ISSN 2181-

RAQAMLI TRANSFORMATSIYA SHAROITIDA TIJORAT BANKLARINING KIBERBARQARORLIGINI TA’MINLASH MEXANIZMLARINI BOSHQARISH VA BANK QURILMALARINING XAVFSIZLIGINI TA’MINLASH

Urmonova Gulmiraxon Muhammadovna

Annotatsiya. Mazkur maqolada raqamli transformatsiya sharoitida tijorat banklarining kiberbarqarorligini ta’minlash mexanizmlarini boshqarish hamda bank qurilmalarining axborot xavfsizligini mustahkamlash masalalari tadqiq etiladi. Tadqiqotda bank tizimida raqamli texnologiyalarning joriy etilishi bilan bog‘liq kiberxavflar, ularning bank faoliyatiga ta’siri va kiberbarqarorlikni oshirishga qaratilgan boshqaruv yondashuvlari tahlil qilinadi. Shuningdek, bank infratuzilmasi va qurilmalarini himoyalashda zamonaviy axborot xavfsizligi vositalaridan foydalanish, risklarni boshqarish hamda profilaktik choralarni takomillashtirish bo‘yicha amaliy tavsiyalar ishlab chiqiladi.

Kalit so‘zlar: raqamli transformatsiya, tijorat banklari, kiberbarqarorlik, kiberxavfsizlik, bank qurilmalari, axborot xavfsizligi, risklarni boshqarish.

Abstract. This article examines the management mechanisms for ensuring the cyber resilience of commercial banks under conditions of digital transformation, as well as issues related to strengthening the security of banking devices. The study analyzes cyber threats arising from the widespread adoption of digital technologies in the banking sector, their impact on banking operations, and modern management approaches aimed at enhancing cyber resilience. Particular attention is paid to the protection of banking infrastructure and devices through the use of advanced information security tools, effective risk management practices, and preventive measures. Based on the analysis, practical recommendations are proposed to improve the cyber security and sustainable functioning of commercial banks in the digital environment.

Keywords: digital transformation, commercial banks, cyber resilience, cyber security, banking devices, information security, risk management.

Kirish

So‘nggi yillarda raqamli texnologiyalarning jadal rivojlanishi bank sektorida tub institutsional va texnologik o‘zgarishlarni yuzaga keltirmoqda. Tijorat banklarida masofaviy bank xizmatlari, mobil va internet banking, avtomatlashtirilgan bank qurilmalari, shuningdek, raqamli to‘lov tizimlarining keng joriy etilishi moliyaviy xizmatlar ko‘rsatish samaradorligini oshirish bilan birga, bank infratuzilmasining kiberxavflarga nisbatan zaifligini ham kuchaytirmoqda. Raqamli transformatsiya sharoitida bank faoliyatining uzluksizligini ta’minlash, moliyaviy ma’lumotlar va mijozlar axborotining daxlsizligini saqlash masalalari tijorat banklarining kiberbarqarorligini ta’minlash zaruratini yuzaga chiqarmoqda.Tijorat banklarining kiberbarqarorligi bank axborot tizimlari, to‘lov infratuzilmasi va bank qurilmalarining kiberhujumlarga bardoshlilik darajasi, kiberhodisalar oqibatlarini minimallashtirish hamda qisqa muddatda normal faoliyatni tiklash qobiliyati bilan belgilanadi. Bankomatlar, POS-terminallar, serverlar, ma’lumotlar bazalari va mobil ilovalar bank tizimining asosiy texnologik elementlari bo‘lib, ularning ishdan chiqishi yoki noqonuniy buzilishi bank operatsiyalarining to‘xtab qolishiga olib kelishi mumkin. Shu sababli, bank qurilmalarining xavfsizligini ta’minlash va kiberbarqarorlikni boshqarish mexanizmlarini takomillashtirish zamonaviy bank tizimi uchun muhim strategik vazifa hisoblanadi.

