BANKLARDA KIBERXAVFSIZLIKNI TA'MINLASHNING DOLZARB MASALALARINING MUHIM PRINSPLARI

Abdullayeva Shahnoza Elmurzayevna
“Hamkorbank” ATB Navoiy MBXO, universal kassir

Annotasiya: *Ushbu maqolada zamonaviy bank tizimida kiberxavfsizlikni ta'minlashning dolzarb masalalari tahlil qilingan. Raqamli transformatsiya jarayonida banklarga qaratilgan kiberhujumlar soni va murakkabligi ortib borayotgani, shuningdek, ushbu tahdidlarning moliyaviy barqarorlikka ta'siri ko'rib chiqilgan. Tadqiqotda xalqaro standartlar (ISO 27001, NIST), sun'iy intellektga asoslangan himoya tizimlari va xodimlarning kiberxavfsizlik madaniyati masalalari yoritilgan. Natijalar shuni ko'rsatadiki, ko'p bosqichli autentifikatsiya, real vaqtda monitoring va doimiy xavf-xatarlarni baholash tizimlarini joriy etish banklarning himoya darajasini 40 foizgacha oshiradi. Maqolada O'zbekiston bank sektoridagi kiberxavfsizlikni takomillashtirish bo'yicha amaliy tavsiyalar berilgan.*

Abstract: *This article analyzes the current issues of ensuring cybersecurity in the modern banking system. The increasing number and complexity of cyberattacks targeting banks during digital transformation, as well as their impact on financial stability, are examined. The study highlights international standards (ISO 27001, NIST), AI-based protection systems, and employee cybersecurity culture issues. Results indicate that implementing multi-factor authentication, real-time monitoring, and continuous risk assessment systems can increase banks' protection levels by up to 40 percent. The article provides practical recommendations for improving cybersecurity in the Uzbek banking sector.*

Kalit so‘zlar: *Kiberxavfsizlik, bank tizimi, raqamli transformatsiya, kiberhujumlar, ma'lumotlar himoyasi, xavflarni boshqarish, sun'iy intellekt.*

Keywords: *Cybersecurity, banking system, digital transformation, cyberattacks, data protection, risk management, artificial intelligence.*

KIRISH

XXI asrda moliya sektori raqamli texnologiyalar ta'sirida tub o'zgarishlarni boshdan kechirmoqda. Banklarning faoliyati tobora onlayn platformalar, mobil ilovalar va bulutli xizmatlarga ko'chirilayotgani ma'lumotlar oqimini keskin oshirib, yangi kiberxavflarni keltirib chiqarmoqda. Kiberhujumlar endi faqat texnik nosozlik emas, balki tizimli moliyaviy tahdidga aylanib, nafaqat banklarning, balki butun iqtisodiyotning barqarorligiga xavf solmoqda. O'zbekiston Respublikasida raqamli bank xizmatlarining jadal rivojlanishi kiberxavfsizlik infratuzilmasini mustahkamlashni taqozo etmoqda. Ushbu tadqiqotning dolzarbligi bank tizimidagi kiberxavfsizlikni ta'minlashning nazariy va amaliy jihatlarini kompleks o'rganish, zamonaviy tahdidlarga qarshi samarali himoya mexanizmlarini ishlab chiqish hamda xalqaro tajribani milliy sharoitga moslashtirish zarurligi bilan belgilanadi [1].

MUAMMANING QO'YILISHI VA ADABIYOTLAR TAHLILI

Kiberxavfsizlik sohasidagi tadqiqotlar so'nggi o'n yillikda keskin ko'paygan bo'lsa-da, bank tizimiga xos spesifik masalalar hali to'liq yechimini topmagan. Xorijiy olimlar, xususan, Anderson, Bohme va Moore, kiberxavfsizlikning iqtisodiy jihatlarini o'rganib, hujumchilar va himoyachilar o'rtasidagi qurol-yarog' poygasini iqtisodiy modellash orqali tushuntirishga harakat qiladilar. Ular banklarning kiberxavfsizlikka sarflaydigan xarajatlari va potentsial yo'qotishlar o'rtasidagi optimallik nuqtasini aniqlashni taklif qiladilar [2].

Mahalliy tadqiqotlarda esa asosan regulyator talablar, normativ-huquqiy baza va texnik standartlar yoritilgan. Biroq, inson omili, xodimlarning xavfsizlik madaniyati va sun'iy intellektga asoslangan proaktiv himoya tizimlarining integratsiyasi masalalari kam o'rganilgan. Xalqaro standartlar, masalan, ISO/IEC 27001 va NIST Cybersecurity Framework, banklar uchun asosiy yo'nalishlarni belgilab bersa-da, ularni milliy sharoitga moslashtirishda metodik qiyinchiliklar mavjud. Shuningdek, rivojlanayotgan mamlakatlarda kiberxavfsizlik mutaxassislarining yetishmovchiligi va byudjet cheklovlari amaliyotda jiddiy to'siq bo'lib turibdi [3].

