BANK KARTALARI XAVFSIZLIGINI TA'MINLASH TEXNOLOGIYALARI VA XAVFSIZLIK CHORALARI

Ravshanova Tursunoy Ismatullayevna
Samarqand Agrobank Chakana biznes bo'limi bosh menejeri

Annotatsiya

Ushbu tezisda bank kartalari xavfsizligini ta'minlashning zamonaviy texnologiyalari va xavfsizlik choralari yoritilgan. Bank kartalaridan foydalanishning kengayib borishi sharoitida mijozlarning moliyaviy mablag'lari va shaxsiy ma'lumotlarini himoya qilish, noqonuniy tranzaksiyalar hamda kiberfiribgarliklarning oldini olish muhim ahamiyat kasb etmoqda.

Shuningdek, banklar tomonidan qo'llaniladigan tranzaksiyalar monitoringi, firibgarlikni aniqlash tizimlari va mijozlarni xabardor qilish mexanizmlarining o'rni tahlil qilingan.

Kalit so'zlar*: bank kartasi, to'lov tizimi, xavfsizlik, EMV, PIN-kod, OTP, tokenizatsiya, biometrik autentifikatsiya, kiberxavfsizlik, firibgarlik, elektron to'lovlar*

Kirish

Bugungi kunda raqamli iqtisodiyotning jadal rivojlanishi natijasida bank xizmatlaridan foydalanish shakllari ham tubdan o'zgarib bormoqda. Ayniqsa, bank kartalari aholiga va xo'jalik yurituvchi subyektlarga naqd pulsiz to'lovlarni tez, qulay va samarali amalga oshirish imkonini beruvchi muhim to'lov vositasiga aylandi. Bank kartalari orqali savdo va xizmat ko'rsatish shoxobchalarida to'lovlarni amalga oshirish, bankomatlardan naqd pul yechib olish, internet orqali xaridlarni amalga oshirish hamda turli moliyaviy xizmatlardan foydalanish imkoniyati kengaymoqda.

Mavzuning dolzarbligi

Bank kartalari xavfsizligini ta'minlash — bu ham banklar qo'llaydigan zamonaviy texnologiyalar, ham foydalanuvchining shaxsiy ehtiyotkorligiga tayanadigan murakkab tizimdir. Karta orqali amalga oshiriladigan operatsiyalar himoyasi ikki tomonlama tashkil etiladi.

Quyida bank kartalarini firgarlardan himoya qiluvchi asosiy texnologiyalar va siz amal qilishingiz kerak bo'lgan xavfsizlik choralari keltirilgan.

1. Banklar va To'lov Tizimlari Qo'llaydigan Texnologiyalar

Banklar va xalqaro to‘lov tizimlari (bunday tizimlarga Humo, Uzcard, Visa, Mastercard kiradi) pullaringizni himoya qilish uchun quyidagi raqamli echimlardan foydalanadi:

• EMV-chiplar (Chip va PIN): Eskirgan magnit tasmali kartalardan farqli o‘laroq, chipli kartalarni nusxalash (skimming) deyarli imkonsiz. Har bir tranzaksiya uchun chip unikal dinamik kod yaratadi.

• 3D-Secure Texnologiyasi: Internet orqali xarid qilayotganda to‘lovni tasdiqlash uchun telefoningizga keladigan bir martalik SMS-kod (yoki push-bildirishnoma) aynan shu tizim hisoblanadi. Bu firgarlarga karta ma’lumotlarini bilsa ham, pulni ishlatishga yo‘l qo‘ymaydi.

• Tokenizatsiya: Apple Pay, Google Pay yoki Samsung Pay kabi xizmatlarga kartani ulaganingizda, kartaning haqiqiy raqami do‘kon bazasida saqlanmaydi. Uning o‘rniga shifrlangan raqamli identifikator — token ishlatiladi.

• Antifrod Tizimi (Antifraud): Banklarning sun’iy intellektga asoslangan maxsus dasturi bo‘lib, shubhali operatsiyalarni avtomatik tarzda aniqlaydi va bloklaydi. Masalan, 5 daqiqa oldin Toshkentda ishlatilgan karta birdaniga AQSHda ishlatilsa, tizim buni shubhali deb topadi.

