

## **BANK TIZIMIDA KIBER-RISKLARNI SUG'URTALASHNI RIVOJLANTIRISHDA XALQARO TAJRIBA VA O'ZBEKISTON AMALIYOTI**

**Qodirova Farangiz Komilovna**

O'zbekiston Respublikasi Bank-moliya akademiyasi

farangizkomilovna123@gmail.ru

<https://doi.org/10.5281/zenodo.21029106>

O'zbekiston bank tizimida raqamli transformatsiya jarayonlarining jadallashuvi mobil banking, masofaviy xizmat ko'rsatish, tezkor to'lovlar va elektron moliyaviy operatsiyalar hajmining keskin oshishiga olib kelmoqda. Ushbu jarayonlar bank xizmatlarining tezkorligi va iqtisodiy samaradorligini ta'minlash bilan birga, axborot tizimlariga noqonuniy kirish, elektron mablag'larni o'g'irlash, ma'lumotlarning buzilishi, kiberfiribgarlik va bank faoliyatining uzilishi bilan bog'liq risklarni kuchaytirmoqda. Natijada kiber-risklar banklarning moliyaviy barqarorligi, kapitali, likvidligi, mijozlar oldidagi majburiyatlari va ishchanlik obro'siga ta'sir ko'rsatuvchi muhim operatsion risklardan biriga aylanmoqda.

Xalqaro amaliyotda kiber-risklarning moliyaviy oqibatlarini kamaytirish uchun sug'urta va qayta sug'urta mexanizmlaridan keng foydalaniladi. Bunda kiber-sug'urta bankning axborot xavfsizligi tizimini almashtirmaydi, balki preventiv choralar qo'llanilganidan keyin saqlanib qoladigan qoldiq riskni moliyaviy transfer qilish vositasi hisoblanadi. O'zbekistonda kiberxavfsizlik va bank operatsiyalarini himoya qilish bo'yicha huquqiy hamda institutsional mexanizmlar rivojlanayotgan bo'lsa-da, bank kiber-risklarini sug'urtalashga oid standart mahsulotlar, tariflash metodikasi, zararlar statistikasi va qayta sug'urtalash amaliyoti hali yetarli darajada shakllanmagan.

Shu bois xalqaro kiber-sug'urta tajribasini milliy bank va sug'urta bozori sharoitiga moslashtirish, banklarning kiber-risk ekspozitsiyasini baholash hamda samarali sug'urta qoplamalarini ishlab chiqish dolzarb ilmiy-amaliy masala hisoblanadi. Mazkur tezisning maqsadi bank tizimidagi kiber-risklarni sug'urtalashning iqtisodiy ahamiyatini ochib berish, xalqaro tajribani tahlil qilish va O'zbekiston amaliyotida kiber-sug'urta mexanizmlarini rivojlantirish yo'nalishlarini asoslashdan iborat.

O'zbekiston bank tizimining raqamli transformatsiyasi kiber-risklar ekspozitsiyasini tez sur'atlarda kengaytirmoqda. 2021-2024-yillarda banklararo to'lovlar hajmi 2 786 trln so'mdan 7 279 trln so'mgacha, ya'ni 2,61 baravarga oshgan. 2024-yilda tezkor to'lovlar tizimi orqali 47,5 mln operatsiya amalga oshirilib, ularning umumiy qiymati 917,9 trln so'mni tashkil etgan. Shu davrda internetdan foydalanuvchi aholi ulushining 93,3 foizga yetgani bank



xizmatlarining raqamli kanallarga bog'liqligini yanada kuchaytirgan. Mazkur tendensiya bank xizmatlarining iqtisodiy samaradorligini oshirgan bo'lsa-da, elektron mablag'larni o'g'irlash, ma'lumotlar sizib chiqishi, DDoS-hujumlar, zararli dasturlar va biznes jarayonlarining uzilishi bilan bog'liq potensial zararlar ko'lamini ham oshirmoqda.

Xalqaro tajriba kiber-risklarning bank sektoriga ta'siri an'anaviy operatsion risklardan farqli ravishda tez tarqalishi, bir nechta moliyaviy institutlarga bir vaqtning o'zida zarar yetkazishi va uchinchi tomon texnologik provayderlari orqali tizimli tus olishi mumkinligini ko'rsatadi. 2024-yilda jahon kiber-sug'urta bozori hajmi qariyb 15 mlrd AQSh dollariga yetgan. Yevropa banklarining 58 foizi kamida bitta kiberhujumga duch kelgan, muvaffaqiyatli hujum natijasida yirik axborot-kommunikatsiya hodisasi yuz bergan banklar ulushi esa 33 foizni tashkil etgan. Bu holat kiber-sug'urtani faqat zararlarni qoplash vositasi sifatida emas, balki bankning operatsion barqarorligi va kapitalini himoya qiluvchi kompleks risk-transfer mexanizmi sifatida baholash zarurligini ko'rsatadi.