O‘zbekiston Respublikasida bank sektorida raqamli texnologiyalarni joriy etish va ularning xavfsizligini ta’minlash masalalari davlat siyosati darajasida belgilangan. Xususan, O‘zbekiston Respublikasi Prezidentining **2020-yil 5-oktabrdagi PF-6079-son “Raqamli O‘zbekiston – 2030 strategiyasini tasdiqlash va uni amalga oshirish chora-tadbirlari to‘g‘risida”gi Farmoni**da raqamli texnologiyalarni iqtisodiyotning barcha sohalariga, jumladan, moliya-bank tizimiga keng joriy etish bilan bir qatorda, axborot va kiberxavfsizlikni ta’minlash muhim vazifalardan biri sifatida belgilangan. Ushbu Farmon bank axborot tizimlarining ishonchliligini oshirish, raqamli

infratuzilmaning barqaror ishlashini ta’minlash hamda kiberxavflarga qarshi himoya choralarini kuchaytirish uchun huquqiy asos bo‘lib xizmat qiladi.Shuningdek, O‘zbekiston Respublikasi Prezidentining **2022-yil 28-yanvardagi PF-60-son “2022–2026-yillarga mo‘ljallangan Yangi O‘zbekistonning taraqqiyot strategiyasi to‘g‘risida”gi Farmoni**da moliya-bank tizimini raqamlashtirish, zamonaviy axborot texnologiyalarini joriy etish va raqamli xizmatlar xavfsizligini ta’minlash ustuvor yo‘nalishlar qatoriga kiritilgan. Mazkur hujjatda axborot tizimlarining barqaror ishlashini ta’minlash, kiberxavflarni boshqarish va muhim axborot infratuzilmasi obyektlarini himoyalash masalalariga alohida e’tibor qaratilgan bo‘lib, bu talablar bevosita tijorat banklari faoliyatiga tatbiq etiladi.

Bank sektorida kiberxavfsizlikni ta’minlashning huquqiy asoslaridan biri sifatida **“Axborotlashtirish to‘g‘risida”gi O‘zbekiston Respublikasi Qonuni (2023-yilgi yangi tahrir)** alohida ahamiyat kasb etadi. Ushbu Qonunda axborot resurslari va axborot tizimlarini himoyalash, ruxsatsiz kirish va noqonuniy aralashuvlarning oldini olish, shuningdek, axborot xavfsizligini ta’minlash bo‘yicha subyektlarning majburiyatlari belgilangan. Bank axborot tizimlari va qurilmalari mazkur Qonun doirasida muhim axborot resurslari sifatida e’tirof etilib, ularning kiberxavfsizligini ta’minlash majburiy hisoblanadi.Amaliy statistik ma’lumotlar ham bank sektorida kiberbarqarorlik masalasining dolzarbligini ko‘rsatmoqda.

O‘zbekiston Respublikasi Markaziy bankining ochiq statistik ma’lumotlariga ko‘ra, mamlakatda muomalada bo‘lgan bank kartalari soni 40 milliondan ortiqni tashkil etib, ular orqali amalga oshirilayotgan naqd pulsiz to‘lovlar hajmi yil sayin sezilarli darajada oshib bormoqda. Mobil va internet banking xizmatlaridan foydalanuvchilar sonining keskin ko‘payishi bank axborot tizimlariga tushayotgan yuklamani kuchaytirib, ularning kiberbardoshliligini ta’minlash zaruratini yanada oshirmoqda.

Tijorat banklarida axborot tizimlari va bank qurilmalarining xavfsizligini ta’minlashda O‘zbekiston Respublikasi Markaziy bankining me’yoriy-huquqiy hujjatlari muhim rol o‘ynaydi. Markaziy bank tomonidan belgilangan axborot

xavfsizligi talablari banklarda xavfsizlik siyosatini ishlab chiqish, kiberxavflarni monitoring qilish, texnik va tashkiliy himoya choralarini joriy etishni nazarda tutadi. Shuningdek, Markaziy bank huzurida faoliyat yurituvchi **CERT-CBU (Computer Emergency Response Team)** bank tizimida kiberhodisalarni aniqlash, tahlil qilish va ularga tezkor javob berish orqali tijorat banklarining kiberbarqarorligini oshirishga xizmat qilmoqda.Raqamli transformatsiya sharoitida tijorat banklarining kiberbarqarorligini ta’minlash mexanizmlarini samarali boshqarish bank risk-menejmenti, axborot xavfsizligi siyosati va strategik boshqaruv tizimlari bilan uzviy bog‘liqdir. Bank qurilmalarining xavfsizligini ta’minlash, kiberxavflarni oldindan aniqlash va ularning salbiy oqibatlarini kamaytirishga qaratilgan kompleks yondashuvlarni joriy etish bank tizimining barqaror faoliyat yuritishini ta’minlashda muhim ahamiyat kasb etadi.