2. Foydalanuvchilar Uchun Shaxsiy Xavfsizlik Choralari

Eng mukammal texnologiya ham foydalanuvchining o‘zi karta ma’lumotlarini firgarlarga berib qo‘ysa, yordam bera olmaydi. Shu sababli quyidagi qoidalarga qat'iy amal qiling:

Hech kimga bermaslik kerak bo‘lgan ma’lumotlar:

• Karta PIN-kodi: Uni hech qayerga yozib qo‘ymang (ayniqsa kartaning orqasiga) va bank xodimlariga ham aytmang.

• SMS-kodlar: Telefoningizga keladigan 4 yoki 6 xonali tasdiqlash kodlarini hech qachon va hech kimga (hatto o‘zini bank xodimi yoki xavfsizlik xizmati deb tanishtirgan shaxslarga ham) aytmang. Bank hech qachon kodni so‘ramaydi.

• CVV/CVC kod: Kartaning orqa tarafidagi 3 xonali maxfiy kod.

Kundalik hayotdagi ehtiyotkorlik:

• Onlayn xaridlar uchun alohida karta: Internet-do‘konlarda asosiy (masalan, oylik tushadigan) kartangizni ko‘rsatmaslik uchun virtual karta oching va unga faqat xarid miqdoricha pul o‘tkazib ishlating.

• Shubhali havolalar (Fishing): SMS, Telegram yoki elektron pochta orqali kelgan shubhali havolalarga (yutuqli o‘yinlar, arzon aksiyalar, moddiy yordam va'da qiladigan saytlar) kirmang va u yerga karta ma’lumotlarini kiritmang. Sayt manzilini doim tekshiring (masalan, click.uz o‘rniga clik-uz.com bo‘lsa — bu soxta sayt).

• Bankomatlardan xavfsiz foydalanish: Bankomatga karta soladigan joyda shubhali yopishtirilgan moslamalar (skimerlar) yo‘qligiga e'tibor bering. PIN-kodni kiritayotganda tugmachalarni qo‘lingiz bilan to‘sib turing.

• SMS-xabarnoma va limitlar: Kartangizga SMS-xabarnoma xizmatini yoqing, shunda har bir xarajat haqida darhol xabar topasiz. Shuningdek, bank ilovasida kunlik xarajat yoki internet-to‘lovlar uchun limitlar belgilab qo‘ying.

Xulosa va Taklif

Moliyaviy hisobotlarni xalqaro standartlar asosida yuritishni to‘liq joriy etish:IFRS (xususan IFRS 9, IFRS 7 va IFRS 16) standartlari asosida hisob yuritish bank hisobotlarining ochiqligi va solishtiriluvchanligini ta’minlaydi.

2.Moliyaviy tahlil jarayonlarini avtomatlashtirish:Power BI, Tableau, 1C va boshqa analitik vositalar orqali real vaqt rejimida moliyaviy ko‘rsatkichlarni vizual va interaktiv tahlil qilish tizimini yaratish tavsiya etiladi.

3.Ichki tahlilni boshqaruv qarorlariga integratsiya qilish:Tahlil natijalarini strategik rejalashtirish, byudjetlashtirish va risklarni boshqarish jarayonlariga bevosita ulash orqali tahlilning amaliy qiymatini oshirish lozim.

4.Tahlilchi kadrlar salohiyatini oshirish:Moliyaviy tahlil, prognozlash, stress-test va modellash bo‘yicha xodimlar uchun xalqaro darajadagi treninglar va sertifikatlash (masalan, CFA, ACCA) tashkil etilishi kerak

FOYDALANILGAN ADABIYOTLAR RO‘YXATI

1. O‘zbekiston Respublikasi Markaziy banki. To‘lov tizimlari va to‘lov xizmatlari bo‘yicha me’yoriy-huquqiy hujjatlar. — Toshkent.

2. O‘zbekiston Respublikasi Markaziy banki. Bank kartalari va zamonaviy to‘lov xizmatlariga oid rasmiy materiallar. — Toshkent.

3. O‘zbekiston Respublikasining “To‘lovlar va to‘lov tizimlari to‘g‘risida”gi Qonuni.