

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

Urmonova Gulmiraxon Muhammadovna

So'nggi yillarda global moliya tizimida raqamli transformatsiya jarayonlari jadal rivojlanib, tijorat banklari faoliyatida innovatsion texnologiyalarni keng joriy etish zaruratini yuzaga keltirdi. Masofaviy bank xizmatlari, mobil va internet-banking, sun'iy intellekt, bulutli texnologiyalar hamda "Big Data" yechimlari bank operatsiyalarining samaradorligini oshirish bilan birga, axborot xavfsizligi va kiberxavflar bilan bog'liq yangi tahdidlarni ham paydo qilmoqda. Shu bois raqamli transformatsiya sharoitida tijorat banklarining kiberbarqarorligini ta'minlash va bank qurilmalarining xavfsizligini boshqarish dolzarb masalaga aylandi. Kiberbarqarorlik bank tizimining kiberhujumlar, texnik nosozliklar va favqulodda holatlarga nisbatan barqarorligini saqlash, uzluksiz faoliyatni ta'minlash hamda mijozlar ma'lumotlarini himoya qilishni nazarda tutadi. Ushbu tezisda tijorat banklarida kiberbarqarorlikni ta'minlash mexanizmlarini boshqarish, bank qurilmalari xavfsizligini kuchaytirish va zamonaviy xavfsizlik yondashuvlarini joriy etish masalalari tahlil qilinadi.

Raqamli transformatsiya bank faoliyatining barcha yo'nalishlarini qamrab olib, operatsion jarayonlarni avtomatlashtirish, xizmatlar tezligini oshirish va mijozlar bilan aloqalarni takomillashtirishga xizmat qiladi. Biroq bank infratuzilmasining raqamlashtirilishi kiberjinoyatchilar uchun yangi imkoniyatlar yaratmoqda. Phishing, zararli dasturlar, DDoS hujumlar, ma'lumotlar sizib chiqishi va ichki xodimlar bilan bog'liq xavflar bank tizimi uchun asosiy tahdidlar hisoblanadi. Tijorat banklarida kiberxavfsizlik muammolari, avvalo, murakkab IT-infratuzilma, ko'p sonli foydalanuvchilar va turli bank qurilmalarining (bankomatlar, POS-terminallar, serverlar, mobil qurilmalar) mavjudligi bilan bog'liq. Har bir qurilma potensial zaiflik manbai bo'lib, ularning himoyasi yetarli darajada ta'minlanmasa, butun bank tizimi xavf ostida qolishi mumkin.

Kiberbarqarorlikni ta'minlash mexanizmlarini samarali boshqarish tizimli va kompleks yondashuvni talab etadi. Avvalo, banklarda axborot xavfsizligi siyosati ishlab chiqilib, u xalqaro standartlar va milliy me'yoriy-huquqiy hujjatlarga muvofiq bo'lishi lozim. Ushbu siyosat bankning barcha bo'linmalarida majburiy ravishda qo'llanilishi kerak.

Ikkinchidan, risklarni boshqarish tizimini takomillashtirish muhim ahamiyatga ega. Kiberxavflarni aniqlash, baholash va ularning oldini olish bo'yicha muntazam monitoring olib borilishi zarur. Bu jarayonda avtomatlashtirilgan xavfsizlik

monitoringi tizimlari va real vaqt rejimida ishlovchi himoya vositalaridan foydalanish samarali natija beradi.

Uchinchidan, inson omilini hisobga olish kiberbarqarorlikning muhim jihatlaridan biridir. Bank xodimlarining axborot xavfsizligi bo'yicha bilim va ko'nikmalarini oshirish, ularni muntazam trening va seminarlar orqali xabardor qilish kiberhujumlar ehtimolini sezilarli darajada kamaytiradi. Chunki ko'plab kiberhodisalar aynan xodimlarning ehtiyotsizligi yoki bilim yetishmasligi sababli yuzaga keladi.

Bank qurilmalari xavfsizligi raqamli transformatsiya sharoitida alohida e'tibor talab qiladigan yo'nalish hisoblanadi. Bankomatlar, POS-terminallar va mobil qurilmalar bank tizimining tashqi muhit bilan bevosita aloqada bo'lgan qismlari bo'lib, ular orqali kiberhujumlar amalga oshirilishi mumkin. Bank qurilmalarining xavfsizligini ta'minlash uchun ularni muntazam ravishda yangilab borish, zaifliklarni aniqlash va bartaraf etish zarur. Shuningdek, qurilmalarda ishlatiladigan dasturiy ta'minot litsenziyalangan va ishonchli bo'lishi shart. Shifrlash texnologiyalaridan foydalanish, autentifikatsiya va avtorizatsiya mexanizmlarini kuchaytirish bank qurilmalarining himoyasini oshiradi. Bundan tashqari, bank qurilmalarini markazlashtirilgan boshqaruv tizimiga ulash orqali ularning holatini masofadan nazorat qilish, nosozliklarni tezkor aniqlash va xavfsizlik hodisalariga tezkor javob berish imkoniyati yaratiladi.

