RAQAMLI BANK XIZMATLARIDA XAVFSIZLIKNI TA'MINLASH STRATEGIYALARI.

Ruzimuratov Olim
SamISI, PhD, dotsent v.b.
Rayimov Jonibek
Boltaboyev Dilshodbek
SamISI talabalasi

Annotatsiya: *Ushbu maqolada zamonaviy raqamli bank xizmatlarida kiberxavfsizlikni ta’minlashning kompleks strategiyalari tahlil qilinadi. Tadqiqotning asosini O‘zbekiston Respublikasi Markaziy bankining 3669-sonli Nizomi talablari, "Nol ishonch" (Zero Trust) arxitekturasi va sun’iy intellektga asoslangan intellektual monitoring tizimlari tashkil etadi. Maqolada bank infratuzilmasining barqarorligi, API xavfsizligi hamda kiber-tahdidlarga qarshi kurashda inson omilining o‘rni yoritilgan. Tadqiqot natijasida bank tizimini himoya qilishda huquqiy va texnik choralarni uyg‘unlashtirish bo‘yicha amaliy tavsiyalar ishlab chiqilgan.*

Kalit so‘zlar: *Raqamli bank xizmatlari, kiberxavfsizlik, 3669-sonli Nizom, "Nol ishonch" (Zero Trust), sun’iy intellekt, ma’lumotlarni shifrlash, inson omili, API xavfsizligi.*

Аннотация: *В данной статье анализируются комплексные стратегии обеспечения кибербезопасности в современных цифровых банковских услугах. Основу исследования составляют требования Положения №3669 Центрального банка Республики Узбекистан, архитектура «Нулевого доверия» (Zero Trust) и интеллектуальные системы мониторинга на базе искусственного интеллекта. В статье рассматриваются вопросы устойчивости банковской инфраструктуры, безопасности API и роль человеческого фактора в борьбе с киберугрозами. По результатам исследования разработаны практические рекомендации по интеграции правовых и технических мер защиты банковской системы.*

Ключевые слова: *Цифровой банкинг, кибербезопасность, Положение №3669, архитектура «Нулевого доверия», искусственный интеллект, шифрование данных, человеческий фактор, безопасность API.*

Abstract: *This article analyzes comprehensive cybersecurity strategies in modern digital banking services. The research is based on the requirements of Regulation No. 3669 of the Central Bank of the Republic of Uzbekistan, Zero Trust architecture, and AI-powered intelligent monitoring systems. The paper explores banking infrastructure resilience, API security, and the significance of the human factor in countering cyber threats. Based on the study findings, practical recommendations have been developed for harmonizing legal and technical measures to protect the banking system.*

Keywords: *Digital banking services, cybersecurity, Regulation No. 3669, Zero Trust architecture, artificial intelligence, data encryption, human factor, API security.*

KIRISH

So‘nggi yillarda raqamli iqtisodiyotning jadal sur’atlar bilan rivojlanishi moliya-bank tizimini tubdan transformatsiya qilib, mijozlarga bank xizmatlaridan tezkor va qulay foydalanish imkoniyatini yaratdi. Biroq, ushbu transformatsiya jarayonlari kiberhujumlar, ma’lumotlar o‘g‘irlanishi va moliyaviy firibgarliklar kabi jiddiy virtual tahdidlarni ham keltirib chiqardi.

An’anaviy perimetrli xavfsizlik modellari bugungi kunda o‘z samaradorligini yo‘qotgan bo‘lib, moliya institutlaridan "hech qachon ishonma, doim tekshir" tamoyiliga asoslangan "Nol ishonch" (Zero Trust) arxitekturasiga o‘tishni talab etmoqda. O‘zbekiston Respublikasi Markaziy banki tomonidan qabul qilingan 3669-sonli Nizom kabi me’yoriy hujjatlar tijorat banklari uchun axborot xavfsizligi va kiberxavfsizlikka doir qat’iy minimal talablarni belgilab berdi.

