MOLIYAVIY TEXNOLOGIYALAR

№4

ILMIY ELEKTRON JURNALI

ISSN: 2181-3965
VOLUME 5
TOSHKENT 2026

O’zbekiston Respublikasi OAK Rayosatining 2023-yil 3-iyundagi 364-son qarori bilan “Moliyaviy texnologiyalar” ilmiy elektron jurnali iqtisodiyot fanlari bo’yicha falsafa doktori (PhD) va fan doktori (DSc) ilmiy darajasiga talabgorlarning dissertatsiyalari yuzasidan assosiy ilmiy natijalarini chop etish tavsiya etilgan ilmiy nashrlar ro’yxatiga kiritilgan.

“**Moliyaviy texnologiyalar**” ilmiy elektron jurnali 23.11.2022-yildan O‘zbekiston Respublikasi Prezidenti Administratsiyasi huzuridagi Axborot va ommaviy kommunikatsiyalar agentligi tomonidan **№R-566966** reyestr raqami tartibi bo‘yicha ro‘yxatdan o‘tkazilgan. Litsenziya raqami: **№049864**

ISSN: 2181-3965
VOLUME 5

MUNDARIJA

ISSN: 2181-3965
VOLUME 5

ISSN: 2181-3965
VOLUME 5

RAQAMLI TO‘LOV INFRATUZILMASIDA MOLIYAVIY XATARLARNI BOSHQARISH VA AXBOROT XAVFSIZLIGINI TA’MINLASH MEXANIZMLARI

Vaxabov Bobur Alisherovich
mustaqil tadqiqotchi
Toshkent Kimyo xalqaro universiteti
E-mail: boburvaxabov@gmail.com

Annotatsiya. *Raqamli to‘lov infratuzilmasining tez kengayishi to‘lovlarni tez, arzon va qulay amalga oshirish imkoniyatlarini oshirayotgan bo‘lsa-da, ayni vaqtda moliyaviy xatarlarning texnologik va institutsional tabiatini murakkablashtirmoqda. Mazkur maqolada raqamli to‘lov ekotizimida kredit, likvidlik, operatsion, firibgarlik, kiberxavfsizlik, ma’lumotlar yaxlitligi va uchinchi tomon texnologik qaramligi bilan bog‘liq xatarlarni kompleks boshqarish mexanizmlari tadqiq etiladi. Tadqiqotning metodik asosini institutsional tahlil, risk-matritsa, indikatorli baholash, qiyosiy tahlil va ssenariy modellashtirish tashkil etadi. O‘zbekiston Respublikasi Markaziy bankining 2024–2025-yillardagi rasmiy hisobotlari hamda to‘lov infratuzilmasi bo‘yicha ma’lumotlari xalqaro prinsiplar bilan taqqoslanib, amaldagi nazorat arxitekturasining kuchli va zaif jihatlari aniqlanadi. 2025-yilda to‘lov infratuzilmasi hajmining sezilarli kengayishi bilan bir qatorda Markaziy bank kiberxavfsizlik va anti-frod yo‘nalishlarida yangi nazorat vositalari, xavfsiz ulanishlar va kiberxavfsizlik reyting tizimini joriy qilgan. Tadqiqot natijasida “aniqlash–baholash–oldini olish–aniqlash–javob–tiklash–qayta baholash” sikliga asoslangan integratsiyalashgan model taklif etildi. Modelda riskka proporsional nazorat, real vaqt monitoringi, xavfsiz API, mustaqil testlar, incident reporting, biznes uzluksizligi va iste’molchi zararini tezkor qoplash mexanizmlari bir butun boshqaruv konturiga birlashtiriladi.*

Kalit so‘zlar: *raqamli to‘lovlar, moliyaviy xatar, kiberxavfsizlik, axborot xavfsizligi, firibgarlik, operatsion barqarorlik, risk-menejment, to‘lov infratuzilmasi, anti-frod, moliyaviy texnologiyalar.*

МЕХАНИЗМЫ УПРАВЛЕНИЯ ФИНАНСОВЫМИ РИСКАМИ И ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ЦИФРОВОЙ ПЛАТЕЖНОЙ ИНФРАСТРУКТУРЕ

Вахабов Бобур Алишерович
независимый исследователь
Ташкентский международный химический университет
E-mail: boburvaxabov@gmail.com

Аннотация. *Быстрое расширение цифровой платежной инфраструктуры повышает скорость, доступность и удобство расчетов, но одновременно усложняет структуру финансовых и технологических рисков. В статье рассматриваются механизмы комплексного управления кредитным, ликвидным, операционным, мошенническим, кибернетическим риском, риском нарушения целостности данных и зависимостью от третьих технологических провайдеров. Методологическая основа включает институциональный анализ, матрицу рисков, индикаторную оценку, сравнительный анализ и сценарное моделирование. На основе официальных материалов Центрального банка Республики Узбекистан за 2024–2025 годы проведено сопоставление национальной практики с международными принципами безопасности платежных систем и операционной устойчивости. В результате предложена интегрированная модель, построенная по циклу «идентификация–оценка–предотвращение–обнаружение–реагирование–восстановление–переоценка». Она объединяет риск-ориентированный надзор, мониторинг вблизи реального времени, защищенные API, независимое*

тестирование, отчетность по инцидентам, непрерывность бизнеса и механизмы оперативного возмещения потерь клиентов.

Ключевые слова: *цифровые платежи, финансовый риск, кибербезопасность, информационная безопасность, мошенничество, операционная устойчивость, управление рисками, платежная инфраструктура, антифрод, финтех.*

MECHANISMS FOR MANAGEMENT OF FINANCIAL RISKS AND ENSURING INFORMATION SECURITY IN DIGITAL PAYMENT INFRASTRUCTURE

Vakhabov Bobur Alisherovich

Independent Researcher
Tashkent International University of Chemistry
E-mail: boburvaxabov@gmail.com

Abstract. *The rapid expansion of digital payment infrastructure improves the speed, affordability and accessibility of transactions, while simultaneously increasing the complexity of financial and technology-related risks. This article examines an integrated risk-management framework for credit, liquidity, operational, fraud, cybersecurity, data-integrity and third-party technology risks in the digital payment ecosystem. The methodology combines institutional analysis, risk matrices, indicator-based assessment, comparative analysis and scenario modelling. Official data and reports of the Central Bank of Uzbekistan for 2024–2025 are assessed against international principles of payment-system security and operational resilience. The study finds that the national ecosystem has strengthened its cybersecurity and anti-fraud capacity through enhanced controls, secure interconnections and cyber-risk assessment tools, but the growing scale of digital transactions requires a more integrated risk architecture. A seven-stage model — identify, assess, prevent, detect, respond, recover and reassess — is proposed. The model integrates proportional supervision, near-real-time monitoring, secure APIs, independent testing, incident reporting, business continuity and rapid consumer-loss remediation into a single governance cycle.*