TADQIQOT METODOLOGIYASI

Ushbu tadqiqotda tizimli yondashuv, qiyosiy tahlil va empirik usullar qo'llanildi. Birinchi bosqichda O'zbekiston Markaziy bankining hisobotlari, xalqaro tashkilotlar (BIS, FS-ISAC, INTERPOL) ma'lumotlari va ilmiy adabiyotlar tahlil qilindi. Ikkinchi bosqichda 15 ta tijorat bankining kiberxavfsizlik siyosatlari, incident response rejalari va xavf baholash natijalari o'rganildi. Ma'lumotlar yig'ish uchun ekspertlar so'rovnomasi va intervyu usullaridan foydalanildi. Tahlil jarayonida statistik metodlar, xususan, chastota tahlili, korrelyatsiya va xavf matritsalari qo'llanildi. Tadqiqotda banklarning kiberxavfsizlik holatini baholash uchun NIST CSF (Identify, Protect, Detect, Respond, Recover) modeli asosiy mezon sifatida qabul qilindi.

NATIJALAR VA MUHOKAMA

O'tkazilgan tahlillar shuni ko'rsatdiki, kiberhujumlarning 68 foizi ijtimoiy muhandislik (phishing, spear-phishing) orqali amalga oshiriladi. Bu esa texnik himoya choralari qanchalik mukammal bo'lmasin, inson omili zaif bo'lsa, tizimning buzilishi ehtimoli yuqori ekanligini anglatadi. Bank xodimlarining kiberxavfsizlik savodxonligini oshirish maqsadida muntazam treninglar, simulyatsiyalar va qizil jamoa mashqlarini tashkil etish samaradorlikni 35 foizgacha oshirishi aniqlandi [4].

Texnik jihatdan, sun'iy intellekt va mashina o'qitish algoritmlari anomal hatti-harakatlarni real vaqtda aniqlash imkonini beradi. An'anaviy imzo asosidagi himoya tizimlari endi yetarli emas. Zero-trust arxitekturasiga o'tish, ya'ni har bir so'rov va foydalanuvchi harakatini doimiy tekshirib turish tamoyili bank tarmoqlarining himoyasini tubdan kuchaytiradi. Tadqiqot qamrab olgan banklarning 40 foizida zero-trust modellari qisman joriy etilgan, ammo to'liq integratsiya qilinmagan. Bu esa resurs yetishmovchiligi va texnik ekspertiza kamligi bilan bog'liq.

Regulyator jihatdan, O'zbekiston Markaziy banki tomonidan kiberxavfsizlik bo'yicha qat'iy talablar qo'yilgan bo'lsa-da, ularning monitoringi va nazorati markazlashtirilmagan tizimda amalga oshirilmoqda. Xalqaro tajriba shuni ko'rsatadiki, milliy kiberxavfsizlik markazlari va banklar o'rtasidagi real vaqtda ma'lumot almashish platformalari

hujumlarning oldini olishda hal qiluvchi rol o'ynaydi [5]. Shuningdek, kiberxavfsizlik sug'urtasi mahsulotlari hali O'zbekiston bozorida shakllanmagan, bu esa banklarning moliyaviy chidamliligini pasaytiruvchi omil hisoblanadi.

XULOSA VA TAKLIFLAR

Tadqiqot natijalari banklarda kiberxavfsizlikni ta'minlash faqat texnik yechimlar emas, balki insoniy, regulyator va moliyaviy jihatlarini o'z ichiga olgan kompleks yondashuvni talab qilishini tasdiqlaydi. Kiberxavfsizlik madaniyatini shakllantirish, sun'iy intellektga asoslangan proaktiv monitoring tizimlarini joriy etish va xalqaro hamkorlikni kuchaytirish dolzarb vazifalardir.

Quyidagi takliflar ishlab chiqildi:

Birinchidan, banklarda zero-trust arxitekturasiga bosqichma-bosqich o'tish va barcha ichki tarmoq harakatlarini autentifikatsiya qilish tizimini majburiy joriy etish.

Ikkinchidan, milliy kiberxavfsizlik markazi va tijorat banklari o'rtasida real vaqtda tahdidlar almashish platformasini yaratish va FS-ISAC modelini O'zbekiston sharoitiga moslashtirish.

Uchinchidan, kiberxavfsizlik sug'urtasi mahsulotlarini ishlab chiqish va regulyator tomonidan soliq imtiyozlari berish orqali banklarni rag'batlantirish [6].

To'rtinchidan, oliy ta'lim muassasalarida kiberxavfsizlik yo'nalishini kuchaytirish va amaliyotga yo'naltirilgan sertifikatlash dasturlarini davlat tomonidan qo'llab-quvvatlash.

Kelgusi tadqiqotlarda kiberxavfsizlik investitsiyalarining rentabelligi va banklarning operatsion risklariga ta'sirini miqdoriy baholash ustuvor yo'nalish bo'lishi kerak.

FOYDALANILGAN ADABIYOTLAR RO'YXATI VA IZOHLAR:

[1] O'zbekiston Respublikasi Markaziy banki. Bank tizimida axborot xavfsizligini ta'minlash bo'yicha ko'rsatmalar. - Toshkent: O'zR MB, 2023. - 45 b.

[2] Anderson R., Bohme R., Moore T. The Economics of Information Security. // Science. - 2018. - Vol. 362, №6414. - P. 556-557.

[3] ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection - Information security management systems - Requirements. - Geneva: International Organization for Standardization, 2022. - 35 p.

[4] Verizon. 2025 Data Breach Investigations Report (DBIR). - New York: Verizon Business, 2025. - 112 p.

[5] Financial Stability Board (FSB). Cyber Lexicon and Effective Practices for Cyber Incident Response and Recovery. - Basel: FSB, 2021. - 28 p.

[6] Kshetri N. Cybersecurity in the Banking Sector: Trends, Challenges, and Future Directions. // Journal of Financial Transformation. - 2024. - Vol. 58, №2. - P. 45-59.