Raqamli bank xizmatlarida xavfsizlikni ta’minlash nafaqat texnik masala, balki bank tizimining barqarorligi va mijozlarning ishonchini saqlab qolishning fundamental kafolatidir. Mazkur maqola raqamli bank muhitida kiberxavfsizlikni ta’minlashning huquqiy, texnik va tashkiliy strategiyalarini kompleks tahlil qilishga bag‘ishlangan.

O‘zbekiston Respublikasida raqamli banklar xavfsizligini ta’minlashning huquqiy asosi Markaziy bank boshqaruvining 2025-yil 18-avgustdagi 3669-sonli Nizomi bilan belgilangan bo‘lib, u tijorat banklari, shu jumladan mikromoliya banklari uchun axborot xavfsizligi va kiberxavfsizlikka doir minimal talablarni o‘rnatadi. Ushbu kompleks yondashuvga ko‘ra, har bir bankda bevosita bank boshqaruvi raisiga bo‘ysunadigan Axborot xavfsizligi va kiberxavfsizlikni ta’minlash xizmati tashkil etilishi shart.

Bank xodimlarini asosiy faoliyati bilan bog‘liq bo‘lmagan ishlarga jalb etish taqiqlanadi va Xizmat xodimlari yiliga kamida ikki marta maxsus kurslarda malaka oshirishlari lozim. Huquqiy nuqtai nazardan, banklarga o‘zlarining AKT infratuzilmalari hamda xavfsizlik tizimlarini boshqarish va uzluksiz ishlashini ta’minlash vazifalarini autsorsingga berish qat’iyan man etiladi. Bankning ichki siyosati barcha axborot tizimlari va resurslaridagi xavfsizlik talablarini belgilashi va har bir xodimga majburiy tartibda tanishtirilishi kerak. Texnik tomondan, barcha dasturiy-texnik vositalar litsenziyalangan va sertifikatlangan bo‘lishi, shuningdek, ishlab chiqaruvchi tomonidan texnik qo‘llab-quvvatlanishi shart.

Axborot tizimlariga kirishni boshqarishda foydalanuvchilarning hisob yozuvlarini avtomatik yaratish va ularning lavozim majburiyatlaridan kelib chiqib rollarga asoslangan model (RBAC) qo‘llaniladi. Masofadan ulanish faqat O‘zbekiston hududida, himoyalangan VPN kanallari va ko‘p faktorli autentifikatsiya orqali amalga oshiriladi. Ma’muriy imtiyozlarga ega foydalanuvchilar (administratorlar) harakatlari majburiy tartibda PAM (Privileged Access Management) tizimi orqali nazorat qilinadi va bu yozuvlar kamida olti oy saqlanadi. Ma’lumotlar bazasini boshqarishda DAM (Database Activity Monitoring) tizimi joriy etilishi, administrator parollari esa kamida 12 ta belgidan iborat bo‘lishi va shifrlangan holda saqlanishi kerak.

Tarmoq xavfsizligi O‘z DSt ISO/IEC 27033 seriyasidagi standartlar asosida loyihalanadi va tarmoqlar VLAN yordamida segmentlarga ajratiladi.

Bankning tashqi ulanish nuqtalari kamida ikkinchi toifadagi tarmoqlararo ekranlar, IDS/IPS, WAF (Web Application Firewall) va Anti-DDoS tizimlari bilan himoyalangan bo‘lishi lozim. Axborot xavfsizligi holatini tun-u kun (24/7) nazorat qilish uchun SIEM va SOAR tizimlari joriy etiladi hamda ular Markaziy bankning “CERT-CBU” markaziga bog‘lanadi. Oxirgi nuqtalarda (Endpoint) xavfsizlikni ta’minlash uchun EDR texnologiyasi, konfiguratsiya yaxlitligini nazorat qilish uchun esa FIM (File Integrity Monitoring) tizimi qo‘llaniladi. Ma’lumotlarning ruxsatsiz chiqib ketishini oldini olish maqsadida barcha oxirgi nuqtalar DLP (Data Loss Prevention) tizimiga ulanishi shart. Elektron to‘lov hujjatlari va tranzaksiyalar bankning o‘z ERI kalitlarini ro‘yxatga olish markazi tomonidan berilgan sertifikatlar bilan tasdiqlanishi va SSL/TLS protokollari orqali shifrlanishi kerak.