Keywords: *digital payments, financial risk, cybersecurity, information security, fraud, operational resilience, risk management, payment infrastructure, anti-fraud, financial technology.*

Kirish

Raqamli to‘lovlar bugungi iqtisodiyotda nafaqat hisob-kitob qilish vositasi, balki banklar, to‘lov tashkilotlari, savdo platformalari, telekommunikatsiya operatorlari va davlat xizmatlarini yagona raqamli oqimga bog‘laydigan infratuzilmaga aylanmoqda. To‘lovning bir necha soniyada bajarilishi foydalanuvchi uchun qulaylikni oshiradi, biroq infratuzilmaning murakkablashishi bilan bir operatsiyadagi nosozlik, firibgarlik yoki kiberhujumning tarqalish kanallari ham ko‘payadi. Shu sababli raqamli to‘lovlar xavfsizligini faqat texnik vositalar yoki faqat prudensial nazorat orqali ta’minlash yetarli emas; xatarlarni boshqarish moliyaviy va axborot xavfsizligini birlashtirgan institutsional tizimga aylanishi zarur.

O‘zbekistonda raqamli to‘lov infratuzilmasining miqyosi so‘nggi yillarda keskin oshdi. Markaziy bank ma’lumotlariga ko‘ra, 2025-yil yakunida muomaladagi bank kartalari soni 68,3 mln donaga, o‘rnatilgan POS-terminallar 430,8 ming taga, bankomatlar va o‘z-o‘ziga xizmat ko‘rsatish qurilmalari 40,1 ming taga yetgan; yil davomida POS terminallari orqali 460,3 trln so‘mlik operatsiyalar amalga oshirilgan. Bu ko‘rsatkichlar to‘lov xizmatlari uchun yangi iqtisodiy imkoniyatlar bilan birga tizimli risklarning miqyosini ham oshiradi [1].

2025-yil Markaziy bankning yillik hisobotida kiberxavfsizlik va axborot himoyasiga oid bir qator amaliy choralar qayd etilgan: to‘lov tizimlari va banklar uchun tegishli talablar kuchaytirildi, 134 ta tashqi aloqa xavfsiz kanallar orqali himoyalandi, kiberxavfsizlik darajasini baholash uchun maxsus reyting axborot tizimi ishlab chiqildi, bank va to‘lov tashkilotlarining kiberxavfsizlik hamda anti-frod bo‘linmalari uchun muntazam treninglar tashkil etildi [2]. Bu holat xavfsizlik

masalasi milliy to‘lov siyosatining alohida texnik yo‘nalishidan tizimli boshqaruv vazifasiga aylanayotganini ko‘rsatadi.

Bundan tashqari, Markaziy bankning moliyaviy barqarorlik bo‘yicha 2024 va 2025-yil hisobotlarida kiberxatarlarning ortishi moliyaviy tizim barqarorligiga tahdid solishi, kiberhujumlar, ma’lumotlarning buzilishi va o‘g‘irlanishi kabi operatsion xatarlar moliyaviy yo‘qotishlarni kuchaytirishi ta’kidlangan. Shu bilan birga shubhali operatsiyalarni cheklash, kiberhimoya tizimlarini mustahkamlash va aholining kiberfiribgarlik bo‘yicha xabardorligini oshirish choralar sifatida ko‘rsatilgan [3;4].

Ilmiy muammoning dolzarbligi shundaki, raqamli to‘lov infratuzilmasida “moliyaviy xatar” va “axborot xatari” chegaralari tobora yemirilmoqda. Masalan, hisobga noqonuniy kirish avval kiberxavfsizlik hodisasi sifatida boshlanib, qisqa vaqt ichida bevosita moliyaviy yo‘qotish, likvidlik bosimi, reputatsion zarar va mijozlar ishonchining pasayishiga olib kelishi mumkin. Demak, boshqaruv tizimi risklarni ketma-ket emas, balki bog‘langan portfel sifatida ko‘rishi kerak.

Maqolaning maqsadi O‘zbekistonda raqamli to‘lov infratuzilmasida moliyaviy xatarlarni boshqarish va axborot xavfsizligini ta’minlashning integratsiyalashgan mexanizmini ishlab chiqish hamda uning institutsional va amaliy samaradorligini baholashdan iborat. Ushbu maqsadga erishish uchun quyidagi vazifalar belgilandi: raqamli to‘lovlar uchun xatarlar taksonomiyasini shakllantirish; milliy va xalqaro nazorat yondashuvlarini qiyoslash; xatarlarni o‘lchash indikatorlarini taklif etish; ikki bosqichli boshqaruv modeli va 2027–2030-yillar uchun siyosiy yo‘l xaritasini ishlab chiqish.

Tadqiqot obyekti — O‘zbekiston raqamli to‘lov infratuzilmasida banklar, to‘lov tashkilotlari, to‘lov tizimi operatorlari va ularga xizmat ko‘rsatuvchi texnologik subyektlar o‘rtasidagi risk-munosabatlardir. Tadqiqot predmeti esa mazkur munosabatlarni tartibga soluvchi tashkiliy, iqtisodiy, texnik va axborot-xavfsizlik mexanizmlarining o‘zaro ta’siridir.

Adabiyotlar sharhi

Raqamli to‘lov tizimlaridagi xatarlarni boshqarish bo‘yicha xalqaro ilmiy va me’yoriy adabiyotlar bir necha asosiy yo‘nalishga ajraladi. Birinchi yo‘nalish to‘lov tizimlarining tizimli ahamiyatiga e’tibor beradi. CPMI-IOSCOning Financial Market Infrastructures uchun Prinsiplari to‘lov tizimlarida kredit, likvidlik, operatsion, huquqiy va boshqa risklarni boshqarish, shuningdek uzluksizlik va umumiy boshqaruvni alohida prinsiplar sifatida ko‘radi [5]. Bu yondashuv raqamli to‘lovlar uchun ham dolzarb, chunki katta hajmli yoki ko‘plab ishtirokchilarni bog‘laydigan platformadagi uzilish butun ekotizimga tarqalishi mumkin.

Ikkinchi yo‘nalish operatsion barqarorlik va kiberxavfsizlikni markazga qo‘yadi. Bazel qo‘mitasi materiallarida muhim operatsiyalarni qo‘llab-quvvatlaydigan ICT infratuzilmasi aniqlanishi, himoya–aniqlash–javob–tiklash sikli muntazam sinovdan o‘tkazilishi va boshqaruvda risk egasi aniq belgilanishi lozimligi ta’kidlanadi [6]. Ushbu sikl moliyaviy xatarlar uchun ham mos keladi, chunki texnologik uzilish tezda likvidlik va hisob-kitob xatariga aylanadi.