Zamonaviy sharoitda tijorat banklarida kiberbarqarorlikni boshqarishda ilg'or texnologiyalar va innovatsion yondashuvlardan foydalanish muhimdir. Sun'iy intellekt va mashinaviy o'rganish asosidagi xavfsizlik tizimlari kiberhujumlarni oldindan aniqlash va ularning oqibatlarini kamaytirishda katta imkoniyatlar yaratmoqda. Bulutli texnologiyalar asosida yaratilgan zaxira tizimlari va ma'lumotlarni tiklash mexanizmlari bank faoliyatining uzluksizligini ta'minlashga xizmat qiladi. Shu bilan birga, "Zero Trust" konsepsiyasini joriy etish orqali har bir foydalanuvchi va qurilmaga nisbatan doimiy tekshiruv olib borish bank tizimining umumiy xavfsizligini oshiradi.

Shuningdek, tijorat banklarida kiberbarqarorlikni ta'minlash jarayonida tashkiliy boshqaruv mexanizmlarini takomillashtirish muhim ahamiyat kasb etadi. Banklarda axborot xavfsizligi uchun mas'ul bo'lgan alohida bo'linmalar faoliyatini kuchaytirish, ularning vakolatlarini aniq belgilash hamda strategik qarorlar qabul qilish jarayoniga faol jalb etish zarur. Kiberxavfsizlik masalalari faqat texnik yo'nalish sifatida emas, balki bankning umumiy boshqaruv strategiyasining ajralmas qismi sifatida ko'rilishi lozim. Bu yondashuv kiberxavflarga nisbatan tezkor va samarali javob berish imkonini yaratadi.

Raqamli transformatsiya sharoitida banklar faoliyatida katta hajmdagi ma'lumotlar bilan ishlash hajmi ortib borayotgani sababli ma'lumotlarni himoyalash masalasi alohida dolzarblik kasb etadi. Mijozlarning shaxsiy va moliyaviy ma'lumotlarini himoyalash bank obro'si va ishonchliligining asosiy omillaridan biri

hisoblanadi. Shu nuqtayi nazardan, ma'lumotlarni saqlash va uzatishda zamonaviy kriptografik himoya vositalaridan foydalanish, ma'lumotlarga kirishni qat'iy tartibga solish va audit mexanizmlarini joriy etish talab etiladi. Ma'lumotlar bazalariga ruxsatsiz kirish holatlarini oldini olish orqali banklar nafaqat moliyaviy zararlarning, balki huquqiy va reputatsion xavflarning ham oldini oladi.

Bank infratuzilmasining muhim qismi hisoblangan tarmoq xavfsizligini ta'minlash ham kiberbarqarorlikning asosiy yo'nalishlaridan biridir. Ichki va tashqi tarmoqlar o'rtasida himoya devorlarini (firewall), hujumlarni aniqlash va oldini olish tizimlarini qo'llash, tarmoq trafigini doimiy monitoring qilish bank tizimining himoyalanganlik darajasini oshiradi. Ayniqsa, masofaviy ishlash va mobil bank xizmatlarining kengayishi sharoitida tarmoq xavfsizligini kuchaytirish strategik ahamiyatga ega bo'lib bormoqda.

Kiberhodisalarga tayyorgarlik va ularga javob berish mexanizmlarini ishlab chiqish ham muhim masala hisoblanadi. Har qanday xavfsizlik tizimi mutlaq himoyani kafolatlamaganligi sababli, kiberhujumlar sodir bo'lgan taqdirda bank faoliyatini tezkor tiklash mexanizmlari mavjud bo'lishi lozim. Favqulodda holatlar rejaları, zaxira ma'lumotlar markazlari va uzluksiz faoliyatni ta'minlash rejalarining mavjudligi bank tizimining kiberbarqarorligini mustahkamlaydi. Ushbu rejalar muntazam ravishda sinovdan o'tkazilib, amaliyotda tekshirib borilishi maqsadga muvofiqdir.

Xalqaro tajriba shuni ko'rsatadiki, tijorat banklarining kiberbarqarorligini ta'minlashda davlat va xususiy sektor hamkorligi muhim rol o'ynaydi. Markaziy banklar, nazorat organlari va tijorat banklari o'rtasida axborot almashinuvi, umumiy standartlar va talablarning joriy etilishi kiberxavflarga qarshi kurash samaradorligini oshiradi. Shu bilan birga, xalqaro xavfsizlik standartlariga moslashish va ilg'or tajribalarni tatbiq etish bank tizimining raqobatbardoshligini kuchaytiradi.