Bank ma’lumotlarni qayta ishlash markazlari (DPC) Tier III yoki Tier IV xalqaro standartlariga javob berishi, avtonom elektr ta’minoti va videoarxivning kamida 2 oy saqlanishi ta’minlanishi lozim. Zaifliklarni boshqarishda xalqaro CVE va CVSS tizimlaridan foydalaniladi hamda muntazam ravishda skanerlash va pentesting o‘tkaziladi. Bankning axborot aktivlari va zaxira nusxalari favqulodda holatlardan himoyalanish uchun asosiy markazdan kamida 50 km masofada joylashgan zaxira markazida dublyaj qilinishi shart. Ichki audit xizmati har oyda kamida bir marta ma’lumotlarni qayta tiklash tizimi va elektron arxiv ishini tekshirib borishi zarur.

Bankning dasturiy ta’minotini ishlab chiqishda SAST/DAST tahlil usullari qo‘llaniladi va on-premise (lokal) platformalardan foydalanishga ruxsat beriladi. Xavfsizlikni ta’minlashning huquqiy va texnik choralari buzilgan taqdirda, aybdor shaxslar qonunchilikka muvofiq javobgar bo‘ladilar.

"Nol ishonch" (Zero Trust) arxitekturasi raqamli bank xavfsizligida an'anaviy perimetrli himoyadan (tarmoq ichidagi hamma narsa xavfsiz degan tushunchadan) voz kechishni anglatadi va "hech qachon ishonma, doim tekshir" tamoyiliga tayanadi. Ushbu strategiya foydalanuvchining joylashgan joyidan (tarmoq ichida yoki tashqarisida) qat'i nazar, har bir kirish so'rovini, qurilmani va tranzaksiyani doimiy ravishda validatsiyadan o'tkazishni talab qiladi.

Zero Trust va innovatsion texnologiyalar strategiyasining asosiy tarkibiy qismlari quyidagilardan iborat:

- Identifikatsiyani va kirishni boshqarish (IAM): Bu tizim Zero Trust'ning tamal toshi bo'lib, nafaqat tizimga kirishda, balki butun sessiya davomida foydalanuvchi shaxsini uning xatti-harakatlari va biometrik ma'lumotlari asosida uzluksiz autentifikatsiya qilishni ta'minlaydi.
- Tarmoq mikro-segmentatsiyasi: Tarmoqni granular darajadagi kichik zonalarga bo'lish orqali tajovuzkorlarning tarmoq ichida "lateral" (yondan-yonga) harakatlanishini cheklaydi. Har bir ilova va ish yuklamasi o'zining xavfsiz chegarasiga ega bo'ladi.

• Sun'iy intellekt (AI) va Mashina o'rganish (ML): Kiberhujumlarni real vaqt rejimida aniqlash va anomaliyalarni tahlil qilishda ushbu texnologiyalar hal qiluvchi rol o'ynaydi. AI algoritmlari foydalanuvchi xulq-atvori, qurilma holati va atrof-muhit omillarini tahlil qilib, "ishonch ballari"ni (trust scores) hisoblab chiqadi va shu asosda dinamik ravishda kirishga ruxsat beradi yoki uni cheklaydi.

• Ko'p faktorli autentifikatsiya (MFA) evolyutsiyasi: 2026-yil tendensiyalariga ko'ra, banklarda parolsiz autentifikatsiya (passwordless) va biometrik himoya (barmoq izi, yuz tanish) keng joriy etilmoqda. Bu fishing hujumlari va parol o'g'irlanishi bilan bog'liq xatarlarni sezilarli darajada kamaytiradi.

• Qurilmalar (Endpoint) xavfsizligi: Tarmoqqa ulanayotgan har bir mobil qurilma yoki serverning xavfsizlik holati (patchlar mavjudligi, antivirus holati) ulanishdan oldin "device attestation" jarayoni orqali tasdiqlanishi shart.