Uchinchi yo‘nalish kiberxatarlarning dinamikasini o‘rganadi. NIST Cybersecurity Framework 2.0 boshqaruv, aniqlash, himoya, aniqlash, javob va tiklash funksiyalarini yagona risk boshqaruvi doirasida ko‘radi. ISO/IEC 27001 esa axborot xavfsizligini axborot aktivlari, boshqaruv jarayonlari va doimiy takomillashtirish prinsiplariga bog‘laydi [7;8]. Bunday yondashuv raqamli to‘lovlar uchun “texnik choralar ro‘yxati”dan ko‘ra ancha samarali, chunki u xavfsizlikni boshqaruv tizimi bilan bog‘laydi.

To‘rtinchi yo‘nalishda firibgarlik va iste’molchi zarari masalalari ko‘riladi. Raqamli to‘lovlarda autentifikatsiya kuchli bo‘lsa ham, ijtimoiy muhandislik, soxta ilovalar, fishing, SIM-swapping, hisob ma’lumotlarini egallash va pulni tezkor ko‘chirish kabi holatlar mavjud. Shuning uchun antifrod tizimlarida faqat “to‘lovni tasdiqlash” emas, balki foydalanuvchi xulqi, qurilma signallari, tranzaksiya konteksti va tarmoq aloqalarini birgalikda baholash zarur.

O‘zbekiston bo‘yicha huquqiy va institutsional bazada “To‘lovlar va to‘lov tizimlari

to‘g‘risida”gi qonun, “Shaxsga doir ma’lumotlar to‘g‘risida”gi qonun, “Kiberxavfsizlik to‘g‘risida”gi qonun hamda Markaziy bankning to‘lov tizimlari uchun axborot va kiberxavfsizlik talablariga oid normativ hujjatlari muhim o‘rin tutadi. 2024-yildagi tegishli nizom to‘lov tizimi operatorlari va to‘lov xizmatlarini yetkazib beruvchilardan axborot va kiberxavfsizlik zaifliklarini tahlil qilish, yiliga kamida ikki marta ruxsatsiz kirishga test o‘tkazish va Markaziy bankka yillik hisobot taqdim etishni talab qiladi [9].

2026-yilda shaxsga doir ma’lumotlarni himoya qilish bo‘yicha yangi o‘zgartirishlar kiritilishi, ayrim toifadagi ma’lumotlarni O‘zbekiston hududida saqlash talablarining kuchaytirilishi raqamli to‘lovlar xavfsizligini ma’lumotlar boshqaruvi bilan yanada chambarchas bog‘laydi [10]. Shuningdek, 2026-yil martidagi davlat siyosati taqdimotlarida kiberjinoyatlarga qarshi kurashni kuchaytirish va raqamli huquqbuzarliklarning oldini olish tizimini takomillashtirish ustuvor vazifa sifatida belgilangan [11].

Adabiyotlar tahlili shuni ko‘rsatadiki, xalqaro yondashuvlarning ko‘pchiligi riskni aniqlash va kiberbarqarorlikni boshqarish uchun yetarli nazariy asos yaratgan bo‘lsa-da, O‘zbekiston sharoitida alohida muammo institutlararo ma’lumot almashinuvi, risklarni yagona taksonomiya asosida baholash, kichik va yirik to‘lov tashkilotlariga proporsional talablarni qo‘llash hamda mijoz zararini tezkor qoplash mexanizmlarini birlashtirishdan iborat. Mazkur maqola aynan shu “bog‘lovchi qatlam”ni ishlab chiqishga intiladi.

Tadqiqot metodologiyasi

Tadqiqotda raqamli to‘lov infratuzilmasining xavf profili moliyaviy va axborot xavfsizligi bloklarini birlashtirgan ko‘p mezonli yondashuv orqali baholandi. Birinchi bosqichda risk taksonomiyasi shakllantirildi. Unda kredit, likvidlik, operatsion, firibgarlik, kiberxavfsizlik, ma’lumotlar yaxlitligi, uchinchi tomon va reputatsion risklar ajratildi. Ikkinchi bosqichda har bir riskning ehtimolligi va ta’sir darajasi 1–5 ballik shkala bo‘yicha baholandi. Uchinchi bosqichda mavjud nazorat choralarining riskni qoplash koeffitsiyenti ekspert-analitik yondashuv bilan hisoblandi.

Taklif etilgan umumiy risk skori quyidagicha ifodalanadi: $R = P \times I \times (1 – C)$, bu yerda P — hodisaning ehtimolligi, I — moliyaviy va operatsion ta’sir, C — amaldagi nazorat choralarining qoplash koeffitsiyenti. Mazkur formula sof statistik parametr emas; u risklarni ustuvorlashtirishga xizmat qiladigan boshqaruv indikatori sifatida ishlatiladi. C koeffitsiyenti nazoratning mavjudligi, avtomatlashtirilishi, mustaqil testdan o‘tkazilishi va incidentdan keyingi tiklanish qobiliyatini birlashtiradi.

Risklarni boshqarishda “himoya darajalari” konsepsiyasi qo‘llanildi: birlamchi profilaktika, autentifikatsiya va kirishni boshqarish; tranzaksiya darajasida antifrod va limitlar; tarmoq darajasida segmentatsiya va himoya; ma’lumot darajasida shifrlash va yaxlitlik; monitoring darajasida SIEM va xulq-atvor analitikasi; javob va tiklash darajasida incident response, backup va disaster recovery. Tizimning barqarorligi bitta qatlamga emas, qatlamlarning bir-birini qoplashiga bog‘liq deb qabul qilindi.

Empirik baza sifatida Markaziy bankning 2025-yil yillik hisobotidagi to‘lov va axborot xavfsizligi ma’lumotlari, 2025-yil yakuni bo‘yicha bank kartalari, POS terminallari va ATM infratuzilmasi statistikasi, 2024 va 2025-yillarga oid moliyaviy barqarorlik hisobotlari, shuningdek milliy normativ hujjatlar va xalqaro standartlardan foydalanildi [1–10]. 2025-yilda POS tranzaksiyalarining 460,3 trln so‘mga yetishi to‘lov oqimlari hajmining oshganini ko‘rsatadi; shu bilan birga Markaziy bankning 2025-yil hisobotida xavfsiz ulanishlar, kiberxavfsizlik reytingi va anti-frod ko‘nikmalarini kuchaytirish choralari qayd etilgan [1;2].