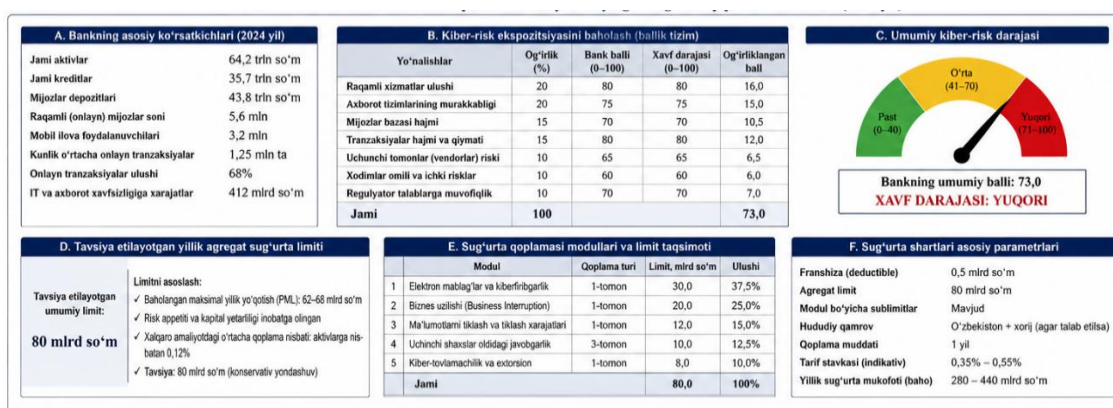
O'zbekiston amaliyotida kiber-risklarni preventiv boshqarish bo'yicha muayyan institutsional natijalarga erishilgan. Markazlashtirilgan antifraud tizimiga 34 ta bank va 9 ta to'lov tashkiloti integratsiya qilingan. Qo'shimcha identifikatsiya va vaqtinchalik cheklov mexanizmi orqali 28 138 ta holatda jami 304,1 mlrd so'm mablag'ning noqonuniy o'zlashtirilishi oldi olingan, bank kartalari bilan bog'liq firibgarlik holatlarida esa 9,5 mlrd so'm mablag' bloklangan. Biroq ushbu mexanizmlar hodisa yuz berish ehtimolini kamaytirishga qaratilgan bo'lib, axborot tizimlarini tiklash, faoliyat uzilishi, uchinchi shaxslar da'volari va reputatsiyani tiklash xarajatlarini to'liq moliyalashtirmaydi. Shu sababli banklarning qoldiq kiber-risklarini sug'urta orqali transfer qilish iqtisodiy jihatdan zarur hisoblanadi.

"Asakabank" AJ misolida o'tkazilgan tahlil bankning raqamli ekspozitsiyasi tez kengayayotganini ko'rsatdi. Bankning masofaviy xizmatlardan foydalanuvchilari soni 2025-yil boshidagi 1 285 457 nafardan yil oxiriga kelib 1 585 809 nafargacha yoki 23,4 foizga oshgan. Yuridik shaxslar va yakka tartibdagi tadbirkorlar soni esa 15 225 tadan 30 622 tagacha ko'payib, 101,1 foizlik o'sishni qayd etgan. Bank tomonidan muomalaga chiqarilgan kartalar soni 1 478 096 tani, to'lov terminallari soni 15 555 tani, terminallar orqali yillik tushum esa 14,558 trln so'mni tashkil etgan. Ushbu ko'rsatkichlar bankning elektron operatsiyalar, ma'lumotlar xavfsizligi va uchinchi shaxslar oldidagi javobgarlik bo'yicha sug'urta ehtiyojini kuchaytiradi.





Tadqiqot natijasida “Asakabank” AJ uchun 80 mlrd so‘mlik yillik agregat kiber-sug‘urta limiti taklif etildi. Mazkur limit bank kapitalining qariyb 1 foiziga va terminallar orqali o‘tadigan ikki kunlik o‘rtacha tushum qiymatiga mos keladi. Limitning 24 mlrd so‘mi elektron mablag‘lar va kiberfiribgarlik, 20 mlrd so‘mi biznes uzilishi, 16 mlrd so‘mi ma‘lumotlar va axborot tizimlarini tiklash, 12 mlrd so‘mi uchinchi shaxslar oldidagi javobgarlik, 8 mlrd so‘mi esa kiber-tovlamachilik va inqirozli boshqaruv xarajatlari uchun ajratilishi maqsadga muvofiq deb topildi. Bunday modulli yondashuv sug‘urta qoplamasini bankning real risk profiliga moslashtirish, yirik zararlarning bank foydasi va kapitaliga ta‘sirini cheklash hamda riskning asosiy qismini qayta sug‘urta bozori orqali diversifikatsiya qilish imkonini beradi.



