RAQAMLI TRANSFORMATSIYA SHAROITIDA TIJORAT BANKLARINING MIJOZLAR BILAN ISHLASHIDA KIBERXAVFSIZLIKKA ASOSLANGAN YANGI YONDASHUVLAR

Istamova Shahzoda Sherali qizi
Zarmed universiteti, Buxoro kampusi,
Iqtisodiyot yo‘nalishi 3-kurs talabasi
E-mail: istamovashahzodaa@gmail.com
https://doi.org/10.5281/zenodo.23629879

Annotatsiya. Maqolada tijorat banklarining raqamli transformatsiyasi sharoitida mijozlarga xizmat ko‘rsatish modellari va ular bilan bog‘liq kiberxavfsizlik xatarlari tahlil qilinadi. Mobil banking, masofaviy identifikatsiya, sun’iy intellekt va ochiq bank xizmatlarining imkoniyatlari hamda firibgarlik, shaxsiy ma’lumotlar sizib chiqishi va ruxsatsiz tranzaksiyalar xavfi qiyosiy-tahliliy usulda ko‘rib chiqiladi. Banklarda mijoz tajribasi va axborot xavfsizligini uyg‘unlashtirish bo‘yicha amaliy takliflar ishlab chiqiladi.
Kalit so‘zlar: raqamli transformatsiya, tijorat banklari, mijoz tajribasi, kiberxavfsizlik, ko‘p omilli autentifikatsiya, raqamli firibgarlik, open banking.

Аннотация. В статье анализируются модели обслуживания клиентов коммерческих банков в условиях цифровой трансформации и связанные с ними риски кибербезопасности. На основе сравнительного анализа рассматриваются возможности мобильного банкинга, дистанционной идентификации, искусственного интеллекта и открытого банкинга, а также угрозы мошенничества, утечки персональных данных и несанкционированных операций. Предложены практические меры по согласованию качества клиентского обслуживания и информационной безопасности.
Ключевые слова: цифровая трансформация, коммерческие банки, клиентский опыт, кибербезопасность, многофакторная аутентификация, цифровое мошенничество, открытый банкинг.

Kirish. Raqamli transformatsiya tijorat banklari faoliyatida xizmat ko‘rsatish kanallari, ichki biznes jarayonlari va mijoz bilan munosabatlarni tubdan o‘zgartirmoqda. Mobil ilovalar orqali to‘lovlar, omonatlar, kredit arizalari va hisobvaraqlarni boshqarish imkoniyatining kengayishi bank xizmatlarini makon va vaqt jihatidan yanada qulaylashtiradi. Biroq masofaviy xizmat ko‘rsatish ko‘lamining ortishi kiberjinoyatchilar uchun yangi hujum yuzalarini ham shakllantiradi. Shu bois banklar uchun asosiy vazifa xizmatning tezkorligi bilan tranzaksiya ishonchliligini birgalikda ta’minlashdan iborat. O‘zbekistonda raqamlashtirish jarayonlarining strategik asoslari “Raqamli O‘zbekiston — 2030” strategiyasi hamda bank tizimini isloh qilishga oid hujjatlarda belgilangan [1; 2].

Tadqiqot maqsadi va metodologiyasi. Tadqiqotning maqsadi tijorat banklarida mijozlar bilan ishlashning raqamli shakllarini kiberxavfsizlik nuqtayi nazaridan baholash va xizmat sifati hamda xavfsizlikni uyg‘unlashtiruvchi takliflarni shakllantirishdir. Ishda ilmiy

adabiyotlar va normativ hujjatlarni tahlil qilish, qiyoslash, tizimlashtirish va sifat jihatidan xavf-xatarlarni baholash usullari qo‘llanildi. Tadqiqot birlamchi so‘rov yoki banklarning maxfiy operatsion ma’lumotlariga asoslanmagan; natijalar konseptual-tahliliy xarakterga ega. Shu sababli takliflarning miqdoriy samarasi alohida empirik tekshiruvni talab qiladi.

Asosiy natijalar va muhokama. Birinchidan, mobil va internet banking bank-mijoz munosabatlarini doimiy raqamli muloqotga aylantiradi. Mijoz bank filialiga bormasdan xizmat oladi, bank esa raqamli izlar asosida so‘rovlarni tezroq qayta ishlaydi. Shu bilan birga, fishing xabarlari, qalbaki ilovalar va ijtimoiy muhandislik usullari mijoz hisobvaraqlariga noqonuniy kirish ehtimolini kuchaytiradi. Shu sababli autentifikatsiyani faqat parol yoki SMS-kod bilan cheklamasdan, risk darajasiga mos qo‘shimcha tekshiruvlarni joriy etish maqsadga muvofiq [3].

Ikkinchidan, sun’iy intellekt va ma’lumotlar tahlili mijozlarga individual takliflar berish, shubhali tranzaksiyalarni aniqlash va xizmat ko‘rsatishdagi kechikishlarni kamaytirishga xizmat qilishi mumkin. Masalan, odatiy tranzaksiya xulq-atvoridan keskin farq qiluvchi operatsiya qo‘shimcha tekshiruvga yuboriladi. Biroq avtomatlashtirilgan baholashda noto‘g‘ri ijobiy signal, algoritmik tarafkashlik va shaxsiy ma’lumotlardan ortiqcha foydalanish xavfi ham mavjud. Demak, inson nazorati, qarorlarning izohlanishi va ma’lumotlarni minimallashtirish tamoyillari saqlanishi lozim [4].