Ssenariy modellashtirishda uch variant tanlandi: inertial, muvozanatli va tezlashtirilgan. Inertial ssenariy mavjud mexanizmlar saqlanib qolishini; muvozanatli ssenariy riskka asoslangan nazorat, incident reporting, interoperabellik va kiberstress-testlarning parallel joriy etilishini; tezlashtirilgan ssenariy esa real vaqtga yaqin nazorat, yagona anti-frod platformasi, xavfsiz API profili va iste’molchilarni himoya qilishning avtomatlashtirilgan mexanizmlarini to‘liqroq joriy

etishni nazarda tutadi.

Metodologiyaning cheklovi shundaki, ochiq manbalarda ayrim kiberhodisalar bo‘yicha granular, bank yoki to‘lov tashkiloti kesimidagi zarar statistikasi mavjud emas. Shu sababli ekspert-analitik ballar sabab-natija dalili sifatida emas, siyosiy diagnostika va ustuvorlashtirish vositasi sifatida talqin qilinadi. Maqolaning ilmiy yangiligi aynan shu cheklovni hisobga olgan holda, mavjud rasmiy ma’lumotlarni risk boshqaruvi indikatorlari bilan integratsiyalashgan modelga kiritishdadir.

Tahlil va natijalar

Raqamli to‘lov infratuzilmasidagi moliyaviy xatarlar texnologik jarayonlardan ajralgan holda mavjud bo‘lmaydi. To‘lovning yakunlanishi uchun mablag‘lar, identifikatsiya ma’lumotlari, aloqa kanallari, dasturiy komponentlar va hisob-kitob platformalari o‘zaro bog‘langan. Shu bois xatarlarni “moliyaviy” va “kiber” deb qat’iy ajratish boshqaruv nuqtai nazaridan yetarli emas. Masalan, autentifikatsiyaga qarshi hujum mablag‘larning noqonuniy chiqib ketishiga, likvidlik muammosiga, iste’molchi shikoyatlarining oshishiga va reputatsion zararga olib kelishi mumkin.

2025-yilda Markaziy bank tomonidan 68,3 mln bank kartasi, 430,8 ming POS-terminal va 40,1 ming ATM/self-service qurilmasi qayd etilgani to‘lov ekotizimining masshtabini ko‘rsatadi. 460,3 trln so‘mlik POS tranzaksiyasi esa infrastrukturaning real iqtisodiy ahamiyatini ifodalaydi [1]. Shu miqyosda bir kunlik uzilishning o‘zi ham minglab tadbirkorlar, aholi va davlat xizmatlari to‘lovlariga ta’sir qilishi mumkin; shuning uchun “uptime” endi oddiy IT ko‘rsatkichi emas, moliyaviy barqarorlik ko‘rsatkichi hamdir.

1-jadval.

Raqamli to‘lov infratuzilmasidagi asosiy moliyaviy va axborot xatarlari*

Xatar turi	Asosiy namoyon bo‘lish shakli	Ehtimollik (1–5)	Ta’sir (1–5)	Ustuvor boshqaruv chorasi
Firibgarlik xatari	Fishing, social engineering, account takeover, soxta ilova	5	5	Real vaqt anti-frod, xulq-atvor modeli, kuchli autentifikatsiya
Operatsion xatar	Tizim uzilishi, dasturiy xato, konfiguratsiya xatosi	4	5	BCP/DR, redundant infratuzilma, failover sinovlari
Kiberxavfsizlik xatari	Zararli dastur, DDoS, credential theft, ransomware	4	5	Zero Trust, segmentatsiya, EDR/SIEM, patch management
Ma’lumotlar yaxlitligi xatari	Tranzaksiya ma’lumotining buzilishi yoki yo‘qolishi	3	5	Shifrlash, integrity check, audit log, backup
Likvidlik xatari	Hisob-kitob kechikishi, settlement uzilishi	3	5	Likvidlik buferi, intraday monitoring, contingency funding
Uchinchi tomon xatari	Cloud, processor, telecom yoki fintech provayder uzilishi	4	4	SLA, vendor risk management, exit plan, multi-vendor
Reputatsion xatar	Katta hodisa va iste’molchi ishonchining pasayishi	3	4	Krizis kommunikatsiyasi, tezkor kompensatsiya, ochiq incident siyosati

*Muallif ishlanmasi

Axborot xavfsizligi va moliyaviy xatarlarni birlashtirish modeli

Xatarlarni boshqarishning integratsiyalashgan modelida asosiy tamoyil — texnik hodisani moliyaviy oqibat bilan bog‘lash. Tizimda kiberhodisa sodir bo‘lganda, parallel ravishda uchta savolga javob topilishi kerak: birinchidan, hodisa qaysi aktiv yoki jarayonni shikastladi; ikkinchidan, qaysi to‘lov oqimi va mijozlar ta’sirlandi; uchinchidan, mablag‘larni himoyalash va xizmatni tiklash uchun qaysi choralar birinchi navbatda bajariladi. Bu yondashuv xavfsizlik bo‘limi va risk bo‘limini alohida ishlashdan integratsiyalashgan boshqaruvga olib keladi.

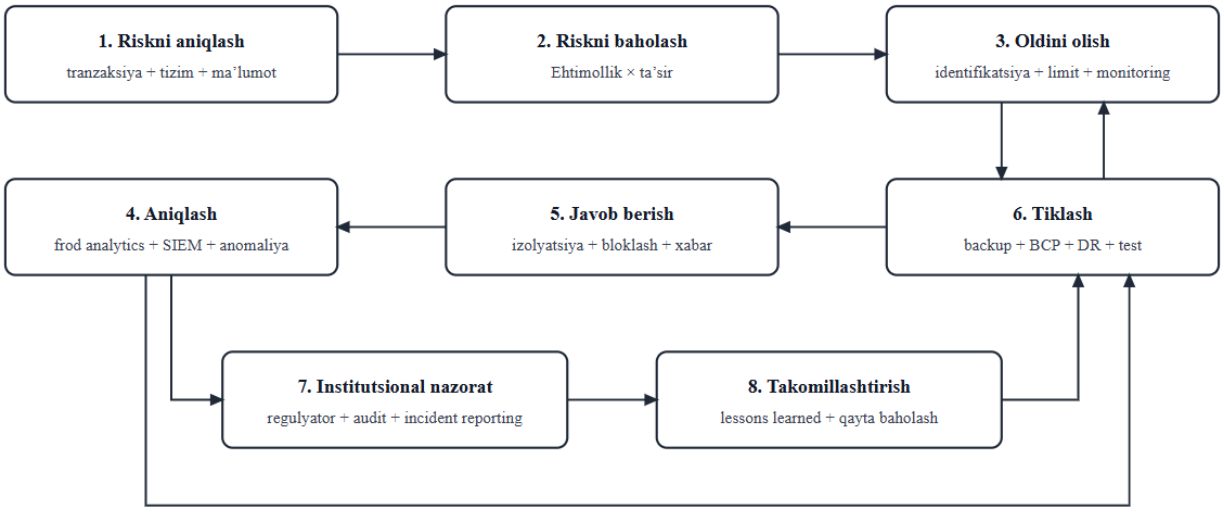
2025-yil hisobotida Markaziy bank axborot tizimlari, banklar va boshqa moliya institutlari o‘rtasidagi 134 ta tashqi ulanishni xavfsiz kanallar orqali himoyalaganini, kiberxavfsizlik reyting tizimini ishlab chiqqanini va anti-frod/kiberxavfsizlik bo‘linmalari uchun muntazam treninglar tashkil etilganini qayd etadi [2]. Bu amaliyot xavfsizlikni faqat ichki IT funksiyasi emas, balki nazorat qilinadigan institutsional ko‘rsatkich sifatida shakllantirish uchun muhim asos yaratadi.