Bank tizimlarining raqamli xizmatlarga o‘tishi kiberxavfsizlik tajovuzlarining global darajada tez sur’atlarda ko‘payishiga sabab bo‘lmoqda. Jahon miqyosida moliyaviy xizmatlar sohasida ransomware (talab pul to‘lashga majbur qiluvchi) hujumlar 2024-yilda taxminan **65 %** moliyaviy tashkilotlarga ta’sir ko‘rsatgan, bu 2021-yilda qayd etilgan **34 %** ko‘rsatkichdan keskin yuqori ekanligi qayd etilgan. Bundan tashqari, finans sohasida 2024-yilda tahdidlar soni **1,338,357 dan ortiq banking trojan hujumlari** aniqlangan va bu global moliyaviy sektor foydalanuvchilari uchun onlayn tahdidlarning jiddiyligini ko‘rsatadi.

Mahalliy statistika ham bu tendensiyani tasdiqlaydi: 2024-yilda O‘zbekiston bo‘yicha **58,800 dan ortiq kiberjinoyat holatlari** rasmiy qayd etilgan bo‘lib, ularning 97,7 %i bank kartalaridan noqonuniy mablag‘ yechib olish bilan bog‘liq bo‘lgan. Shuningdek, O‘zbekiston bo‘yicha **2024-yilda 12 milliondan ortiq kiberhujum urinishlari** qayd etilgan bo‘lib, bu 2023-yil bilan solishtirganda yanada ko‘paygan ko‘rsatkichlarni anglatadi. Bu holat, bank tizimlarining tez raqamlashtirilayotgani va kiberhujumlar ko‘lamining global tendentsiyalarga uyg‘un ravishda oshayotganini ko‘rsatadi.

Mahalliy statistika kiberxavfsizlikning bank tizimiga bo‘lgan ta’sirini ham oydinlashtiradi: masalan, 2025-yil yozida Jizzax mintaqasidagi tijorat banklaridan birining mobil ilovasiga qilingan kiberhujum natijasida mijozlar depozit hisobidan **taxminan 3 milliard so‘m noqonuniy mablag‘ yechib olingan** holat ham qayd etildi, bu bank infratuzilmasining xavfsizlik zaifliklarini amaliy misol orqali ko‘rsatadi.

Xorijiy tajribalarda ham moliyaviy sektor uchun cyberxavflar tobora keng tarqalayapti. Masalan, AQShdagi yirik moliyaviy institutlarning 97 %i 2024-yilda uchinchi tomon tarmog‘i orqali buzilish holatlarini boshdan kechirgan, shu bilan birga kiberhujumlar soni 2023-yilga nisbatan 109 %ga oshgani qayd etilgan. Bu ko‘rsatkichlar tijorat banklarining global miqyosda xavfsizlik zanjirida zaif nuqtalar mavjudligini va kiberbarqarorlikni oshirish zaruratini ko‘rsatadi.

Yevropa Ittifoqining kibertahdidlar bo‘yicha hisobotida kredit muassasalari moliyaviy xizmatlar ichida eng ko‘p kiberhodisalarga duch keladigan sektor ekanligi, kredit uyushmalari va banklarda **300 dan ortiq** huquqbuzarliklar qayd etilgani tasdiqlangan. Bu raqamlar bank infratuzilmasining strategik muhim obyekti sifatida global iqtisodiyotda kiberxavfsizlikning ustuvorligini ta’kidlaydi.

Bundan tashqari, statistik tadqiqotlar moliyaviy sektorning cyberxavfsizlik turida yuzaga kelayotgan yo‘qotishlarni ham aniqlaydi; masalan, 2024-yilda moliyaviy soha ma’lumotlar buzilishi bo‘yicha o‘rtacha zarar **6,08 million AQSh dollarini** tashkil etgan, bu o‘tgan yillardagi ko‘rsatkichlardan oshgan.

