

TIJORAT BANKLARI AVTOMATLASHTIRILGAN HISOB TIZIMLARIDA AXBOROTNI MUHOFAZA QILISH VA UNING NAZORATINI TAKOMILLASHTIRISH (“IPOTEKA BANK” ATB MISOLIDA)

Hudoyberdiev Azizbek Anvarjon o'g'li

O'zbekiston Respublikasi

Bank-moliya akademiyasi 2-kurs tinglovchisi

Hudoyberdievazizbek123@gmail.com

<https://doi.org/10.5281/zenodo.17096936>

Tijorat banklari raqamli iqtisodiyot sharoitida moliyaviy barqarorlik, mijozlar ishonchi va operatsion xavfsizlikni ta'minlashda muhim iqtisodiy institutlar hisoblanadi. Ayniqsa, raqamlashtirish jarayonlari bank xizmatlarini tezkor, ommabop va masofaviy shakllarda taklif qilish imkonini bergani sababli, avtomatlashtirilgan hisob tizimlarining samaradorligi bilan bir qatorda, ushbu tizimlar orqali shakllanadigan axborotlarning xavfsizligi va ularning ustidan doimiy nazoratni ta'minlash masalalari ham dolzarb ahamiyat kasb etmoqda.

Avtomatlashtirilgan hisob tizimlari orqali moliyaviy operatsiyalarni yuritish, real vaqt rejimida tranzaksiyalarni nazorat qilish, hisobotlar shakllantirish va strategik qarorlar qabul qilish imkoniyatlari bank faoliyatini yuqori darajaga olib chiqmoqda. Biroq, bu imkoniyatlar bilan bir qatorda, axborotning sizib chiqishi, ruxsatsiz kirish, xakerlik hujumlari, ichki xodimlar tomonidan ma'lumotlarning suiste'mol qilinishi kabi kiberxavf tahdidlari ham ortmoqda. Shu sababli, har qanday bank faoliyatining zamonaviy infratuzilmasida axborot xavfsizligini ta'minlash va uni nazorat qilish mexanizmlarini kuchaytirish asosiy vazifalardan biri hisoblanadi.

“Ipoteka Bank” ATB misolida olib borilgan amaliy kuzatuvlar va statistik tahlillar shuni ko'rsatdiki, bankning avtomatlashtirilgan hisob tizimlari orqali yuritilayotgan operatsiyalarda aniqlik darajasi yuqori bo'lishiga qaramay, ayrim bo'limlarda (ayniqsa, mijozlarga xizmat ko'rsatish va axborot almashinuvi bilan bog'liq segmentlarda) axborotlarning tarqashi, inson omiliga bog'liq xatoliklar va muhofaza darajasining yetarli emasligi kabi zaifliklar mavjud. Bu esa bank faoliyatida axborot muhofazasi madaniyatini shakllantirish, tashqi va ichki xavfsizlik siyosatini kuchaytirish zaruratini keltirib chiqarmoqda.

Dissertatsiyada axborot xavfsizligiga oid xalqaro standartlar, jumladan ISO/IEC 27001, NIST Cybersecurity Framework hamda Yevropa Markaziy banki tomonidan ishlab chiqilgan “Cyber Resilience” tamoyillariga tayanilgan. Ular asosida axborot tizimining turli jihatlar: ruxsatsiz kirish, ma'lumotlar sizib chiqishi, kiberhujumlarga qarshi mudofaa darajasi va xodimlar malakasi chuqur tahlil qilinadi. Tadqiqotda, shuningdek, O'zbekiston Respublikasi “Axborotlashtirish to'g'risida”gi Qonuni, “Shaxsiy ma'lumotlar to'g'risida”gi Qonuni, “Banklar va bank faoliyati to'g'risida”gi Qonuni va Markaziy bank tomonidan tasdiqlangan tegishli yo'riqnomalar normativ-huquqiy asos sifatida o'rganildi.