Uchinchidan, open banking va API integratsiyalari banklar bilan moliyaviy texnologiya kompaniyalari o‘rtasida yangi xizmatlarni rivojlantiradi. Bunday modelda mijoz roziligi, uchinchi tomonning huquqlari, API kalitlari va sessiyalar xavfsizligi alohida ahamiyat kasb etadi. Ruxsatlar aniq chegaralanmagan bo‘lsa, ma’lumotlar nazoratsiz tarqalishi yoki begona tizimlar orqali noqonuniy so‘rovlar yuborilishi mumkin. Xalqaro amaliyotda API xavfsizligi uchun kuchli identifikatsiya, avtorizatsiya va doimiy monitoring muhim deb baholanadi [5].

To‘rtinchidan, bank xizmatlarining inklyuzivligi xavfsizlik siyosatining ajralmas qismi bo‘lishi kerak. Keksalar, raqamli savodxonligi cheklangan shaxslar va internet sifati past hududlar aholisi murakkab tekshiruv bosqichlarida qiyinchilikka duch kelishi mumkin. Shuning uchun xavfsizlikni kuchaytirish mijoz uchun tushunarli interfeys, oddiy ogohlantirishlar va muqobil yordam kanallari bilan birga amalga oshirilishi zarur.

1-jadval. Raqamli bank xizmatlarida imkoniyatlar va xavflar

Texnologiya	Mijoz uchun imkoniyat	Asosiy xavf va himoya
Mobil banking	24/7 operatsiyalar, tezkor to‘lov	Fishing; qurilma bog‘lash va ko‘p omilli autentifikatsiya
Sun’iy intellekt	Shaxsiylashtirish, firibgarlikni aniqlash	Noto‘g‘ri signal; inson nazorati va audit
Masofaviy identifikatsiya	Bankka bormasdan xizmat olish	Shaxsni soxtalashtirish; hujjat va tiriklik tekshiruvi
Open banking / API	Yagona raqamli ekotizim	Ruxsatsiz kirish; rozilik va API avtorizatsiyasi

Manba: muallif tomonidan adabiyotlar tahlili asosida tizimlashtirilgan.

Amaliy takliflar. Tahlil asosida tijorat banklari uchun quyidagi izchil yondashuv taklif etiladi: 1) yuqori riskli operatsiyalarda adaptiv ko‘p omilli autentifikatsiyani qo‘llash; 2) shubhali operatsiyalarni avtomatik aniqlashni inson tomonidan qayta ko‘rib chiqish mexanizmi

bilan to‘ldirish; 3) mijozning shaxsiy ma’lumotlarini yig‘ish va saqlashda minimal zaruriyat tamoyiliga rioya qilish; 4) API hamkorlari uchun ruxsatlar va xavfsizlik auditini joriy etish; 5) mijozlarga firibgarlik sxemalari bo‘yicha qisqa, tushunarli ogohlantirishlar yuborish; 6) xizmat sifatini faqat tezlik bilan emas, balki muvaffaqiyatli tranzaksiyalar, shikoyatlar va xavfsizlik hodisalari bilan birgalikda baholash.

Takliflar natijasini o‘lchash uchun operatsiyani yakunlash vaqti, mijoz murojaatlarini hal qilish muddati, shubhali operatsiyalarning tekshiruv ulushi, noto‘g‘ri bloklangan operatsiyalar va tasdiqlangan firibgarlik holatlari kabi ko‘rsatkichlardan foydalanish mumkin. Ular bankning ichki ma’lumotlari asosida vaqt bo‘yicha solishtirilsa, raqamli innovatsiyalarning real samarasi aniqlanadi.

Xulosa. Raqamli transformatsiya tijorat banklarida mijoz bilan ishlashni tezkor, moslashuvchan va masofaviy shaklga olib chiqmoqda. Shu bilan birga, yangi texnologiyalar xavfsizlikka doir mas’uliyatni kamaytirmaydi, aksincha kuchaytiradi. Tahlil shuni ko‘rsatadiki, mijoz tajribasi, ma’lumotlar maxfiyligi, kuchli autentifikatsiya va firibgarlik monitoringini yagona boshqaruv tizimida uyg‘unlashtirish maqsadga muvofiq. O‘zbekiston banklari uchun texnologik yangilanishlarni raqamli savodxonlik va riskka asoslangan nazorat bilan birga olib borish barqaror raqamli xizmat ko‘rsatishning muhim shartidir.

Foydalanilgan adabiyotlar:

1. O‘zbekiston Respublikasi Prezidentining 2020-yil 5-oktabrdagi PF-6079-son Farmoni. “Raqamli O‘zbekiston — 2030” strategiyasi. https://lex.uz/docs/5030957
2. 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”. https://lex.uz/docs/4811025
3. NIST. Digital Identity Guidelines: Authentication and Lifecycle Management. SP 800-63B. https://pages.nist.gov/800-63-3/sp800-63b.html
4. NIST. AI Risk Management Framework (AI RMF 1.0). 2023. https://doi.org/10.6028/NIST.AI.100-1
5. OWASP. API Security Top 10 — 2023. https://owasp.org/API-Security/editions/2023/en/0x11-t10/