Xalqaro tajriba shuni ko‘rsatadiki, bank sektorida kiberbarqarorlikni oshirish bo‘yicha yuqori samarali choralar quyidagi yo‘nalishlarni o‘z ichiga oladi: ko‘p bosqichli autentifikatsiya (multi-factor authentication), sun’iy intellekt yordamida xato va shubhali tranzaksiyalarni avtomatik aniqlash, mustahkam shifrlash protokollari, muntazam ichki va tashqi auditlar, shuningdek yetkazib beruvchilarning xavfsizlik darajasini baholash.

Xorijiy tajriba shuni ko‘rsatadiki, tijorat banklarida kiberbarqarorlikni oshirishda tizimli va standartlarga asoslangan yondashuv muhim ahamiyat kasb etadi. Masalan, Yevropa Ittifoqida 2025-yildan kuchga kirayotgan **DORA (Digital**

Operational Resilience Act) talablari banklardan muhim axborot tizimlarining uzluksiz ishlashini ta’minlash, kiberhodisalarga tayyorgarlik darajasini sinovdan o‘tkazish va uchinchi tomon IT-provayderlari risklarini qat’iy nazorat qilishni talab etadi. AQSh Federal zaxira tizimi ma’lumotlariga ko‘ra, yirik banklarda kiberxavfsizlikka yo‘naltirilgan yillik investitsiyalar bankning umumiy IT-byudjetining o‘rtacha **10–15 foizini** tashkil etmoqda, bu esa kiberbarqarorlikni strategik ustuvor yo‘nalish sifatida qaralayotganini ko‘rsatadi. Osiyo mamlakatlarida, xususan Singapur banklarida real vaqt rejimida tranzaksiyalarni tahlil qiluvchi sun’iy intellekt tizimlari joriy etilishi natijasida firibgarlik bilan bog‘liq yo‘qotishlar **30 foizdan ortiq** qisqargani qayd etilgan. Ushbu xorijiy amaliyotlar raqamli transformatsiya sharoitida bank qurilmalarining xavfsizligini ta’minlash va kiberbarqarorlikni boshqarish mexanizmlarini takomillashtirish zarurligini yana bir bor tasdiqlaydi.

1-jadval

Tijorat banklarida kiberbarqarorlikni ta’minlash bo‘yicha xorijiy tajriba va asosiy ko‘rsatkichlar

Mamlakat / Hudud	Asosiy normativ hujjat yoki yondashuv	Amaliy choralar	Statistik natijalar
Yevropa Ittifoqi	Digital Operational Resilience Act (DORA, 2025)	IT-tizimlar uzluksizligini testdan o‘tkazish, uchinchi tomon risklarini nazorat qilish	Moliyaviy sektorda yirik kiberuzilishlar soni 2023–2024 yillarda 20 % ga kamaygan
AQSh	Federal Reserve va NIST Cybersecurity Framework	Ko‘p bosqichli autentifikatsiya, doimiy kiberxavfsizlik auditlari	Banklarda IT-byudjetning 10–15 % kiberxavfsizlikka yo‘naltiriladi
Buyuk Britaniya	Operational Resilience Framework (FCA)	Muhim biznes xizmatlarini identifikatsiya qilish va stress-testlar	Kiberhodisalardan tiklanish vaqti o‘rtacha 35 % ga qisqargan
Singapur	Monetary Authority of Singapore (MAS) Technology Risk Management Guidelines	Sun’iy intellekt asosida tranzaksiyalarni real vaqt rejimida monitoring qilish	Firibgarlik bilan bog‘liq yo‘qotishlar 30 % dan ortiq kamaygan
Yaponiya	Financial Services Agency (FSA) Cybersecurity Policy	Bank qurilmalarida majburiy shifrlash va apparat darajasida himoya	Bank qurilmalariga ruxsatsiz kirish holatlari 25 % ga qisqargan

