

Banklarda raqamli texnologiyalardan foydalanishda yuzaga keladigan moliyaviy xatarlarni boshqarish usullarini takomillashtirish

Asemova Rano Japbarbergenovna
Uzsanoatqurilishbank ATB Qo'ng'iroq BXM
Service manager bosh mutaxasisi

Annotatsiya: Raqamli texnologiyalar bank tizimida xizmatlar ko'rsatish sifati va tezligini oshirishga xizmat qilmoqda. Shu bilan birga, bu texnologiyalar moliyaviy xatarlarning yangi shakllarini keltirib chiqarmoqda. Ushbu maqolada bank tizimida raqamli texnologiyalardan foydalanish jarayonida yuzaga keladigan moliyaviy xatarlar, ularning turlari, sabablari va oqibatlari tahlil qilinadi. Shuningdek, mavjud xatarlarni aniqlash, baholash va samarali boshqarish mexanizmlarini takomillashtirish bo'yicha ilg'or yondashuvlar va amaliy tavsiyalar bayon etiladi. Maqolada xalqaro tajriba asosida O'zbekistonda bank sektorida raqamli xavfsizlikni ta'minlash va risklarni kamaytirish bo'yicha strategik yo'nalishlar ishlab chiqiladi.

Kalit so'zlar: raqamli texnologiyalar, bank tizimi, moliyaviy xatarlar, risklarni boshqarish, raqamli xavfsizlik, kiberxavf, bank xizmatlari, texnologik risk, strategik boshqaruv

Аннотация: Цифровые технологии повышают качество и скорость предоставления услуг в банковской системе. Одновременно эти технологии порождают новые формы финансовых рисков. В данной статье анализируются финансовые риски, возникающие при использовании цифровых технологий в банковской системе, их виды, причины и последствия. Также описываются передовые подходы и практические рекомендации по совершенствованию механизмов выявления, оценки и эффективного управления существующими рисками. В статье разрабатываются стратегические направления обеспечения цифровой безопасности и снижения рисков в банковском секторе Узбекистана на основе международного опыта.

Ключевые слова: цифровые технологии, банковская система, финансовые риски, управление рисками, цифровая безопасность, киберриск, банковские услуги, технологический риск, стратегическое управление



Abstract: Digital technologies are improving the quality and speed of service provision in the banking system. At the same time, these technologies are creating new forms of financial risks. This article analyzes the financial risks that arise in the process of using digital technologies in the banking system, their types, causes and consequences. It also describes advanced approaches and practical recommendations for improving mechanisms for identifying, assessing and effectively managing existing risks. The article develops strategic directions for ensuring digital security and reducing risks in the banking sector of Uzbekistan based on international experience.

Keywords: digital technologies, banking system, financial risks, risk management, digital security, cyber risk, banking services, technological risk, strategic management

Kirish: Bugungi kunda raqamli texnologiyalarning jadal rivojlanishi bank-moliya tizimini tubdan o'zgartirib yubormoqda. An'anaviy bank xizmatlari asta-sekinlik bilan zamonaviy raqamli yechimlar bilan almashtirilmoqda. Masofaviy bank xizmatlari, mobil ilovalar, blokcheyn, sun'iy intellekt va bulutli texnologiyalar bank amaliyotining ajralmas qismiga aylangan. Bu o'zgarishlar bir tomondan xizmatlarning qulayligi va samaradorligini oshirsa, ikkinchi tomondan, yangi moliyaviy xatarlar va xavf-xatarlarni boshqarish zaruratini yuzaga keltirmoqda.

Banklar uchun raqamli muhitda faoliyat yuritish nafaqat texnik imkoniyatlarga, balki xatarlarni oldindan aniqlash, baholash va ularni samarali boshqarishga ham bog'liq. Shu sababli, banklarda raqamli texnologiyalar bilan bog'liq moliyaviy xatarlarni chuqur o'rganish va ularga qarshi kurashish strategiyalarini ishlab chiqish bugungi kunning dolzarb masalalaridan biridir. Ushbu maqolada aynan shu yo'nalishdagi muammolar tahlil qilinadi va takomillashtirish bo'yicha asosli tavsiyalar beriladi.

Asosiy qism: Zamonaviy bank tizimi global raqamli transformatsiya jarayonining eng faol ishtirokchilaridan biri hisoblanadi. Moliya muassasalari mijozlarga qulay va tezkor xizmat ko'rsatish maqsadida raqamli texnologiyalarni joriy etishga katta e'tibor qaratmoqda. Xususan, mobil banking, onlayn to'lovlar, elektron hisob-kitoblar, sun'iy intellektga asoslangan xizmatlar va blokcheyn texnologiyalar bank amaliyotining ajralmas qismiga aylangan.