2024-yil moliyaviy barqarorlik hisobotida kiberxatarlarning kuchayishi, kiberhujumlar, ma’lumotlarning buzilishi va o‘g‘irlanishi moliyaviy yo‘qotishlarni oshirishi qayd etilgan. Tavsiya etilgan choralar orasida shubhali operatsiyalarni cheklash, barqaror axborot xavfsizligi tizimlarini rivojlantirish va aholining kiberfiribgarlik bo‘yicha savodxonligini oshirish keltirilgan [3]. Mazkur choralar bizning modelimizda mos ravishda aniqlash, oldini olish va iste’molchi qatlamlariga to‘g‘ri keladi.

2024-yilda bank karta firibgarligi bo‘yicha murojaatlar doirasida 9,5 mlrd so‘mlik mablag‘ bloklangani va onlayn mikroqarz firibgarligini kamaytirish uchun ayrim kredit operatsiyalarida 48 soatgacha qo‘shimcha tekshiruv cheklovlari joriy etilgani Markaziy bank yillik hisobotida qayd etilgan [2]. Ushbu tajriba xavf yuqori bo‘lgan operatsiyalar uchun “friksiya”ni oshirish, xavf past bo‘lgan operatsiyalarda esa to‘lovni maksimal tezlashtirish tamoyilining amaliy ahamiyatini ko‘rsatadi.

1-rasm.

Raqamli to‘lov infratuzilmasida moliyaviy xatarlarni boshqarish va axborot xavfsizligi konturi*



*Muallif ishlanmasi.

Rasmda ifodalangan model klassik “himoyalash” tushunchasidan farq qiladi. Unda xavfsizlik choralari incident sodir bo‘lishidan oldin va keyin ham ishlaydi. Masalan, identifikatsiya qatlamidagi xato tarmoq monitoringi, tranzaksiya monitoringi va mijoz xulqi analitikasi orqali qayta aniqlanishi mumkin. Shuningdek, tizim qayta tiklangandan so‘ng “lessons learned” bosqichi risk profillarini yangilashi va kelgusi davrda yangi nazorat talablarini shakllantirishi kerak.

Mazkur model institutsional nuqtai nazardan uch boshqaruv sathini talab qiladi: 1)

tashkilotning ichki risk egasi va xavfsizlik funksiyasi; 2) to‘lov tizimi operatori yoki boshqa ekotizim koordinatori; 3) Markaziy bank va tegishli vakolatli davlat organlarining nazorati. Ularning har biri uchun incident toifalari, xabar berish chegaralari, ma’lumot almashish protokoli va javob muddatlari oldindan standartlashtirilishi lozim.

Moliyaviy xatarlarni boshqarish samaradorligini baholash

Xatarni boshqarish samaradorligi mavjud nazorat choralarining soni bilan emas, ularning riskni qanchalik kamaytirayotgani bilan o‘lchanishi kerak. Shu maqsadda maqolada “qoplash koeffitsiyenti” va “qoldiq risk” tushunchalaridan foydalanildi. Masalan, boshlang‘ich firibgarlik riskining ehtimolligi 5 ball bo‘lib, real vaqt antifrod tizimi, qurilma identifikatsiyasi va kuchli autentifikatsiya nazoratlari 0,70 qoplash koeffitsiyentiga ega deb baholansa, qoldiq risk R formula bo‘yicha sezilarli kamayadi. Bu ko‘rsatkichlarni har oy qayta hisoblash orqali nazorat investitsiyalarining samarasini monitoring qilish mumkin.

Baholashning asosiy amaliy foydasi resurslarni bir xil taqsimlamaslikdir. Yuqori riskli tashkilotlar yoki xizmatlar uchun mustaqil penetration test, doimiy SIEM monitoringi, stress-test va muhim komponentlar bo‘yicha zaxira infratuzilmasi talab qilinadi. Past riskli xizmatlar uchun esa soddalashtirilgan talablar qo‘llanilishi mumkin. Proporsionallik innovatsiya va xavfsizlik o‘rtasidagi muvozanatni yaxshilaydi.

2-jadval.

Integratsiyalashgan risk boshqaruvi uchun taklif etilayotgan indikatorlar va maqsadli darajalar*

Indikator	Og‘irlik	Bazaviy analitik baho	2027 maqsad	2030 maqsad
Kiberhodisani aniqlash tezligi	15%	62	78	90
Firibgarlikni tranzaksiya bosqichida bloklash	15%	68	82	92
Muhim xizmatlar uzluksizligi va DR tayyorgarligi	15%	70	84	93
Zaifliklarni muntazam test qilish qamrovi	10%	66	85	95
Incident reporting to‘liqligi va tezligi	10%	58	80	94
Ma’lumotlar yaxlitligi va audit izi	10%	71	86	95
Uchinchi tomon risklarini boshqarish	10%	55	76	90
Iste’molchi zararini ko‘rib chiqish va qoplash tezligi	10%	64	82	93
Kadrlar va kiberxavfsizlik kompetensiyasi	5%	69	82	92
Yakuniy integrallashgan indeks	100%	64.4	82.0	93.0

*Muallif ishlanmasi.

Jadvaldagi bazaviy qiymatlar rasmiy milliy reyting emas, mazkur tadqiqot uchun ochiq ma’lumotlar va xalqaro talablar asosida tuzilgan analitik skoringdir. Undagi eng past yo‘nalishlar uchinchi tomon risklari, incident reporting va aniqlash tezligidir. Bu uchlik raqamli to‘lovlarda tobora ko‘proq “ekotizim xavfi” paydo bo‘layotganini anglatadi: tashkilot o‘zining IT tizimini yaxshi himoya qilgan bo‘lsa ham, processor, cloud, telekom yoki boshqa provayderdagi nosozlikdan zarar ko‘rishi mumkin.