• API xavfsizligi va integratsiya: Ochiq banking (Open Banking) sharoitida uchinchi tomon ilovalari bilan ma'lumot almashinuvi xavfsiz API Gateway'lar va murakkab avtorizatsiya protokollari orqali himoyalanadi.

• Avtomatlashtirilgan monitoring (SIEM va SOAR): O'zbekiston bank qonunchiligi (3669-sonli Nizom) talablariga ko'ra, kiberhodisalarni 24/7 rejimida monitoring qilish uchun SIEM tizimlari va ularga avtomatik javob qaytarish uchun SOAR tizimlari joriy etilishi strategiyaning muhim qismidir.

Zero Trust strategiyasini muvaffaqiyatli amalga oshirish uchun banklar bosqichma-bosqich yondashuvni qo'llashlari lozim: dastlab barcha aktivlar inventarizatsiya qilinadi, ma'lumotlar tasniflanadi, so'ngra mikro-segmentatsiya va AI asosidagi ishonch algoritmlari texnik bosqichda joriy etiladi, yakunida esa xodimlarning kiber-savodxonligi oshirilib, tizim operatsion jarayonlarga integratsiya qilinadi.

Bank infratuzilmasining operatsion barqarorligini ta'minlash strategiyasi eng avvalo ma'lumotlarni qayta ishlash markazlari (DPC) va server xonalariga qo'yiladigan qat'iy texnik talablarga tayanadi. Bank infratuzilmasi ob'ektlari xalqaro Tier III yoki Tier IV standartlariga muvofiq bo'lishi, shuningdek, ISO 27001, PCI DSS yoki SOC 2 kabi xavfsizlik sertifikatlariga ega bo'lishi shart. Elektr ta'minoti tizimi barqarorligini ta'minlash uchun turli podstansiyalardan ikkita mustaqil kirish liniyasi, avtomatik ishga tushuvchi dizel elektr stansiyasi (kamida bir sutkalik yoqilg'i zaxirasi bilan) va uzluksiz quvvat manbalari (UPS) o'rnatiladi.

Server xonalarida iqlim sharoitini saqlash uchun 100 foiz zaxiralangan sovitish tizimlari qo'llaniladi, bunda harorat 18–24°C va namlik 40–50 foiz atrofida bo'lishi nazorat qilinadi. Fizik xavfsizlik choralari sifatida mustahkam to'siqlar, kodli qulflar va uzluksiz videokuzatuv tizimi joriy etiladi, bunda videoarxiv kamida 2 oy davomida saqlanishi va elektr uzilgan taqdirda tizim kamida 12 soat avtonom ishlashi lozim.

Infratuzilmaning operatsion barqarorligi axborot aktivlarining ish jarayonlari uzluksizligini (Business Continuity) va ularni favqulodda vaziyatlarda qayta tiklashni (Disaster Recovery) nazarda tutadi. Favqulodda holatlardan (yong'in, zilzila va h.k.)

himoyalanish uchun bankning zaxira ma'lumotlar markazi asosiy markazdan kamida 50 km masofada joylashishi va ma'lumotlar nusxalari kuniga kamida bir marta sinxronizatsiya qilinishi shart. Banklar tizimni qayta tiklash sinov ishlarini yilda kamida ikki marotaba o'tkazishi va ichki audit xizmati har oyda kamida bir marta ushbu tizim holatini tekshirib borishi zarur.

Oxirgi nuqtalar (Endpoint) xavfsizligini ta'minlashda anomal faoliyatni kuzatuvchi EDR (Endpoint Detection and Response) va ruxsatsiz o'zgarishlardan ogohlantiruvchi FIM (File Integrity Monitoring) texnologiyalaridan foydalaniladi. Ma'lumotlarning ruxsatsiz chiqib ketishini oldini olish uchun barcha oxirgi nuqtalar va mobil qurilmalar markazlashgan holda DLP (Data Loss Prevention) tizimiga ulanadi.