Biroq, texnologik rivojlanish bilan bir qatorda yangi moliyaviy xatarlar, xususan **kiberxavfsizlik tahdidlari, axborotlar oqish xavfi, texnik nosozliklar va**



inson omiliga bog‘liq risklar ortib bormoqda. Bu holat banklar faoliyatining barqarorligi, mijozlar mablag‘larining himoyalaniishi va umuman moliyaviy tizim ishonchliligiga salbiy ta‘sir ko‘rsatishi mumkin.

O‘zbekiston Respublikasida ham raqamli iqtisodiyot konsepsiyasining bosqichma-bosqich amalga oshirilishi, banklar tomonidan zamonaviy texnologiyalarni joriy etishning jadallashuvi ushbu mavzuni dolzarb qilib qo‘ymoqda. Ayniqsa, **raqamli texnologiyalar bilan bog‘liq moliyaviy xatarlarni aniqlash, baholash va samarali boshqarish usullarini takomillashtirish** bugungi kundagi muhim masalalardan biridir.

Shu nuqtai nazardan, ushbu mavzuni chuqur o‘rganish nafaqat nazariy, balki amaliy ahamiyatga ega bo‘lib, bank tizimida xavfsizlikni ta‘minlash, mijozlar ishonchini oshirish va barqaror raqamli rivojlanishga zamin yaratishga xizmat qiladi.

Bank tizimida raqamli texnologiyalar: imkoniyatlar va xavflar

So‘nggi yillarda bank sohasida raqamli transformatsiya jarayoni tezlashib bormoqda. Masofaviy bank xizmatlari, mobil bank ilovalari, onlayn to‘lov tizimlari, sun‘iy intellekt asosidagi mijozlarga xizmat ko‘rsatish tizimlari va blokcheyn texnologiyalarining joriy etilishi bank amaliyotini sezilarli darajada soddalashtirdi. Biroq, bu bilan birga quyidagi moliyaviy xatarlar ham kuchaymoqda:

- **Kiberxavfsizlik tahdidlari** – xakerlik hujumlari, ma‘lumotlar o‘g‘irlanishi, firibgarlik holatlari;
- **Texnologik nosozliklar** – serverlar ishdan chiqishi, dasturiy ta‘minotdagi xatoliklar;
- **Inson omiliga bog‘liq xatarlar** – xodimlarning noto‘g‘ri harakatlari, e‘tiborsizlik;
- **Regulyator talablariga rioya qilinmasligi** – yangi texnologiyalarning qonunchilikka mos kelmasligi.

Ushbu xavflarning barchasi bank faoliyatida moliyaviy yo‘qotishlarga, mijozlar ishonchini yo‘qotishga va hatto moliyaviy barqarorlikka tahdid solishi mumkin.

Moliyaviy xatarlarni boshqarishning amaldagi usullari

Bugungi kunda ko‘plab banklar moliyaviy xatarlarni kamaytirish uchun quyidagi usullardan foydalanmoqda:



- **Risiklarni aniqlash va tahlil qilish tizimlari** – potentsial xatarlarni oldindan baholash orqali profilaktik choralar ko‘rish;
- **Axborot xavfsizligi siyosatlarini** – bank ichida qat’iy xavfsizlik protokollarini ishlab chiqish va amaliyotga joriy etish;
- **Texnologik audit** – bank infratuzilmasining texnik holatini muntazam tahlil qilish;
- **Xodimlar malakasini oshirish** – xavfsizlik bo‘yicha muntazam treninglar va ko‘nikmalarni shakllantirish;
- **Sug‘urtalash** – muayyan xatarlarni sug‘urtalab moliyaviy yo‘qotishlarning oldini olish.

Ammo mavjud choralar yetarli darajada kompleks emas, ko‘plab banklar zamonaviy texnologiyalarga moslashishda qiynalmoqda.

