustuvor yo‘nalishga aylanishi kerak. Banklar dasturiy mahsulotni ishlab chiqish jarayonining dastlabki bosqichidan boshlab xavfsizlik talablarini inobatga olishi zarur. Bu yondashuv “Security by Design” tamoyili sifatida e’tirof etiladi. Mobil ilovalarda kodni himoya qilish, root yoki jailbreak qilingan qurilmalarni aniqlash, sessiyalarni xavfsiz boshqarish, API so‘rovlarini autentifikatsiyalash, ma’lumotlarni shifrlash hamda zaifliklarni muntazam bartaraf etish talab etiladi.

To‘lov kartalari bilan ishlovchi banklar va xizmat ko‘rsatuvchi subyektlar PCI DSS talablariga muvofiq karta ma’lumotlarini himoya qilishga e’tibor qaratishi lozim. Ushbu standart karta hisobvaraqlari ma’lumotlari xavfsizligini ta’minlash uchun texnik va tashkiliy minimal talablarni belgilaydi. Axborot xavfsizligini boshqarish tizimida esa ISO/IEC 27001:2022 standarti risklarni aniqlash, himoya choralarini belgilash, ularning samaradorligini baholash va doimiy takomillashtirish uchun metodik asos bo‘lib xizmat qiladi.

Raqamli bank xizmatlaridagi eng murakkab muammo inson omili bilan bog‘liqdir. Ko‘plab holatlarda kiberjinoyatchilar bankning texnik tizimini buzishdan ko‘ra, mijozning ishonchidan foydalanishga harakat qiladi. Soxta bank xodimi sifatida telefon qilish, mijozga “karta bloklanadi” mazmunidagi xabar yuborish, soxta havola orqali mobil ilovaga o‘xshash sahifaga yo‘naltirish kabi usullar aynan shu omilga asoslanadi. Shu sababli banklar tomonidan mijozlarga doimiy ravishda “bank xodimi hech qachon karta paroli yoki SMS-kod so‘ramaydi” mazmunidagi tushuntirishlar berib borilishi muhimdir.

Xulosa va takliflar

Tadqiqot natijalari shuni ko‘rsatdiki, raqamli bank xizmatlarining kengayishi O‘zbekistonda bank xizmatlari sifati, tezkorligi va qulayligini oshirmoqda. Biroq mobil banking, internet-banking, elektron to‘lovlar, biometrik identifikatsiya va onlayn kreditlash xizmatlarining ko‘payishi bilan birga kiberxatarlar ham murakkablashib bormoqda.

Phishing, ijtimoiy muhandislik, karta firibgarligi, mobil ilova zaifliklari, ma’lumotlar sizib chiqishi, DDoS hujumlari, ichki tahdidlar va uchinchi tomon servislaridan kelib chiqadigan risklar bank tizimi uchun asosiy tahdidlar hisoblanadi. Ularni kamaytirish uchun texnik, tashkiliy va huquqiy choralarni yagona tizim sifatida qo‘llash talab etiladi.

Tadqiqot yakunlari asosida quyidagi takliflar ilgari suriladi:

1. **Banklarda kuzatuv kengashi darajasida kiberxavfsizlik boshqaruvini kuchaytirish zarur.** Har bir bankning kiberxatarlar bo‘yicha risk-appetiti, javobgar shaxslari, ichki siyosati va asosiy samaradorlik ko‘rsatkichlari belgilanishi lozim.
2. **Ko‘p omilli autentifikatsiya tizimini kengaytirish kerak.** Parol, Face ID, qurilma identifikatsiyasi va bir martalik tasdiqlash kodlari yuqori xatarli operatsiyalarda birgalikda qo‘llanilishi maqsadga muvofiq.
3. **Markazlashgan antifrod tizimlarini rivojlantirish lozim.** Banklar va to‘lov tashkilotlari o‘rtasida shubhali tranzaksiyalar, firibgarlik kartalari va zararli rekvizitlar bo‘yicha tezkor axborot almashinuvi yo‘lga qo‘yilishi kerak.
4. **Mobil ilovalar va API xavfsizligini muntazam baholash talab etiladi.** Dasturiy mahsulotlar ishga tushirilishidan oldin xavfsizlik sinovlari, kod tahlili, penetratsion test va zaifliklarni skanerlash amaliyotini joriy qilish zarur.
5. **Mijozlarning kiberxavfsizlik savodxonligini oshirish muhimdir.** Banklar mobil ilovalar, SMS-xabarlar, ijtimoiy tarmoqlar va ommaviy axborot vositalari orqali phishing hamda karta firibgarligi xavfi bo‘yicha muntazam tushuntirish ishlari olib borishi kerak.
6. **Xodimlar uchun doimiy kiberxavfsizlik treninglari tashkil etilishi lozim.** Xodimlarning fishing xabarlarini aniqlash, mijoz ma’lumotlari bilan xavfsiz ishlash, shubhali hodisalarni tezkor xabar qilish ko‘nikmalarini rivojlantirish zarur.
7. **Uchinchi tomon risklarini boshqarish mexanizmlarini kuchaytirish kerak.** Fintech kompaniyalari, bulutli xizmatlar, dasturiy mahsulot yetkazib beruvchilari va boshqa hamkorlarning xavfsizlik darajasini oldindan baholash zarur.
8. **Biznes uzluksizligi va avariya tiklash rejalarini sinovdan o‘tkazish talab etiladi.** Banklar kiberhodisa, ma’lumotlar markazi ishdan chiqishi yoki to‘lov tizimi uzilishi kabi holatlar uchun muntazam amaliy mashqlar o‘tkazishi lozim.
9. **Shaxsga doir ma’lumotlarni himoya qilish kuchaytirilishi zarur.** Banklar faqat zarur ma’lumotlarni yig‘ishi, ularni shifrlashi, kirish vakolatlarini cheklashi va ma’lumotlarni qayta ishlash jarayonlari bo‘yicha shaffof axborot taqdim etishi kerak.

Umuman olganda, raqamli bank xizmatlarida kiberxavfsizlikni ta’minlash banklarning raqobatbardoshligi, mijozlar ishonchi va moliyaviy tizim barqarorligini ta’minlashning asosiy shartlaridan biridir. Shu bois O‘zbekistonda raqamli bank rivoji xavfsizlik, ishonchlilik va operatsion barqarorlik tamoyillari bilan uyg‘un holda davom ettirilishi zarur.

FOYDALANILGAN ADABIYOTLAR:

1. O‘zbekiston Respublikasining 2022-yil 15-apreldagi O‘RQ-764-son Qonuni. **“Kiberxavfsizlik to‘g‘risida”**.

2. O‘zbekiston Respublikasining 2019-yil 2-iyuldagi O‘RQ-547-son Qonuni. **“Shaxsga doir ma’lumotlar to‘g‘risida”**.

3. O‘zbekiston Respublikasi Markaziy banki. **Annual Report 2024.** Toshkent, 2025.

4. O‘zbekiston Respublikasi Markaziy banki. **CERT-CBU kiberxavfsizlik markazi faoliyati to‘g‘risida rasmiy ma’lumotlar.** 2025.

5. O‘zbekiston Respublikasi Markaziy banki. **Bank kartalari bilan bog‘liq firibgarlikning oldini olish bo‘yicha rasmiy bayonot.** 2025.

6. National Institute of Standards and Technology. **The NIST Cybersecurity Framework (CSF) 2.0.** Gaithersburg, MD: NIST, 2024.

7. Basel Committee on Banking Supervision. **Principles for Operational Resilience.** Bank for International Settlements, 2021.

8. PCI Security Standards Council. **Payment Card Industry Data Security Standard: PCI DSS v4.0.1.** 2024.

9. International Organization for Standardization. **ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection — Information security management systems — Requirements.** Geneva: ISO, 2022.

10. International Monetary Fund. **Republic of Uzbekistan: Financial Sector Assessment Program — Financial System Stability Assessment.** IMF Country Report, 2025.

11. O‘zbekiston Respublikasi Prezidentining 2020-yil 12-maydagi PF-5992-son Farmoni. **“2020–2025-yillarga mo‘ljallangan O‘zbekiston Respublikasining bank tizimini isloh qilish strategiyasi to‘g‘risida”**.