## 1-rasm. O‘zbekiston bank tizimida raqamli ekspozitsiyaning o‘shishi va “Asakabank” AJ uchun tavsiya etilayotgan kiber-sug‘urta mexanizmi

Rasm ma‘lumotlari bank sektoridagi raqamli operatsiyalar hajmi va foydalanuvchilar sonining o‘shishi kiber-risklarning potensial moliyaviy og‘irligini oshirayotganini ko‘rsatadi. Banklararo to‘lovlar hajmining 2,61 baravarga oshishi va “Asakabank” AJ korporativ masofaviy mijozlari sonining 101,1 foizga ko‘payishi bankning kiberhodisalarga sezgirligini kuchaytiradi. Shu sharoitda 80 mlrd so‘mlik modulli sug‘urta limiti kiber-risklarning barcha oqibatlarini to‘liq bartaraf etmasa-da, yirik zararlarni bank, sug‘urtalovchi va qayta sug‘urtalovchi o‘rtasida taqsimlashga xizmat qiladigan amaliy moliyaviy himoya mexanizmini shakllantiradi.

Tadqiqot natijalari O‘zbekiston bank tizimining jadal raqamlashtirilishi kiber-risklarni banklarning moliyaviy barqarorligi, operatsion uzluksizligi va mijozlar oldidagi javobgarligiga bevosita ta‘sir qiluvchi muhim iqtisodiy riskka aylantirayotganini ko‘rsatdi. Mamlakatda kiberxavfsizlik, antifraud nazorati va elektron operatsiyalar monitoringi bo‘yicha institutsional mexanizmlar shakllanayotgan bo‘lsa-da, kiberhodisalar oqibatida yuzaga keladigan moliyaviy zararlarni qoplash tizimi yetarli darajada rivojlanmagan. Shu sababli kiber-

sug'urta banking axborot xavfsizligi choralarini almashtiruvchi vosita sifatida emas, balki texnik va tashkiliy nazoratdan keyin saqlanib qoladigan qoldiq riskni sug'urtalovchi va qayta sug'urtalovchiga transfer qilish mexanizmi sifatida joriy etilishi zarur.

Milliy amaliyotda banklar uchun modulli kiber-sug'urta mahsulotlarini ishlab chiqish, sug'urta limitini bank kapitali, elektron operatsiyalar hajmi va ehtimoliy maksimal zarar asosida belgilash hamda riskga asoslangan andarrayting tizimini qo'llash maqsadga muvofiq. Shuningdek, kiberhodisalar va ular natijasida yuzaga kelgan zararlar bo'yicha anonimlashtirilgan yagona statistik bazani yaratish, milliy sug'urta hisobotlarida kiber-risklar uchun alohida klassifikator joriy etish, standart qoplama va istisnolarni ishlab chiqish hamda yirik risklarni xalqaro qayta sug'urta bozori orqali diversifikatsiya qilish lozim. Mazkur choralar bank kapitalini yirik kiberzararlardan himoya qilish, raqamli moliyaviy xizmatlarning uzluksizligini ta'minlash va O'zbekistonda barqaror kiber-sug'urta bozorini shakllantirishga xizmat qiladi.

#### Foydalanilgan adabiyotlar ro'yxati:

O'zbekiston Respublikasining 2022-yil 15-apreldagi O'RQ-764-son "Kiberxavfsizlik to'g'risida"gi Qonuni.

O'zbekiston Respublikasining 2021-yil 23-noyabrdagi O'RQ-730-son "Sug'urta faoliyati to'g'risida"gi Qonuni.

Nomozova Q.I. Improvement of Capital Requirements in Insurance Companies of Uzbekistan // European Science Review. - 2025. - No. 3-4. - P. 38-42. DOI: 10.29013/ESR-25-3.4-38-42.

Ergasheva F.Sh. Оптимизация капитальных требований страховых компаний в Узбекистане // Iqtisodiy taraqqiyot va tahlil ilmiy elektron jurnali. - 2025. - Mart, 3-son. - B. 89-95.

Mamadiyarov Z., Karshiev D. Cybersecurity in Digital Banking: Safeguarding Customer Trust in Uzbekistan // American Journal of Corporate Management. - 2024. - Vol. 1, No. 2. - P. 13-18.

Biener C., Eling M., Wirfs J.H. Insurability of Cyber Risk: An Empirical Analysis // The Geneva Papers on Risk and Insurance - Issues and Practice. - 2015. - Vol. 40, No. 1. - P. 131-158. DOI: 10.1057/gpp.2014.19.

Eling M., Schnell W. What Do We Know About Cyber Risk and Cyber Risk Insurance? // The Journal of Risk Finance. - 2016. - Vol. 17, No. 5. - P. 474-491. DOI: 10.1108/JRF-09-2016-0122.