Tadqiqot natijalari shuni ko'rsatdiki, bank tizimlarida axborotni muhofaza qilishga doir xavfsizlik siyosati mavjud bo'lsa-da, ularni real vaqtda monitoring qilish, xodimlar o'rtasida samarali axborot xavfsizligi madaniyatini shakllantirish, risklarni tez aniqlovchi texnologiyalarni joriy qilish kabi masalalar dolzarbligicha qolmoqda. Shu bois, “Ipoteka Bank” ATB misolida ishlab chiqilgan takliflar, jumladan xavfsizlik platformalarini yagona tizimda integratsiyalash, har bir bo'lim uchun individual xavfsizlik siyosatini shakllantirish, texnik

xizmat ko'rsatish tizimlarini qat'iy nazorat ostida yuritish bankda samarali xavfsizlik muhitini shakllantirishga xizmat qiladi.

Tezisdan shuningdek, mijozlarning shaxsiy ma'lumotlarini himoya qilish, ma'lumotlar bazasini shifrlash, xodimlarga nisbatan xavfsizlik attestatsiyasini joriy etish, texnik xizmat ko'rsatuvchi xodimlar faoliyatini real vaqtda loglashtirish kabi takliflar ilgari surildi. Bunday yondashuv nafaqat bank ichki xavfsizligini kuchaytiradi, balki tashqi regulyatorlar oldida ham bank ishonchliligining oshishiga olib keladi.

Bank axborot xavfsizligining yana bir muhim jihati — bu inson omiliga bog'liq bo'lgan xavflarni kamaytirishdir. Dissertatsiyada ta'kidlanganidek, har qanday ilg'or texnologik yechim ham xodimlar tomonidan noto'g'ri boshqarilsa yoki shaxsiy mas'uliyat darajasi past bo'lsa, bank xavfsizlik tizimida jiddiy zaifliklar yuzaga kelishi mumkin. Shu bois, xodimlar uchun axborot xavfsizligi bo'yicha doimiy treninglar tashkil etish, ularni attestatsiyadan o'tkazish, maxfiylik darajasiga mos kirish huquqlarini belgilash zaruriy choralar sifatida ilgari surildi.

Shuningdek, dissertatsiyada raqamli transformatsiya jarayonida xavfsizlikni ta'minlashda sun'iy intellekt, "big data" va "machine learning" texnologiyalaridan foydalanish imkoniyatlari ham ko'rib chiqildi. Bunday ilg'or yondashuvlar xavflarni avtomatik aniqlash, tranzaktsiyalarni anomaliya bo'yicha filtrlash va real vaqt rejimida ogohlantirish tizimlarini ishlab chiqishda muhim ahamiyatga ega.

Xulosa qilib aytganda, bank tizimida avtomatlashtirilgan hisob jarayonlarini ishonchli va xavfsiz yuritish, axborotni himoyalash va nazorat qilish jarayonlarini raqamli yondashuvlar asosida tashkil qilish – nafaqat texnologik muammo, balki boshqaruv, nazorat va madaniyat masalasi ekanini dissertatsiya davomida ilmiy asosda isbotlab berildi. Ushbu tezis milliy bank tizimi raqamli transformatsiyasining asosiy ustunlaridan biri bo'lmish axborot xavfsizligiga oid yondashuvlarni shakllantirish va keng tatbiq etish zarurligini asoslab beradi.

Bank axborot xavfsizligi sohasida amalga oshirilayotgan islohotlar, bir tomondan, tizimni mustahkamlashga xizmat qilsa-da, amaliyotda uchrayotgan ayrim to'siqlar hali to'liq bartaraf etilmagan. Jumladan, bank axborot tizimlarida foydalanilayotgan dasturiy vositalarning yangilanmaganligi, litsenziyasiz yoki kam sertifikatlangan texnologiyalar asosida ishlayotgan segmentlar mavjudligi, xavfsizlik protokollarining har doim ham xalqaro talablar bilan muvofiq bo'lmashligi kabi muammolar mavjud. Bu kabi holatlar operatsion barqarorlikka, bank tizimining raqamli imijiga va eng muhimi, mijozlar ishonchiga salbiy ta'sir ko'rsatadi.