Kiberhodisani aniqlash tezligi moliyaviy xavfni kamaytirishda alohida ahamiyatga ega. Birinchi daqiqalarda aniqlangan hisob egallash hodisasi bloklanishi, kech aniqlanganida esa mablag‘lar bir necha tashkilot va hisoblar bo‘ylab ko‘chib ketishi mumkin. Shu sababli xavfsizlikning samaradorligi “oldini olish” bilan birga “aniqlash va javob berish” tezligi orqali o‘lchanishi lozim.

Riskni o‘lchashda iste’molchi zararini qoplash tezligi ham alohida indikator sifatida kiritildi. Bu ko‘rsatkich texnik xavfsizlik indikatorlari orasida ko‘pincha e’tibordan chetda qoladi, biroq raqamli to‘lovlar bozorining ishonchliligini aynan foydalanuvchi tajribasi belgilaydi. Foydalanuvchi himoya tizimiga ishonmasa, raqamli kanalning iqtisodiy afzalliklari kamayadi. Shu nuqtai nazardan tezkor kompensatsiya va shaffof nizoni hal etish tizimi risk boshqaruvining bir qismidir.

O‘zbekistonda institutsional mexanizmlarni takomillashtirish yo‘nalishlari

Milliy institutlarni takomillashtirishning birinchi yo‘nalishi — “yagona risk taksonomiyasi”ni joriy etish. Banklar, to‘lov tashkilotlari, to‘lov tizimi operatorlari va texnologik provayderlar bir xil atamalar, incident toifalari va risk darajalaridan foydalanishi kerak. Hozirgi holatda alohida tashkilotlar o‘z ichki risk xaritalariga ega bo‘lishi tabiiy, biroq nazoratchi uchun ularni umumiy ko‘rsatkichga aylantirish qiyinlashadi. Yagona taksonomiya esa SupTech va idoralararo tahlil uchun “umumiy til” yaratadi.

Ikkinchi yo‘nalish — real vaqtga yaqin risk monitoringi. Markaziy bankning kiberxavfsizlik reyting tizimi va xavfsiz ulanishlar bo‘yicha amaliyoti ushbu yo‘nalish uchun institutsional asos yaratadi [2]. Keyingi bosqichda tranzaksiya xavfi, kiberhodisa, uzilish, mijoz shikoyati va uchinchi tomon hodisalarini birlashtirgan umumiy risk panelini ishlab chiqish maqsadga muvofiq. Bu platforma individual mijoz ma’lumotlarini oshkor qilmasdan, agregat ko‘rsatkichlar orqali regulyatorga erta ogohlantirish signalini berishi mumkin.

Uchinchi yo‘nalish — uchinchi tomon risklarini regulyativ nazoratga kiritish. Cloud servis, processor, data-center, telecom operator yoki antifrod texnologiyasi provayderi to‘lov zanjirining muhim qismiga aylanganida uning uzilishi bank yoki to‘lov tashkilotining o‘zidan kelib chiqmagan bo‘lsa ham xizmatga ta’sir qiladi. Shu bois muhim vendorlar uchun minimal SLA, audit huquqi, incident notification, ma’lumotni qaytarish va “exit plan” talablarini standartlashtirish kerak.

To‘rtinchi yo‘nalish — muhim to‘lov infratuzilmasi uchun operatsion barqarorlik testlarini kuchaytirish. BIS va boshqa xalqaro yondashuvlar muhim operatsiyalar uchun himoya, aniqlash, javob va tiklash funksiyalarining muntazam sinovini talab qiladi [6]. O‘zbekistonda bu talablar riskka proporsional ravishda stress-testlar, failover mashqlari, zaxira markazni ishga tushirish testlari va tiklanish vaqtini o‘lchash bilan kengaytirilishi mumkin.

Beshinchi yo‘nalish — anti-frod ma’lumotlarini ekotizimlararo almashish. Firibgarlar bitta bank yoki bitta ilova doirasida emas, turli platformalar o‘rtasida ishlaydi. Shu sababli banklar, to‘lov tashkilotlari, operatorlar va vakolatli davlat organlari uchun huquqiy asosda ma’lum darajadagi “fraud intelligence sharing” mexanizmi yaratilishi foydali. Bunda shaxsga doir ma’lumotlarni himoya qilish talablari bajarilgan holda, xavf signallari, qurilma indikatorlari, shubhali hisoblar va takroriy sxemalar bo‘yicha ma’lumotlar almashinuvi yo‘lga qo‘yiladi.

Oltinchi yo‘nalish — kuchli autentifikatsiyani foydalanuvchi tajribasi bilan muvofiqlashtirish. Barcha operatsiyalarga bir xil qattiq tasdiqlash talabini qo‘yish xizmatni sekinlashtiradi va ayrim foydalanuvchilarni norasmiy kanallarga o‘tishga undashi mumkin. Shuning uchun “risk-based authentication” tamoyili muhim: oddiy va odatiy to‘lovlar minimal

ishqalanish bilan, yuqori riskli operatsiyalar esa qo‘shimcha verifikatsiya bilan bajariladi.

Yettinchi yo‘nalish — ma’lumotlar boshqaruvida “maxfiylik va xavfsizlikni dizaynning boshidan kiritish” tamoyilini joriy etish. 2026-yildagi qonunchilik o‘zgarishlari ayrim toifadagi shaxsga doir ma’lumotlarni O‘zbekiston hududida saqlash talablarini kuchaytirdi [10]. Raqamli to‘lov tashkilotlari uchun bu ma’lumotlar ombori, backup, cloud va transchegaraviy ishlov berish arxitekturasini qayta ko‘rib chiqishni anglatadi. Bunday talablarni texnik xavfsizlik bilan birgalikda ishlab chiqish compliance va innovatsiya o‘rtasidagi muvozanatni saqlashi kerak.

Sakkizinchi yo‘nalish — incident reporting standartini bir xillashtirish. 2024-yilgi to‘lov tizimlari uchun normativ talablar allaqachon axborot va kiberxavfsizlik holati bo‘yicha yillik hisobotni nazarda tutadi [9]. Keyingi bosqichda muhim kiberhodisalar bo‘yicha qisqa muddatli “early notification”, to‘liq texnik hisobot va yakuniy lessons learned hisobotini alohida formatlarga ajratish lozim. Bu regulyatorning hodisani tezroq koordinatsiya qilishiga imkon beradi.

To‘qqizinchi yo‘nalish — kiberxavfsizlik iqtisodiyotini hisoblash. Har bir qo‘shimcha xavfsizlik chorasi xarajat talab qiladi; shu bois risk kamayishining iqtisodiy qiymatini ham o‘lchash kerak. Masalan, anti-frod tizimiga kiritilgan investitsiya natijasida bloklangan firibgarliklar, kamaygan kompensatsiyalar va qisqargan servis uzilishlarining iqtisodiy qiymati alohida indikator sifatida baholanadi. Bu “xavfsizlik xarajati”ni oddiy IT xarajatidan investitsiya sifatida ko‘rishga imkon beradi.