Umuman olganda, raqamli transformatsiya jarayonlari tijorat banklari uchun yangi imkoniyatlar bilan bir qatorda jiddiy kiberxavflarni ham yuzaga keltirmoqda. Ushbu sharoitda kiberbarqarorlikni ta'minlash mexanizmlarini samarali boshqarish, bank qurilmalarining xavfsizligini mustahkamlash va zamonaviy texnologiyalardan oqilona foydalanish bank tizimining barqaror rivojlanishini ta'minlaydi. Kiberxavfsizlikka tizimli yondashuv banklarning moliyaviy barqarorligi, mijozlar ishonchi va umumiy iqtisodiy xavfsizlikni ta'minlashda muhim omil bo'lib xizmat qiladi.

Raqamli muhitda tijorat banklari faoliyatining kengayib borishi tashqi provayderlar va texnologik hamkorlarga bo'lgan bog'liqlikni kuchaytirmoqda. Shu sababli uchinchi tomonlar bilan bog'liq kiberxavflarni boshqarish masalasi alohida ahamiyat kasb etadi. Dasturiy ta'minot yetkazib beruvchilar, bulutli xizmatlar provayderlari va texnik servis ko'rsatuvchi tashkilotlarning axborot xavfsizligi darajasini baholash, ular bilan tuziladigan shartnomalarda xavfsizlik talablarini qat'iy

belgilash bank tizimining umumiy kiberbarqarorligini oshiradi. Ushbu jarayonda yetkazib beruvchilarni tanlash va monitoring qilish mexanizmlarini kuchaytirish muhim hisoblanadi.

Shu bilan birga, raqamli bank xizmatlaridan foydalanuvchi mijozlarning axborot xavfsizligi madaniyatini oshirish ham kiberxavflarni kamaytirishda muhim omil sanaladi. Mijozlarning shaxsiy ma'lumotlarini himoyalash qoidalari, xavfsiz parollardan foydalanish, shubhali havolalar va xabarlar orqali amalga oshiriladigan firibgarliklardan ogoh bo'lishi bank tizimi xavfsizligiga bevosita ta'sir ko'rsatadi. Tijorat banklari tomonidan mijozlar uchun axborot-kengash xizmatlarini yo'lga qo'yish, ogohlantiruvchi bildirishnomalar va ta'limiy materiallar taqdim etish kiberxavfsizlikni mustahkamlashga xizmat qiladi.

Kelgusida tijorat banklarining kiberbarqarorligini ta'minlash jarayonida innovatsion yondashuvlar va raqamli texnologiyalarning roli yanada ortib boradi. Kiberxavflarning murakkablashuvi banklardan doimiy ravishda xavfsizlik strategiyalarini yangilab borishni, moslashuvchan va prognozli boshqaruv mexanizmlarini joriy etishni talab qiladi. Shu jihatdan, raqamli transformatsiya sharoitida kiberbarqarorlikni ta'minlash banklar faoliyatining uzluksizligi va barqaror rivojlanishini ta'minlovchi muhim strategik yo'nalish sifatida namoyon bo'ladi.

Foydalanilgan adabiyotlar

1. O'zbekiston Respublikasi Markaziy banki. Tijorat banklarida axborot xavfsizligi va kiberxavfsizlikni ta'minlashga oid me'yoriy talablar : me'yoriy hujjat. – Toshkent : O'zbekiston Respublikasi Markaziy banki, 2022. – 45 b.
2. Abdurahmonov A.A. Raqamli bank xizmatlari sharoitida moliya tizimi xavfsizligini ta'minlash masalalari // Iqtisodiyot va innovatsion texnologiyalar : ilmiy elektron jurnal. – 2023. – № 4. – B. 112–118.
3. Kozyrev A.N. Kiberbezopasnost bankovskix sistem v usloviyax tsifrovoy transformatsii : monografiya. – Moskva : Yurayt, 2021. – 256 b.
4. Fedorova E.A. Upravleniye kiberriskami v finansovix organizatsiyax : o'quv qo'llanma. – Moskva : Finansy i statistika, 2022. – 240 b.
5. Anderson R. Security Engineering: A Guide to Building Dependable Distributed Systems. – 3rd ed. – Hoboken, NJ : Wiley, 2021. – 1248 p.
6. Schneier B. Click Here to Kill Everybody: Security and Survival in a Hyper-connected World. – New York : W. W. Norton & Company, 2023. – 352 p.