Moliyaviy xatarlarni boshqarish usullarini takomillashtirish yo‘llari

Bank sohasida raqamli texnologiyalar asosida yuzaga keladigan xatarlarni samarali boshqarish uchun quyidagi takomillashtirish yo‘llari muhim hisoblanadi:

- ✓ **Kiberxavfsizlik infratuzilmasini mustahkamlash:** ilg‘or shifrlash algoritmlari, ikki bosqichli autentifikatsiya va xavfsizlik devorlarini (firewall) keng joriy etish.
- ✓ **AI va Big Data asosida risk monitoring tizimlarini ishlab chiqish:** katta hajmdagi ma‘lumotlar tahlili orqali xavflarni real vaqt rejimida aniqlash.
- ✓ **Raqamli transformatsiya strategiyasini ishlab chiqish:** texnologik yangiliklarni bosqichma-bosqich, tizimli joriy qilish.
- ✓ **Xodimlar va mijozlar uchun raqamli savodxonlik dasturlarini ishlab chiqish:** foydalanuvchilarning xatolarga yo‘l qo‘ymasligi uchun ularni o‘qitish.
- ✓ **Moliyaviy va texnologik auditlarni avtomatlashtirish:** muntazam monitoring qilish imkonini beruvchi tizimlar orqali ichki nazoratni kuchaytirish.

Bundan tashqari, banklar o‘z faoliyatida xalqaro tajribaga tayangan holda, regulyatorlar bilan yaqin hamkorlikda ishlashi lozim.

Muhokama: Raqamli texnologiyalarning bank tizimidagi keng ko‘lamli joriy etilishi bir tomondan xizmatlar samaradorligini oshirish, xarajatlarni kamaytirish va mijozlarga qulaylik yaratish imkonini bersa, ikkinchi tomondan, murakkab va o‘zgaruvchan xatarlarni ham yuzaga keltirmoqda. Ayniqsa, oxirgi yillarda tez-tez



uchrayotgan kiberhujumlar va texnologik nosozliklar banklarning raqamli xavfsizlik infratuzilmasini jiddiy mustahkamlash zaruratini ko‘rsatmoqda.

Tahlillar shuni ko‘rsatadiki, O‘zbekiston bank tizimi bu borada hali to‘liq integratsiyalashgan, xavfsizlikni to‘la ta‘minlaydigan raqamli muhitni yaratishda muammolarga duch kelmoqda. Banklarning bir qismi zamonaviy texnologiyalarni joriy etgan bo‘lsa-da, ularda xatarlarni real vaqt rejimida tahlil qilish va boshqarish tizimlari yetarli darajada rivojlanmagan.

Muhokamaga sabab bo‘ladigan muhim jihatlardan biri – bu xatarlarning xilma-xilligi va murakkabligidir. Ular quyidagicha tasniflanadi:

- **Texnik xatarlar** – server ishdan chiqishi, dasturiy nosozliklar, texnologik yangiliklarga noto‘g‘ri moslashuv.

- **Axborot xavfsizligi xatarlar** – shaxsiy ma‘lumotlarning sizib chiqishi, kiberfiribgarlik.

- **Inson omiliga bog‘liq xatarlar** – xodimlarning noto‘g‘ri harakati, sabotaj, kam savodxonlik.

- **Tashqi muhit xatarlari** – regulyator talablari o‘zgarishi, xalqaro talablar bilan nomuvofiqlik.

Shu sababli, banklar uchun xavflarni faqatgina reaktiv choralar (ya‘ni, xavf sodir bo‘lgandan keyin aralashish) orqali emas, balki **proaktiv yondashuv**, ya‘ni xavflarni oldindan aniqlab, ularning ehtimolini pasaytirish asosida boshqarish dolzarb hisoblanadi.

Shuningdek, muhokamada e‘tibor qaratilishi lozim bo‘lgan muhim jihatlardan biri – bu xalqaro tajribadir. Masalan, rivojlangan davlatlarda banklar sun‘iy intellekt, blokcheyn, real vaqt monitoringi, foydalanuvchi xulqini tahlil qilish kabi texnologiyalar orqali moliyaviy xatarlarni ancha samarali boshqarmoqda. Bu tajribani O‘zbekiston bank amaliyotiga bosqichma-bosqich moslashtirish orqali raqamli xavfsizlikni sezilarli kuchaytirish mumkin.

Natijada, moliyaviy barqarorlik, mijozlar ishonchi, banklararo raqobatbardoshlik va umuman iqtisodiyotda raqamli islohotlarning muvaffaqiyati bank tizimining xatarlarni boshqarish salohiyatiga bevosita bog‘liq bo‘lib qolmoqda.

