BIG DATA TEXNOLOGIYALARINI TIJORAT BANKLARIDA QO'LLASHNING XAVF-XATARLARI VA TARTIBGA SOLISH JIHATLARI

Turabova Shaxnoza
TDIU Raqamli iqtisodiyot va xalqaro raqamli integratsiya kafedrasi doktoranti

Annotatsiya. *Ushbu maqolada O'zbekiston tijorat banklarida Big Data (katta hajmdagi ma'lumotlar) texnologiyalarini qo'llashdan kelib chiqadigan asosiy xavf-xatar turlari – kiberxavfsizlik, operatsion, me'yoriy-huquqiy va obro'ga oid xavf-xatarlar tasniflanadi. Amaldagi me'yoriy-huquqiy baza, jumladan, shaxsiy ma'lumotlar to'g'risidagi qonun va Markaziy bankning axborot xavfsizligiga oid normativ hujjatlari tahlil qilinadi. Xalqaro tajriba, xususan GDPR (Yevropaning shaxsiy ma'lumotlarni muhofaza qilish reglamenti) va BIS (Xalqaro hisob-kitoblar banki) standartlari ko'rib chiqiladi hamda tartibga solish mexanizmlarini takomillashtirish bo'yicha amaliy tavsiyalar ishlab chiqiladi.*

Kalit so'zlar: *Big Data, kiberxavfsizlik, shaxsiy ma'lumotlar, bank xavf-xatarlari, tartibga solish, RegTech (tartibga solishda texnologiyalar), SupTech (nazoratda texnologiyalar).*

Zamonaviy raqamli iqtisodiyot sharoitida tijorat banklari faoliyatida ma'lumotlar hajmi misli ko'rilmagan darajada ortib bormoqda. Mijozlar tranzaksiyalari, kredit tarixi, to'lov xulq-atvori va boshqa moliyaviy operatsiyalar natijasida shakllanadigan katta hajmdagi tarkibsiz ma'lumotlar massivi – Big Data texnologiyalarini bank sektorida qo'llashning dolzarbligini belgilab bermoqda. Hajmi, tezligi va xilma-xilligi jihatidan an'anaviy usullar bilan qayta ishlash imkoni bo'lmagan ma'lumotlar to'plamini amaldagi bank tizimining imkoniyatlari doirasida boshqarish tobora qiyinlashib bormoqda.

O'zbekiston Respublikasida raqamli bank xizmatlarining jadal rivojlanishi mazkur muammoning amaliy ahamiyatini yanada kuchaytiradi. O'zbekiston Respublikasi Markaziy banki statistik ma'lumotlariga ko'ra, masofaviy bank xizmatlaridan foydalanuvchilar soni 2020-yil yanvar oyidagi 10,1 million kishidan 2024-yil yanvar oyida 43,6 million kishiga yetib, to'rt yil ichida 4 martadan ziyod o'sdi. Muomalaga chiqarilgan bank plastik kartalar soni esa 2024-yil boshida 46,2 million donaga yetdi[239]. Ushbu ko'rsatkichlar bank tizimida shakllanayotgan ma'lumotlar oqimining ko'lami va jadalligi to'g'risida yaqqol tasavvur beradi.

Biroq Big Data texnologiyalarining keng joriy etilishi bir qator jiddiy xavf-xatarlarni ham yuzaga keltiradi: kiberhujumlar va ma'lumotlar xavfsizligiga tahdidlar, operatsion nosozliklar, shaxsiy ma'lumotlarni qayta ishlash bilan bog'liq huquqiy muammolar hamda tartibga solish talablariga rioya etmaslik

[239] O'zbekiston Respublikasi Markaziy banki. Statistik byulleten – 2025-yil. – Toshkent: O'zR Markaziy banki, 2025. – 132 b.

natijalari. Bu xavf-xatarlar o'z navbatida bank faoliyatining barqarorligiga, mijozlar ishonchiga va moliyaviy tizimning yaxlitligiga bevosita ta'sir ko'rsatishi mumkin.