Jadvalda tijorat banklarida kiberbarqarorlikni ta’minlash bo‘yicha yetakchi xorijiy mamlakatlar va hududlar tajribasi umumlashtirilgan. Jadvalda har bir mamlakat yoki mintaqa bo‘yicha kiberxavfsizlikni tartibga soluvchi asosiy normativ hujjatlar, amaliy boshqaruv va texnologik choralar hamda ularning natijasida erishilgan aniq statistik ko‘rsatkichlar keltirilgan. Xususan, Yevropa Ittifoqida DORA reglamenti orqali bank axborot tizimlarining operatsion barqarorligini oshirishga qaratilgan talablar joriy etilgani, AQShda esa kiberxavfsizlikka ajratilayotgan IT-byudjet ulushining yuqori darajasi banklar uchun kiberbarqarorlikning strategik ahamiyatga ega ekanini ko‘rsatadi. Singapur va Yaponiya tajribasi zamonaviy raqamli texnologiyalar hamda apparat darajasidagi himoya choralarini qo‘llash bank qurilmalariga qaratilgan kiberxavflarni sezilarli kamaytirishga xizmat qilayotganini tasdiqlaydi. Umuman olganda, jadvalda keltirilgan ma’lumotlar kiberbarqarorlikni ta’minlashda normativ talablar, boshqaruv mexanizmlari va ilg‘or texnologiyalar uyg‘unligining muhimligini yaqqol namoyon etadi.

Raqamli transformatsiya jarayonida tijorat banklarining kiberbarqarorligini ta’minlash masalasi bank risklarini boshqarish tizimi bilan chambarchas bog‘liq bo‘lib, u moliyaviy, operatsion va reputatsion risklarning oldini olishga xizmat qiladi. Kiberhodisalar natijasida bank operatsiyalarining to‘xtab qolishi, mijozlar ma’lumotlarining oshkor bo‘lishi yoki moliyaviy yo‘qotishlarning yuzaga kelishi bank barqarorligiga bevosita salbiy ta’sir ko‘rsatadi. Shu sababli, rivojlangan mamlakatlar tajribasida kiberxavfsizlik masalalari bank strategiyasining ajralmas qismi sifatida ko‘rilib, kiberxavflar alohida risk kategoriyasi sifatida baholanadi va doimiy monitoring qilinadi.

Xalqaro amaliyot shuni ko‘rsatadiki, kiberbarqarorlikni ta’minlashda bank qurilmalarining texnik holati va dasturiy ta’minotning yangilanish darajasi muhim rol o‘ynaydi. Bankomatlar va POS-terminallar uchun muntazam ravishda xavfsizlik yangilanishlarini o‘rnatish, eski protokollardan voz kechish hamda apparat darajasida himoya mexanizmlarini qo‘llash kiberxavflarni sezilarli darajada kamaytiradi. Masalan, rivojlangan bank tizimlarida bank qurilmalarining ishlash holati real vaqt

rejimida monitoring qilinib, shubhali faollik aniqlangan taqdirda qurilma avtomatik tarzda tarmoqdan uziladi. Bunday yondashuv kiberhujumlarning keng ko‘lamda tarqalishini cheklash imkonini beradi.

Shuningdek, inson omili tijorat banklarining kiberbarqarorligiga ta’sir etuvchi muhim faktor hisoblanadi. Xorijiy tadqiqotlar natijalariga ko‘ra, moliyaviy sektordagi kiberhodisalarning katta qismi xodimlarning bexosdan yo‘l qo‘ygan xatolari yoki fishing hujumlariga aldanishi bilan bog‘liq. Shu bois, banklarda axborot xavfsizligi bo‘yicha xodimlar malakasini oshirish, muntazam treninglar va simulyatsiya mashg‘ulotlarini o‘tkazish kiberxavflarni kamaytirishning samarali vositasi sifatida qaraladi. Raqamli transformatsiya sharoitida kiberxavfsizlik madaniyatini shakllantirish bank qurilmalarining texnik himoyasi bilan bir qatorda muhim ahamiyat kasb etadi.

Bundan tashqari, uchinchi tomon texnologik provayderlari bilan bog‘liq risklar ham banklarning kiberbarqarorligiga jiddiy ta’sir ko‘rsatmoqda. Bulutli xizmatlar, to‘lov platformalari va tashqi IT-xizmatlardan foydalanish bank faoliyatini yanada samarali qilsa-da, ular orqali yuzaga keladigan kiberxavflar bank nazoratidan tashqarida bo‘lishi mumkin. Shu sababli, xorijiy bank amaliyotida uchinchi tomon risklarini baholash, ularning axborot xavfsizligi darajasini tekshirish va shartnomaviy majburiyatlar orqali xavfsizlik talablarini belgilash keng qo‘llanilmoqda. Bu yondashuv bank infratuzilmasining umumiy kiberbarqarorligini mustahkamlashga xizmat qiladi.

