BANK XIZMATLARI DIVERSIFIKATSIYASIDA KIBERXAVFSIZLIKNI TA’MINLASH MASALALARI

Ilmiy rahbar: **Azimov Otabek Ma’mirjon o‘g‘li**
ATB “Biznesni rivojlantirish bank” Andijon BXM boshlig‘i,
Sobirjonov Sherdorbek Sherzodbek o‘g‘li
Andijon davat texnika instituti
“Bank ishi va audit” yo‘nalishi 4-kurs talabasi

Raqamli iqtisodiyotning jadal rivojlanishi bank tizimida yangi xizmat turlarining paydo bo‘lishiga olib kelmoqda. Hozirgi kunda tijorat banklari mobil banking, internet banking, QR-to‘lovlar, contactless to‘lovlar, onlayn kreditlash, elektron hamyon va masofaviy identifikatsiya kabi ko‘plab innovatsion xizmatlarni joriy qilmoqda. Bank xizmatlari diversifikatsiyasi mijozlarga qulaylik yaratish, bank daromadlarini oshirish va raqobatbardoshlikni kuchaytirishda muhim omil hisoblanadi. Biroq bank xizmatlarining raqamlashtirilishi bilan bir qatorda kiberxavfsizlik tahdidlari ham ortib bormoqda. Shu sababli bank xizmatlari diversifikatsiyasida kiberxavfsizlikni ta’minlash masalasi zamonaviy bank tizimining eng dolzarb yo‘nalishlaridan biriga aylangan.

Bugungi kunda dunyo miqyosida kiberjinoyatlar bank sektoriga katta iqtisodiy zarar yetkazmoqda. Cybersecurity Ventures tashkiloti prognozlariga ko‘ra [1], 2025-yilda global kiberjinoyatlar oqibatida yetkaziladigan zarar hajmi 10,5 trillion AQSH dollariga yetadi. IBM kompaniyasining 2024-yilgi “Cost of a Data Breach” hisobotida qayd etilishicha, moliyaviy sektorda bitta ma’lumotlar sizib chiqishi bilan bog‘liq o‘rtacha zarar 6 million dollardan oshgan. Ayniqsa, phishing, malware, ransomware va DDoS hujumlari bank tizimi uchun asosiy tahdid sifatida baholanmoqda.

Bank xizmatlari diversifikatsiyasi natijasida banklarning raqamli platformalari soni ortmoqda. Bu esa kiberhujumlar uchun yangi imkoniyatlarni yuzaga keltiradi. Masalan, mobil banking xizmatlari kengaygani sari foydalanuvchilarning login, parol va bank karta ma’lumotlarini o‘g‘irlash holatlari ko‘paymoqda. Kaspersky kompaniyasi ma’lumotlariga ko‘ra [2], 2024-yilda dunyo bo‘yicha mobil bank ilovalariga qilingan kiberhujumlar soni 32 foizga oshgan. Ayniqsa, Android operatsion tizimidagi zararli dasturlar orqali bank ma’lumotlarini qo‘lga kiritish holatlari keng tarqalgan.

AQSH va Yevropa davlatlari tajribasida bank tizimida kiberxavfsizlikni ta’minlash uchun kuchli himoya mexanizmlari joriy etilgan. Masalan, Yevropa Ittifoqida PSD2 (Payment Services Directive 2) direktivasi asosida “Strong Customer Authentication” tizimi qo‘llaniladi. Ushbu tizim foydalanuvchini tasdiqlash uchun kamida ikki bosqichli autentifikatsiyani talab qiladi. Natijada onlayn bank firibgarligi bilan bog‘liq holatlar 40 foizgacha kamaygan. AQSH banklarida esa sun’iy intellekt asosidagi fraud-detection tizimlari keng qo‘llanmoqda. Bu tizimlar foydalanuvchining odatiy moliyaviy harakatlarini tahlil qilib, shubhali operatsiyalarni avtomatik aniqlaydi.

O‘zbekistonda ham bank xizmatlari diversifikatsiyasi jadal sur’atlarda rivojlanmoqda. Markaziy bank ma’lumotlariga ko‘ra [3], 2024-yilda mobil banking foydalanuvchilari soni 42 milliondan oshgan. Elektron to‘lovlar hajmi esa yil davomida 35 foizga o‘sib, 900 trillion so‘mdan ortiqni tashkil etgan. Shu bilan birga, kiberjinoyatlar soni ham ortib bormoqda. O‘zbekiston Ichki ishlar vazirligi ma’lumotlariga ko‘ra, 2024-yilda bank kartalari va elektron to‘lov tizimlari bilan bog‘liq kiberfiribgarlik holatlari 27 mingdan oshgan. Yetkazilgan zarar hajmi esa 340 milliard so‘mga yaqinlashgan. Bank xizmatlari diversifikatsiyasida kiberxavfsizlikni ta’minlashning muhim yo‘nalishlaridan biri zamonaviy autentifikatsiya tizimlarini joriy etish hisoblanadi. Hozirgi kunda ko‘plab banklarda biometrik autentifikatsiya – barmoq izi, Face ID va ovoz orqali identifikatsiya qilish tizimlari joriy qilinmoqda. Tadqiqotlarga ko‘ra, biometrik himoya tizimlari firibgarlik xavfini 60 foizgacha kamaytiradi. Shuningdek, OTP (One Time Password) va token tizimlari ham qo‘shimcha himoya vositasi sifatida muhim ahamiyat kasb etadi.