Shuningdek, tahlillar shuni ko'rsatadiki, bir qator tijorat banklarida, jumladan "Ipoteka Bank" ATBda, axborot xavfsizligi siyosati ko'proq texnik va regulyatoriy darajada shakllangan bo'lib, uning strategik boshqaruvga integratsiyalashuvi yetarli emas. Aslida, axborot xavfsizligi — bu alohida texnik xizmat emas, balki bankning umumiy strategik boshqaruv tizimiga bog'langan faoliyat turidir. Shu sababli, dissertatsiyada tavsiya qilinganidek, axborot xavfsizligini mustaqil bo'lim darajasida emas, balki strategik boshqaruv darajasida – ya'ni bank boshqaruv kengashi va direktorlar kengashi darajasida qaror qabul qilish mexanizmlariga kiritish maqsadga muvofiq bo'ladi.

Tadqiqotda axborot muhofazasini kuchaytirishga xizmat qiluvchi zamonaviy yondashuvlar, xususan, Zero Trust Architecture, Role-Based Access Control (RBAC), Data Loss Prevention (DLP), va Security Information and Event Management (SIEM) tizimlari imkoniyatlari tahlil qilindi. Ularning joriy etilishi orqali bank faoliyatida xavfsizlikni proaktiv

yondashuv asosida boshqarish, oldindan xavf omillarini aniqlash va real vaqt rejimida chora ko'rish imkoniyatlari kengayadi.

Yana bir muhim jihat – bank tizimida faoliyat yuritayotgan filial va hududiy bo'linmalarda axborot xavfsizligi madaniyati darajasining notekisligi. Poytaxtdagi asosiy ofisda xavfsizlik bo'yicha qat'iy reglamentlar mavjud bo'lsa-da, ayrim chekka filiallarda bu borada jiddiy bo'shliqlar mavjud. Shu sababli, tezisda taklif etilganidek, axborot xavfsizligi siyosatini butun bank tizimi miqyosida yagona standart asosida tartibga solish, uni amaliyotga joriy etishda onlayn nazorat mexanizmlari, masofaviy audit va doimiy attestatsiya tizimlari ishlab chiqilishi lozim.

References:

Используемая литература:

Foydalanilgan adabiyotlar:

1. O'zbekiston Respublikasi Konstitutsiyasi. 1992-yil, 8-dekabr.
2. O'zbekiston Respublikasining "Banklar va bank faoliyati to'g'risida"gi Qonuni. Qabul qilingan sana: 2022-yil, 5-aprel.
3. O'zbekiston Respublikasining "Axborotlashtirish to'g'risida"gi Qonuni. 2020-yil, 23-iyun.
4. O'zbekiston Respublikasining "Shaxsiy ma'lumotlar to'g'risida"gi Qonuni. 2019-yil, 2-iyul.
5. O'zbekiston Respublikasi Prezidentining PQ-197-sonli qarori. "Raqamli O'zbekiston – 2030" strategiyasi to'g'risida. 2020-yil, 5-oktabr.
6. O'zbekiston Respublikasi Prezidentining PQ-3418-sonli qarori. "Bank tizimini isloh qilish strategiyasi" to'g'risida. 2017-yil, 12-may.
7. O'zbekiston Respublikasi Markaziy bankining 2022-yilgi "Bank axborot tizimlari xavfsizligini ta'minlash bo'yicha yo'riqnoma"si.
8. Davlat xavfsizlik xizmati huzuridagi "Cyber Security Center" tavsiyalari, 2023-yil.
9. O'zbekiston Respublikasi Prezidentining PQ-60-son qarori. "Axborot xavfsizligini mustahkamlash bo'yicha chora-tadbirlar". 2022-yil, 28-dekabr.
10. O'zbekiston Respublikasi Vazirlar Mahkamasining 541-son qarori. "Axborot resurslarini muhofaza qilish to'g'risida". 2021-yil, 15-iyun.