Xulosa va takliflar: Bank-moliya tizimida raqamli texnologiyalarni joriy etish zamonaviy iqtisodiyotning ajralmas qismiga aylanib bormoqda. Biroq bu jarayon bilan birga, moliyaviy faoliyatda yangi xatarlar, ayniqsa, texnik, kiberxavfsizlik va inson omiliga bog‘liq xavf-xatarlar kuchaymoqda. Tahlillar shuni ko‘rsatmoqdaki,

banklar xatarlarni aniqlash va boshqarish bo'yicha ayrim chora-tadbirlarni amalga oshirayotgan bo'lsada, bu yetarli emas — zamonaviy texnologiyalar bilan uyg'unlashgan, real vaqt rejimida ishlaydigan kompleks tizimlarga ehtiyoj kuchli.

Shu nuqtai nazardan, raqamli texnologiyalar sharoitida moliyaviy xatarlarni boshqarish usullarini takomillashtirish bank tizimining barqarorligi, mijozlar ishonchi va raqamli iqtisodiyotning izchil rivojlanishi uchun zaruriy shart hisoblanadi.

Takliflar

1. ✓ **Xatarlarni proaktiv boshqarish tizimini joriy etish:** Banklar moliyaviy xatarlarni faqat sodir bo'lgandan so'ng emas, balki oldindan aniqlab, tahlil qilishga asoslangan ilg'or monitoring tizimlarini yo'lga qo'yishi lozim.
2. ✓ **Kiberxavfsizlik infratuzilmasini mustahkamlash:** Ilg'or xavfsizlik devorlari (firewall), ikki bosqichli autentifikatsiya, shifrlash tizimlari va xavfsizlik bo'yicha auditlarni muntazam amalga oshirish kerak.
3. ✓ **Sun'iy intellekt va Big Data asosida xavf tahlili tizimlarini ishlab chiqish:** Bank mijozlari xatti-harakatlarini avtomatik o'rganish orqali firibgarlikni oldindan aniqlash va yo'qotishlarni kamaytirish mumkin.
4. ✓ **Xodimlar va mijozlar uchun raqamli savodxonlikni oshirish:** Bank xodimlari va foydalanuvchilarga zamonaviy texnologiyalar va xavfsizlik choralari tushuntirishga qaratilgan o'quv dasturlari tashkil etilishi lozim.
5. ✓ **Texnologik va moliyaviy audit tizimlarini avtomatlashtirish:** Bank tizimlarining ishonchliligini baholovchi mustaqil va avtomatik nazorat mexanizmlari joriy etilishi zarur.
6. ✓ **Xalqaro tajriba va standartlardan foydalanish:** Xatarlarni boshqarish bo'yicha xalqaro reytinglar, ISO/IEC 27001, Basel III kabi me'yoriy hujjatlar asosida ichki siyosatni shakllantirish tavsiya etiladi.
7. ✓ **Regulyator bilan interaktiv hamkorlikni kengaytirish:** Banklar va moliyaviy regulyatorlar o'rtasida raqamli xavfsizlik bo'yicha ochiq axborot almashinuvi va tajriba ulashish tizimi yo'lga qo'yilishi kerak.

Foydalanilgan adabiyotlar

1. Axrorova G'.M. “Raqamli iqtisodiyot sharoitida moliyaviy xavfsizlikni ta'minlash muammolari va ularni hal etish yo'llari” // Iqtisodiyot va innovatsion texnologiyalar. – 2021. – №6. – B. 52–58.
2. Yusupov A.X., Bobojonov F. “Bank ishi va moliya bozorlarida axborot xavfsizligi”. – Toshkent: “Fan va texnologiya”, 2020. – 210 b. – B. 89–115.
3. Basel Committee on Banking Supervision. “Principles for the Sound Management of Operational Risk”. – Bank for International Settlements, 2011. – P. 7–29. <https://www.bis.org/publ/bcbs195.pdf>
4. ISO/IEC 27001:2022. “Information Security Management Systems – Requirements”. – International Organization for Standardization. – Geneva: ISO, 2022. – P. 15–32.
5. OECD (2020). “Digital Disruption in Banking and Its Impact on Financial Stability”. – OECD Working Papers. – P. 3–18. <https://www.oecd.org/finance>
6. Rakhimova M.M. “Bank tizimida raqamli transformatsiya jarayonida risklarni boshqarish mexanizmlari” // Moliyaviy tadqiqotlar jurnali. – 2022. – №4. – B. 27–33.
7. O'zbekiston Respublikasi Markaziy banki hisobotlari (2023). “Bank tizimining raqamli rivojlanishi bo'yicha statistik ma'lumotlar”. – www.cbu.uz
8. Khudoyberganova D.T. “Elektron moliyaviy operatsiyalardagi xavflar va ularni boshqarish” // “Innovatsion iqtisodiyot” jurnali. – 2023. – №2. – B. 40–46.

Research Science and Innovation House