2027–2030-yillarda risk-boshqaruv tizimini bosqichma-bosqich joriy etish

Institutsional mexanizmni bir vaqtning o‘zida to‘liq qayta qurish amaliy jihatdan qimmat va tashkiliy jihatdan murakkab bo‘lishi mumkin. Shu sababli taklif etilayotgan model bosqichma-bosqich joriy etilishi lozim. Birinchi bosqich 2027-yilda normativ va ma’lumotlar arxitekturasini birxillashtirishga qaratiladi. Bu davrda yagona risk taksonomiyasi, incident kategoriyalari, minimal vendor risk talablari, xavfsiz API uchun bazaviy profil va to‘lov tashkilotlari uchun umumiy kiberhodisa xabar berish shakllari tasdiqlanishi kerak.

Ikkinchi bosqich 2028-yilda nazoratni avtomatlashtirish va risk signallarini birlashtirishni ko‘zda tutadi. SupTech platformasi orqali to‘lov tashkilotlari va banklardan olinadigan agregat risk ma’lumotlari yagona panelga yig‘iladi. Ushbu platformada operatsion uzilishlar, shubhali tranzaksiyalar, kiberhodisalar, mijoz shikoyatlari va uchinchi tomon hodisalari bo‘yicha indikatorlar birlashtiriladi. Natijada nazoratchi tashkilotning moliyaviy ko‘rsatkichlarini uning texnologik va operatsion risk profili bilan birgalikda ko‘ra oladi.

Uchinchi bosqich 2029–2030-yillarda tizimli barqarorlikka yo‘naltiriladi. Bu bosqichda muhim to‘lov tizimlari uchun umumiy kiberstress-test ssenariylari, tarmoqlararo fraud intelligence sharing, xizmat uzilishi paytida avtomatik tranzaksiya yo‘naltirish va iste’molchi zararini tezkor qoplash mexanizmlari kengaytiriladi. Tizimning natijasi faqat xavfsizlik darajasining oshishi emas, balki to‘lov xizmatlarining iqtisodiy samaradorligi va ishonchliligining o‘sishi bo‘lishi kerak.

Bosqichma-bosqich yondashuvda muhim tamoyil — “bir xil talab, turlicha chuqurlik” prinsipidir. Masalan, barcha to‘lov tashkilotlari uchun minimal identifikatsiya, audit log, zaifliklarni boshqarish va incident reporting talablari bir xil bo‘lishi mumkin. Biroq tizimli ahamiyatga ega operatorlar uchun talablar ancha chuqur: mustaqil audit, zaxira markaz, RTO/RPO ko‘rsatkichlari, muntazam penetration testing va scenario-based resilience exercise talab qilinadi. Bu proporsional yondashuv kichik innovatsion kompaniyalarning bozorga kirishiga ortiqcha to‘siq qo‘ymasdan tizimli riskni cheklaydi.

Joriy etish samaradorligi uch darajada o‘lchanishi lozim. Birinchi daraja texnik: aniqlash va tiklash vaqti, tizim uzilishlarining soni, zaifliklarni yopish muddati. Ikkinchi daraja moliyaviy: firibgarlik yo‘qotishlari, kompensatsiya xarajatlari, uzilish tufayli boy berilgan tranzaksiyalar va xavfsizlik investitsiyasining oldi olingan zarar bilan nisbati. Uchinchi daraja institutsional: incident reporting tezligi, ma’lumot almashish sifati, nazorat tekshiruvlarining riskka mosligi va ishtirokchilarning compliance yukining o‘zgarishi. Aynan uchinchi daraja modelning davlat

boshqaruvi nuqtai nazaridan samaradorligini ko‘rsatadi.

Xatarlar boshqaruvini iqtisodiy jihatdan asoslash uchun “oldi olingan zarar qiymati” ko‘rsatkichini kiritish tavsiya etiladi. Masalan, anti-frod investitsiyasi natijasida bloklangan operatsiyalarning ehtimoliy zarari, tezroq tiklangan xizmat tufayli saqlab qolingan tranzaksiya hajmi va iste’molchi kompensatsiyasining qisqarishi hisobga olinadi. Ushbu ko‘rsatkich rahbariyat va regulyatorga kiberxavfsizlik xarajatlarini oddiy ma’muriy xarajat emas, riskni kamaytiradigan kapital qo‘yilma sifatida baholash imkonini beradi.

Institutional maturity nuqtai nazaridan eng katta o‘zgarish “hodisa sodir bo‘lgandan keyingi” boshqaruvdan “hodisa sodir bo‘lishidan oldingi” boshqaruvga o‘tishdir. Buning uchun threat intelligence, vulnerability management, transaction analytics va scenario testing tizimlari bir-biriga ulanadi. Kelgusida sun’iy intellekt asosidagi anomaliya aniqlash vositalari ham kengayishi mumkin, biroq ulardan foydalanishda model riski, noto‘g‘ri ijobiy signallar, explainability va ma’lumotlarning sifati alohida nazorat obyekti bo‘lishi kerak.

Mazkur yo‘l xaritasida davlat organlari va bozor ishtirokchilari o‘rtasidagi hamkorlik ham muhim. Markaziy bank regulyativ standartlar va nazorat metodologiyasini belgilaydi; banklar va to‘lov tashkilotlari risklarni operatsion darajada boshqaradi; telekommunikatsiya, texnologik va boshqa provayderlar uchinchi tomon risklarini kamaytirish talablariga rioya qiladi; huquqni muhofaza qiluvchi organlar esa raqamli firibgarlik sxemalari bo‘yicha tezkor axborot almashinuvi va tergov choralarini ta’minlaydi. Shunday qilib, raqamli to‘lov xavfsizligi yagona tashkilotning emas, ekotizimning umumiy institutsional javobgarligiga aylanadi.

Xulosa

Tadqiqot natijalari raqamli to‘lov infratuzilmasida moliyaviy xatarlar va axborot xavfsizligi xatarlarini alohida boshqarish tobora samarasizlashayotganini ko‘rsatdi. To‘lov ekotizimining texnologik murakkabligi ortishi bilan bitta kiberhodisa bir vaqtning o‘zida moliyaviy yo‘qotish, likvidlik bosimi, xizmat uzilishi, ma’lumotlar buzilishi va iste’molchi ishonchining pasayishiga olib kelishi mumkin. Shu sababli boshqaruv modeli risklar portfeli va hodisalar hayot siklini birlashtirishi kerak.