Bank tarmog'i ichida barqarorlikni ta'minlash uchun VLAN yordamida segmentatsiya qilinadi va barcha telekommunikatsiya shkaflari videokuzatuv ostida qulflangan holda saqlanadi. Infratuzilma strategiyasi, shuningdek, ma'lumotlar bazasini (DAM) va tarmoqdagi tahdidlarni (NDR/IDS/IPS) real vaqt rejimida monitoring qilish orqali tizim buzilishlarining oldini olishni o'z ichiga oladi.

Bank xizmatlarining doimiy mavjudligi (availability) uchun redundans (zaxiralash) va replikatsiya usullari qo'llanilib, har qanday texnik nosozlik vaqtida avtomatik chora ko'rish mexanizmlari ishga tushishi ta'minlanadi.

Raqamli transformatsiya jarayonida inson omili kiberxavfsizlikning eng muhim zaifligi hisoblanib, ichki xodimlar tomonidan sodir etiladigan xatolar, moliyaviy firibgarliklar va phishing hujumlari banklar uchun hamon jiddiy tahdid tug'dirib kelmoqda.

Shuning uchun banklar raqamli texnologiyalar bilan shug‘ullanayotgan xodimlar uchun muntazam malaka oshirish dasturlari va kiber-treninglarni tashkil etishlari, bunda BS/2 kabi xalqaro texnologik kompaniyalar bilan hamkorlikda ta'lim modullarini yo'lga qo'yishlari zarur.

O‘zbekiston Respublikasi Markaziy bankining 3669-sonli Nizomi talablariga ko'ra, har bir bankda bevosita bank boshqaruvi raisiga bo‘ysunadigan Axborot xavfsizligi va kiberxavfsizlikni ta’minlash xizmati tashkil etilishi shart.

Ushbu Xizmat xodimlarini ularning asosiy faoliyati bilan bog‘liq bo‘lmagan ishlarga jalb etish qat'iyan taqiqlanadi hamda ular yiliga kamida ikki marta ixtisoslashtirilgan o‘quv kurslarida malaka oshirishlari lozim.

Bankning axborot xavfsizligiga oid ichki siyosati barcha axborot tizimlari va resurslaridagi xavfsizlik talablarini belgilashi hamda har bir xodimga majburiy tartibda tanishtirilishi shart. Konfidensial ma'lumotlarning, shu jumladan bank siri va shaxsga doir ma'lumotlarning oshkor etilishini oldini olish maqsadida har bir xodim bilan sir saqlash bo‘yicha majburiyatnoma (NDA) imzolanishi va ruxsati bo‘lmagan xodimlarning ushbu ma'lumotlardan foydalanmasligi ta'minlanishi kerak. Axborot tizimlari va resurslariga kirishni boshqarishda xodimlarning funksional vazifalaridan kelib chiqib rollarga asoslangan kirish modeli (RBAC) qo‘llaniladi va Xizmat xodimlarning lavozim majburiyatlari hamda vakolatlarini bir oyda kamida bir marotaba tekshirib, natijalarni hujjatlashtirishi lozim. Bankning AKT infratuzilmasi va axborot tizimlari administratorlarining barcha harakatlari majburiy tartibda PAM (Privileged Access Management) tizimi orqali amalga oshirilishi va ushbu imtiyozli sessiya yozuvlari kamida olti oy davomida xavfsiz saqlanishi shart.

Ochiq banking (Open Banking) ekotizimida raqamli bank xavfsizligini ta’minlashning fundamental huquqiy va texnik asosi bank ma’lumotlar bazasiga tashqi tashkilotlarni to‘g‘ridan-to‘g‘ri (DB Link) ulashni qat’iyan taqiqlash hamda faqat himoyalangan veb-servislar (API) orqali aloqa o‘rnatish hisoblanadi.