Kiberxavfsizlikni ta’minlashda sun’iy intellekt texnologiyalarining roli tobora ortib bormoqda. AI asosidagi monitoring tizimlari soniyalar ichida millionlab tranzaksiyalarni tahlil qilib, shubhali operatsiyalarni aniqlash imkonini beradi. Masalan, Mastercard kompaniyasi tomonidan joriy etilgan Decision Intelligence texnologiyasi tranzaksiyalarni real vaqt rejimida tekshiradi va fraud holatlarini 50 foizgacha qisqartirishga xizmat qilmoqda. O‘zbekistonda ham ayrim yirik banklar sun’iy intellekt asosida ishlovchi antifraud tizimlarini joriy etishni boshlagan.

Bank tizimida xodimlarning kiberxavfsizlik bo‘yicha bilimini oshirish ham muhim omillardan biri hisoblanadi. Chunki ko‘plab kiberhujumlar inson omili sababli muvaffaqiyatli amalga oshiriladi. Verizon kompaniyasining 2024-yilgi

hisobotiga ko‘ra [4], kiberxavfsizlik bilan bog‘liq hodisalarning 68 foizi inson xatosi bilan bog‘liq. Shu sababli rivojlangan davlatlarda bank xodimlari muntazam ravishda cyber training dasturlarida ishtirok etadi. O‘zbekistonda ham bank xodimlari va mijozlari uchun kiberxavfsizlik bo‘yicha targ‘ibot va treninglarni kengaytirish zarur. Shuningdek, bank xizmatlari diversifikatsiyasida ma’lumotlarni himoya qilish tizimlarini kuchaytirish talab etiladi. Ma’lumotlarni shifrlash (encryption), firewall, antivirus, SIEM tizimlari va bulutli xavfsizlik texnologiyalari bank infratuzilmasining muhim qismiga aylangan. Gartner kompaniyasi prognozlariga ko‘ra [5], 2026-yilgacha banklarning kiberxavfsizlikka ajratadigan xarajatlari global miqyosda 300 milliard dollardan oshadi. Bu banklar uchun kiberxavfsizlik strategik investitsiya ekanligini ko‘rsatadi.

Bank xizmatlari diversifikatsiyasi sharoitida qonunchilik bazasini takomillashtirish ham muhim ahamiyatga ega. Xorijiy davlatlarda GDPR, PCI DSS va ISO/IEC 27001 kabi xalqaro standartlar keng qo‘llaniladi [6]. O‘zbekistonda ham “Shaxsga doir ma’lumotlar to‘g‘risida”gi qonun hamda Markaziy bankning axborot xavfsizligi bo‘yicha talablarini xalqaro standartlarga moslashtirish zarur. Bu bank tizimining barqarorligini oshirishga xizmat qiladi.

Xulosa qilib aytganda, bank xizmatlari diversifikatsiyasi bank tizimining rivojlanishida muhim omil hisoblanadi. Biroq raqamli xizmatlar hajmining ortishi bilan kiberxavfsizlik tahdidlari ham kuchaymoqda. Shu sababli tijorat banklarida zamonaviy himoya texnologiyalarini joriy etish, sun’iy intellekt asosidagi monitoring tizimlarini rivojlantirish, biometrik autentifikatsiyani kengaytirish hamda xodimlar va mijozlarning kiberxavfsizlik savodxonligini oshirish dolzarb vazifalardan biri bo‘lib qolmoqda. Ana shundagina bank xizmatlari diversifikatsiyasining samaradorligi va xavfsizligini ta’minlash mumkin bo‘ladi.

Foydalanilgan adabiyotlar:

1. Cybersecurity Ventures. Global Cybercrime Report. – New York, 2024.
2. Kaspersky Lab. Financial Cyberthreats Report. – Moskva, 2024.
3. O‘zbekiston Respublikasi Markaziy banki ma’lumotlari. www.cbu.uz

4. Verizon. Data Breach Investigations Report (DBIR). – New York, 2024.
5. Gartner Research. Cybersecurity Spending Forecast. – Stamford, 2024
6. European Union. PSD2 – Payment Services Directive 2. – Brussels, 2023.