Xulosa

Raqamli transformatsiya sharoitida tijorat banklari faoliyatining tobora raqamli platformalar va avtomatlashtirilgan bank qurilmalariga tayanib borishi bank tizimining kiberxavflarga nisbatan sezgirligini oshirmoqda. Bankomatlar, POS-terminallar, mobil va internet banking tizimlari, shuningdek, markazlashtirilgan axborot tizimlari bank infratuzilmasining asosiy tarkibiy qismlariga aylangan bir sharoitda ularning uzluksiz va xavfsiz ishlashini ta’minlash bank barqarorligining muhim sharti hisoblanadi. Tadqiqot davomida keltirilgan statistik ma’lumotlar va xorijiy tajribalar bank sektorida

kiberbarqarorlik masalasining nafaqat texnik, balki strategik va boshqaruv darajasidagi muammo ekanini ko‘rsatdi.

Tahlillar shuni ko‘rsatadiki, tijorat banklarining kiberbarqarorligini ta’minlash faqat alohida texnik himoya vositalarini joriy etish bilan cheklanmaydi, balki kompleks boshqaruv mexanizmlarini shakllantirishni talab etadi. Xususan, kiberxavflarni bank risk-menejment tizimiga integratsiya qilish, bank qurilmalarining texnik va dasturiy holatini doimiy monitoring qilish, kiberhodisalarga tezkor javob berish va faoliyatni tiklash rejalarini ishlab chiqish muhim ahamiyat kasb etadi. Xalqaro amaliyotda qo‘llanilayotgan DORA, NIST, MAS kabi yondashuvlar bank tizimida kiberbarqarorlikni oshirishda normativ talablar, texnologik yechimlar va tashkiliy choralar uyg‘unligini ta’minlash zarurligini tasdiqlaydi.

Shuningdek, inson omili va uchinchi tomon provayderlari bilan bog‘liq risklar banklarning kiberbarqarorligiga sezilarli ta’sir ko‘rsatishi aniqlanadi. Xodimlarning axborot xavfsizligi bo‘yicha malakasini oshirish, kiberxavfsizlik madaniyatini shakllantirish va tashqi IT-xizmatlar xavfsizligini baholash mexanizmlarini joriy etish bank qurilmalarining umumiy xavfsizlik darajasini oshirishga xizmat qiladi. Shu bilan birga, Markaziy bank tomonidan belgilangan axborot xavfsizligi talablari va CERT-CBU faoliyati tijorat banklarining kiberbarqarorligini institutsional jihatdan qo‘llab-quvvatlashda muhim o‘rin tutadi.

Takliflar

Raqamli transformatsiya sharoitida tijorat banklarining kiberbarqarorligini ta’minlash va bank qurilmalarining xavfsizligini mustahkamlash maqsadida quyidagi ilmiy-amaliy takliflarni ilgari surish maqsadga muvofiq deb hisoblanadi.

Birinchidan, tijorat banklarida kiberbarqarorlikni alohida strategik yo‘nalish sifatida shakllantirish va uni bankning umumiy rivojlanish strategiyasiga integratsiya qilish zarur. Bunda kiberxavflar bank risk-menejment tizimida mustaqil risk turi sifatida baholanib, ularni aniqlash, baholash va monitoring qilish mexanizmlarini kuchaytirish tavsiya etiladi. Bu bank faoliyatining uzluksizligini ta’minlash va

kiberhodisalarning moliyaviy hamda reputatsion salbiy oqibatlarini kamaytirishga xizmat qiladi.

Ikkinchidan, bank qurilmalarining xavfsizligini ta’minlash maqsadida bankomatlar va POS-terminallar uchun yagona texnik va dasturiy xavfsizlik standartlarini joriy etish maqsadga muvofiqdir. Xususan, bank qurilmalarida apparat darajasida shifrlash, muntazam xavfsizlik yangilanishlarini avtomatik o‘rnatish va real vaqt rejimida monitoring tizimlaridan foydalanishni kengaytirish zarur. Bu chora-tadbirlar bank qurilmalariga qaratilgan zararli dasturlar va ruxsatsiz aralashuvlar xavfini sezilarli darajada kamaytiradi.