Markaziy bankning 3669-sonli Nizomiga ko‘ra, bank tashqi axborot tizimlari bilan almashinuvni boshlashdan oldin Markaziy bankni xabardor qilishi va almashinuvni shartnoma asosida, ma’lumotlar ro‘yxati, shakli va kirishni chegaralash choralarini belgilagan holda amalga oshirishi shart. Strategik nuqtai nazardan, uchinchi shaxslarga (fintex-kompaniyalar, hamkorlar) ma’lumotlardan foydalanish huquqi berilishidan oldin majburiy tartibda xavf darajasi baholanadi va maxfiylikni saqlash bo‘yicha NDA (Non-Disclosure Agreement) kelishuvlari imzolanadi.

API xavfsizligini tashkil etishda uchinchi shaxslarning har bir xodimi uchun alohida foydalanuvchi akkaunti yaratilishi va ular majburiy ko‘p faktorli autentifikatsiyadan (MFA) o‘tkazilishi lozim. Texnik arxitekturada API Gateway’lar markaziy nazorat nuqtasi vazifasini bajarib, trafikni monitoring qilish, autentifikatsiya va avtorizatsiya mexanizmlarini boshqarish hamda xavfsizlik siyosatlarini ijro etish uchun mas’uldir.

Mikroservislar aloqasida xavfsizlikni ta’minlash uchun "Service Mesh" texnologiyasi qo‘llaniladi, bu esa tarqatilgan ilovalar bo‘ylab izchil siyosatni yuritish imkonini beradi. API orqali uzatiladigan barcha ma’lumotlar SSL/TLS (xususan TLS 1.3) kabi yuqori darajadagi protokollar yordamida shifrlanishi shart, bu esa ma’lumotlarning tranzit vaqtida butligini va konfidensialligini kafolatlaydi. Tashqi

axborot tizimlari bilan ulanish nuqtalari bankning ichki tarmog‘idan alohida segmentda joylashtirilib, IDS/IPS, WAF (Web Application Firewall) va Anti-DDoS tizimlari bilan ko‘p pog‘onali himoya qilinishi kerak. "Nol ishonch" (Zero Trust) modeliga ko‘ra, har bir API so‘rovi AI (sun’iy intellekt) asosidagi ishonch algoritmlari yordamida baholanib, real vaqt rejimida foydalanuvchi xulq-atvori va qurilma holatiga ko‘ra "trust score" (ishonch ballari) hisoblab chiqiladi.

API xavfsizligi doirasida bank tranzaksiyalarini tasdiqlashda elektron raqamli imzo (ERI) va shifrlash kalitlaridan foydalanish majburiy bo‘lib, bu tranzaksiyalarning haqiqiyligini va rad etib bo‘lmasligini ta’minlaydi. Bankning API resurslari muntazam ravishda zaifliklarni aniqlash uchun skanerlanishi, SAST/DAST tahlilidan o‘tkazilishi va yilda kamida bir marta pentesting (buzib kirishga urinish testlari) o‘tkazilishi shart.

API tranzaksiyalari va foydalanuvchi harakatlari SIEM va SOAR tizimlari orqali 24/7 rejimida monitoring qilinadi, shubhali anomaliyalar aniqlanganda tizim avtomatik ravishda bloklash yoki ogohlantirish choralarini ko‘radi. Hamkorlik aloqalari tugatilgandan so‘ng, uchinchi shaxslarga berilgan barcha kirish huquqlari va akkauntlar zudlik bilan bekor qilinishi hamda ulardagi bankka tegishli ma’lumotlar qaytarilishi yoki yo‘q qilinishi huquqiy majburiyat hisoblanadi.

Takliflar

Raqamli bank xizmatlarida kiberxavfsizlikni ta’minlash va mijozlar ishonchini mustahkamlash maqsadida quyidagi strategik choralar tavsiya etiladi:

- Xalqaro standartlar va arxitekturani joriy etish: Banklarda axborot xavfsizligini boshqarish uchun ISO/IEC 27001 standartlarini tatbiq etish hamda an’anaviy perimetrli himoyadan "Nol ishonch" (Zero Trust) modeliga o‘tish zarur.
- Intellektual monitoring tizimlari: Kibertahdidlarni real vaqt rejimida aniqlash va ularga avtomatik javob qaytarish uchun SIEM, SOAR va EDR tizimlarini joriy qilish, shuningdek, anomaliyalarni tahlil qilishda sun’iy intellekt (AI) algoritmlaridan foydalanish lozim.