O‘zbekiston uchun muhim institutsional afzallik shundan iboratki, to‘lov infratuzilmasi bo‘yicha Markaziy bankning nazorat amaliyoti so‘nggi yillarda axborot xavfsizligi va anti-frod yo‘nalishlari bilan kengayib bormoqda. 2025-yilda xavfsiz ulanishlar, kiberxavfsizlik reytingi, kiberxavfsizlik va anti-frod bo‘yicha treninglar kabi choralarning amalga oshirilishi tizimning tayyorgarlik darajasi oshayotganini ko‘rsatadi [2]. Biroq raqamli to‘lov hajmi va ishtirokchilar sonining o‘sishi bu mexanizmlarni yagona risk arxitekturasiga integratsiya qilishni talab etadi.

Maqolada taklif etilgan integratsiyalashgan model “aniqlash–baholash–oldini olish–aniqlash–javob–tiklash–qayta baholash” sikliga asoslanadi. Uning asosiy ustunligi shundaki, xavfsizlik nazorati xizmatning faqat kirish qismida emas, tranzaksiya, tarmoq, ma’lumot, monitoring va tiklash darajalarida takroriy tarzda ishlaydi. Bunday “defense-in-depth” arxitekturasi bitta himoya mexanizmi buzilgan taqdirda ham riskning to‘liq amalga oshish ehtimolini kamaytiradi.

Birinchi amaliy taklif — banklar, to‘lov tashkilotlari va operatorlar uchun yagona risk taksonomiyasi hamda yagona incident reporting lug‘atini ishlab chiqish. Ikkinchi taklif — yuqori riskli xizmatlar uchun real vaqtga yaqin monitoring va risk-based authenticationni joriy etish. Uchinchi taklif — muhim uchinchi tomon provayderlari uchun vendor risk management va exit plan talablarini standartlashtirish. To‘rtinchi taklif — muhim to‘lov infratuzilmasida kiberstress-test va failover mashqlarini muntazam o‘tkazish.

Beshinchi taklif — fraud intelligence sharing mexanizmini huquqiy va texnik jihatdan shakllantirish. Oltinchi taklif — iste’molchi zararini baholash va qoplashning yagona SLA tizimini joriy etish. Yettinchi taklif — 2026-yildagi shaxsga doir ma’lumotlar bo‘yicha yangi talablarni payment-by-design va privacy-by-design tamoyillari bilan uyg‘unlashtirish. Sakkizinchi taklif — kiberxavfsizlik investitsiyalarining iqtisodiy samaradorligini yillik risk kamayishi bilan

o‘lchaydigan indikatorni kiritish.

2027–2030-yillar uchun tavsiya etiladigan siyosiy yo‘l xaritasi uch bosqichdan iborat. 2027-yilda risk taksonomiyasi, incident reporting va vendor risk standartlari ishlab chiqiladi. 2028-yilda SupTech, antifrod ma’lumot almashinuvi va risk-based authenticationning kengaytirilgan mexanizmlari joriy etiladi. 2029–2030-yillarda esa kiberstress-testlarning sektoral darajadan tizimli darajaga o‘tkazilishi, xizmatlararo interoperabellik va iste’molchi nizolarini avtomatlashtirish yakuniy bosqichga olib chiqiladi.

Xulosa qilib aytganda, raqamli to‘lov infratuzilmasida xavfsizlikning iqtisodiy qiymati faqat yo‘qotishlarni oldini olish bilan o‘lchanmaydi. Barqaror, tezkor va xavfsiz to‘lovlar tranzaksiya xarajatlarini kamaytiradi, raqamli moliyaviy inklyuziyani kuchaytiradi, biznesning pul oqimini tezlashtiradi va iqtisodiyotdagi ishonch kapitalini oshiradi. Shu bois moliyaviy xatarlarni boshqarish va axborot xavfsizligini ta’minlash bir-biridan ajralgan texnik yo‘nalish emas, raqamli iqtisodiyotning institutsional barqarorligini belgilaydigan strategik boshqaruv funksiyasi sifatida qaralishi lozim.

Foydalanilgan adabiyotlar

1. O‘zbekiston Respublikasi Markaziy banki. Information about issued banking cards, POS-terminals, ATM’s and Self-Service Kiosks as of 1 January 2026, transactions through POS-terminals in January–December 2025. Toshkent, 2026.

2. Central Bank of the Republic of Uzbekistan. Annual Report 2025. Tashkent, 2026.

3. Central Bank of the Republic of Uzbekistan. Financial Stability Report for 2024. Tashkent, 2025.

4. Central Bank of the Republic of Uzbekistan. Financial Stability Report for H1 2025. Tashkent, 2025.

5. CPMI-IOSCO. Principles for Financial Market Infrastructures. Bank for International Settlements and International Organization of Securities Commissions, 2012.

6. Basel Committee on Banking Supervision. Principles for operational resilience. Bank for International Settlements, 2021.

7. National Institute of Standards and Technology. Cybersecurity Framework (CSF) 2.0. Gaithersburg, MD, 2024.

8. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection — Information security management systems — Requirements. International Organization for Standardization, 2022.

9. O‘zbekiston Respublikasi qonunchilik to‘plami. To‘lov tizimlari operatorlari va to‘lov xizmatlarini yetkazib beruvchilarning axborot xavfsizligi va kiberxavfsizligini ta’minlashga oid normativ talablar, 2024.

10. O‘zbekiston Respublikasi. “Shaxsga doir ma’lumotlar to‘g‘risida”gi O‘RQ-547-son Qonun va 2026-yil 26-martdagi O‘RQ-1125-son o‘zgartirishlar.

11. O‘zbekiston Respublikasi Prezidenti. Uyushgan jinoyatchilik va kiberjinoyatlarga qarshi kurashish takomillashtiriladi. 12.03.2026.

12. O‘zbekiston Respublikasi. “Kiberxavfsizlik to‘g‘risida”gi O‘RQ-764-son Qonun, 15.04.2022.

13. European Union Agency for Cybersecurity (ENISA). Threat Landscape for Financial Sector and related cybersecurity guidance. ENISA publications.

14. BIS. Operational resilience and technology risk management: selected supervisory principles and practices. Bank for International Settlements, Basel.

15. World Bank. The Global Findex Database 2021: Financial Inclusion, Digital Payments, and Resilience in the Age of COVID-19. Washington, DC, 2022.

16. Arner, D.W., Barberis, J., Buckley, R.P. The evolution of FinTech: A new post-crisis paradigm? Georgetown Journal of International Law, 47, 2016.

17. Gomber, P., Koch, J.-A., Siering, M. Digital Finance and FinTech: current research and

future research directions. Journal of Business Economics, 87, 2017.

18. Ozili, P.K. Impact of digital finance on financial inclusion and stability: A review of empirical evidence. Digital Finance and Financial Stability literature.