Uchinchidan, tijorat banklarida kiberhodisalarga tezkor javob berish va faoliyatni tiklash mexanizmlarini takomillashtirish tavsiya etiladi. Buning uchun favqulodda holatlar bo‘yicha aniq reglamentlar ishlab chiqish, muntazam stress-testlar va kiberhujum ssenariylari asosida mashg‘ulotlar o‘tkazish zarur. Ushbu yondashuv bank tizimining kiberhujumlarga bardoshliligini oshirish va tiklanish vaqtini qisqartirish imkonini beradi.

To‘rtinchidan, inson omilidan kelib chiqadigan kiberxavflarni kamaytirish maqsadida bank xodimlari uchun axborot xavfsizligi va kiberxavfsizlik bo‘yicha doimiy o‘quv-trening dasturlarini joriy etish muhim hisoblanadi. Xodimlarda kiberxavfsizlik madaniyatini shakllantirish, fishing va ijtimoiy muhandislik hujumlarini aniqlash ko‘nikmalarini rivojlantirish bank axborot tizimlari va qurilmalarining umumiy xavfsizlik darajasini oshiradi.

Beshinchidan, uchinchi tomon IT-provayderlari va to‘lov platformalari bilan bog‘liq kiberxavflarni boshqarish mexanizmlarini kuchaytirish lozim. Bunda tashqi xizmat ko‘rsatuvchi tashkilotlarning axborot xavfsizligi darajasini baholash, ular bilan tuziladigan shartnomalarda kiberxavfsizlik bo‘yicha majburiy talablarni belgilash hamda doimiy audit tizimini joriy etish bank infratuzilmasining umumiy kiberbarqarorligini ta’minlashga xizmat qiladi.

Umuman olganda, taklif etilgan chora-tadbirlarni izchil amalga oshirish tijorat banklarining kiberbarqarorligini oshirish, bank qurilmalarining xavfsizligini

ta’minlash hamda raqamli transformatsiya sharoitida bank tizimining barqaror va ishonchli faoliyat yuritishini ta’minlashga imkon beradi.

FOYDALANILGAN ADABIYOTLAR

1. O‘zbekiston Respublikasi Prezidenti. **Raqamli O‘zbekiston – 2030 strategiyasini tasdiqlash va uni amalga oshirish chora-tadbirlari to‘g‘risida** : PF-6079-son Farmon. — Toshkent, 2020-yil 5-oktabr.

2. O‘zbekiston Respublikasi Prezidenti. **2022–2026-yillarga mo‘ljallangan Yangi O‘zbekistonning taraqqiyot strategiyasi to‘g‘risida** : PF-60-son Farmon. — Toshkent, 2022-yil 28-yanvar.

3. O‘zbekiston Respublikasi. **Axborotlashtirish to‘g‘risida** : O‘zbekiston Respublikasi Qonuni (yangi tahrir). — Toshkent, 2023.

4. O‘zbekiston Respublikasi Markaziy banki. **To‘lov tizimlari va banklarda axborot xavfsizligiga qo‘yiladigan talablar to‘g‘risida nizom**. — Toshkent : Markaziy bank, 2022.

5. Mamadiyarov Z., Karshiev D. **Cybersecurity in digital banking: safeguarding customer trust in Uzbekistan** // American Journal of Corporate Management. — 2024. — Vol. 1, №2. — B. 33–47.

6. Shirinova S. **Cybersecurity risks in the context of digitalization of the banking industry in the Republic of Uzbekistan** // Proceedings of ACM International Conference. — 2023. — B. 112–118.

7. Basel Committee on Banking Supervision. **Principles for operational resilience**. — Basel : Bank for International Settlements, 2021.

8. European Union. **Digital Operational Resilience Act (DORA)**. — Brussels : Official Journal of the European Union, 2022.

9. National Institute of Standards and Technology. **Cybersecurity Framework 2.0**. — Gaithersburg : NIST, 2024.

10. IBM Security. **Cost of a data breach report 2024**. — Armonk : IBM Corporation, 2024.