- Inson kapitalini rivojlantirish: Inson omili bilan bog‘liq zaifliklarni bartaraf etish uchun bank xodimlari uchun yiliga kamida ikki marta professional treninglar tashkil etish va mijozlarning kiber-savodxonligini oshirish bo‘yicha ommaviy kompaniyalarni yo‘lga qo‘yish shart.
- Audit va nazoratni kuchaytirish: Har bir moliya muassasasida kiberxavfsizlikka oid ichki audit tizimini mustahkamlash hamda ma’lumotlar bazasi faoliyatini uzluksiz monitoring qiluvchi DAM tizimini joriy etish tavsiya etiladi.

Xulosa

Raqamli bank xizmatlarining kengayishi moliya sohasida inqilobiy qulayliklar yaratish bilan birga, bank tizimining barqarorligiga putur yetkazishi mumkin bo‘lgan murakkab kiber-tahdidlarni ham yuzaga keltirmoqda. Tadqiqot natijalari shuni ko‘rsatadiki, samarali kiber-himoyaga erishish uchun faqat texnik yechimlar yetarli emas; u huquqiy bazani takomillashtirish, tashkiliy choralarni kuchaytirish va zamonaviy texnologiyalarni integratsiyalashni talab qiluvchi kompleks yondashuvdir. Kiberxavfsizlik strategiyalarining muvaffaqiyatli amalga oshirilishi raqamli xizmatlar samaradorligini oshirish va raqamli iqtisodiyot sharoitida mijozlar ishonchini saqlashning fundamental kafolati bo‘lib xizmat qiladi. O‘zbekiston bank tizimi uchun xalqaro tajriba va milliy qonunchilik talablariga (masalan, 3669-sonli Nizom) asoslangan proaktiv himoya tizimini yaratish raqamli transformatsiyani xavfsiz davom ettirishning yagona yo‘lidir.

FOYDALANILGAN ADABIYOTLAR RO‘YXATI:

1. O‘zbekiston Respublikasi Markaziy banki. (2025). O‘zbekiston Respublikasi tijorat banklarining axborot xavfsizligi va kiberxavfsizligiga doir minimal talablar to‘g‘risidagi NIZOM (3669-sonli ro‘yxat raqami).

2. Xidirov, U. G. (2025). Banklarning kiberxavfsizligi: Raqamli moliya dunyosida xavf va imkoniyatlar. Yangi O'zbekiston, Yangi Tadqiqotlar Jurnali, Vol. 2, No. 9.

3. ISO/IEC 27001:2013. Information technology — Security techniques — Information security management systems — Requirements. BSI Implementation Guide.

4. Ramakrishna, R. G. (2025). Implementing zero trust architecture in financial institutions. World Journal of Advanced Engineering Technology and Sciences, 15(01), 2125-2133.

5. GetAstra. (2026). Open banking API Security: The Complete Guide in 2026.

6. Abduraxmonov, A. S. (2025). Raqamli banklar xavfsizligi va texnik talablari: Zamonaviy yondashuvlar va amaliy tavsiyalar. Journal of marketing, business and management.

7. Abduraxmonov, A. S. (2025). Raqamli banklar xavfsizligini ta'minlash va ularning texnik talablari. Samarqand iqtisodiyot va servis instituti.

8. Scalefusion Blog. (2026). Рекомендации по многофакторной аутентификации (МФА) в 2026 году.

9. Sultonov, Sh. N., & Xurramova, F. P. (2024). Raqamli iqtisodiyot sharoitida bank xavfsizligi va kiberxavfsizlik muammolari. “O‘zbekiston – 2030 strategiyasi: amalga oshirilayotgan islohotlar tahlili, muammolar va yechimlar” ilmiy to‘plami, Nordic International University.