Mazkur maqolada O'zbekiston tijorat banklari misolida Big Data texnologiyalarini qo'llashdan kelib chiqadigan asosiy xavf-xatar turlari tasniflanadi, amaldagi me'yoriy-huquqiy baza tahlil qilinadi va xalqaro tajriba asosida tartibga solish mexanizmlarini takomillashtirish bo'yicha tavsiyalar ishlab chiqiladi.

Big Data xavf-xatarlarining tasnifi. BIS – Bank for International Settlements (Xalqaro hisob-kitoblar banki, Bazel, Shveytsariya) tadqiqotlariga ko'ra, katta hajmdagi ma'lumotlarni qayta ishlash moliyaviy institutlar uchun to'rtta asosiy xavf-xatar guruhini yuzaga keltiradi[240]. Mazkur tasnif O'zbekiston bank tizimi sharoitiga quyidagicha tatbiq etiladi.

Kiberxavfsizlik xavf-xatarlari. Bankning Big Data infratuzilmasi katta hajmdagi maxfiy ma'lumotlarni birlashtirganida u kiberjinoyatchilar uchun asosiy nishonga aylanadi. Phishing (fishing – foydalanuvchilarni aldab shaxsiy ma'lumotlarini olish), ransomware (to'lov dasturlari – tizimni bloklash orqali to'lov talab qilish) va DDoS (Distributed Denial of Service – tarqatilgan xizmatni rad etish hujumi) bank faoliyatiga jiddiy zarar yetkazishi mumkin. O'zbekiston Respublikasi Markaziy bankining Computer Emergency Response Team – CERT-CBU kompyuter favqulodda vaziyatlarni bartaraf etish markazi yildan yilga kiberhujumlar sonining o'sib borayotganini qayd etmoqda[241].

Operatsion xavf-xatarlar. Big Data tizimlarining texnik murakkabligi boshqaruv xatolariga, algoritm nosozliklariga va tizim uzilishlariga olib kelishi mumkin. Xususan, machine learning modellari noto'g'ri parametrlar asosida kredit riskini baholasa, bu noto'g'ri qarorlarga va moliyaviy yo'qotishlarga sabab bo'ladi. Bundan tashqari, uchinchi tomon yetkazib beruvchilardan foydalanish operatsion xavf-xatarni sezilarli darajada oshiradi.

Me'yoriy-huquqiy (regulatory) xavf-xatarlar. Big Data tizimlarida shaxsiy ma'lumotlarni to'plash, saqlash va qayta ishlash bo'yicha talablar doimiy ravishda kuchaytirilmoqda. Bankning amaldagi qonunchilik talablariga rioya etmasligi moliyaviy jarimalar, litsenziyaning bekor qilinishi va yuridik javobgarlikka sabab bo'ladi. Ayniqsa, xalqaro ma'lumot almashinuvi hamda cloud computing texnologiyalaridan foydalanish chog'ida chegaralararo ma'lumot uzatishga qo'yilgan cheklovlar muhim ahamiyat kasb etadi.

Obro'ga oid xavf-xatarlar. Mijozlar ma'lumotlarining oshkor bo'lishi yoki ma'lumotlarni noto'g'ri ishlatish faktlari ommaga ma'lum bo'lganda bank obro'si tez va sezilarli darajada zarar ko'radi. Mijozlar ishonchining yo'qolishi depozitlar oqimiga, bozor ulushiga va bank aksiyalari qiymatiga salbiy ta'sir ko'rsatishi mumkin. BIS tadqiqotlari shuni ko'rsatadiki, ma'lumotlar xavfsizligiga oid

[240] Doerr S., Gambacorta L., Serena J.M. Big data and machine learning in central banking // BIS Working Papers. – 2021. – No.930. – 43 p.

[241] O'zbekiston Respublikasi Markaziy banki Boshqaruvi qarori. Tijorat banklarining axborot xavfsizligi va kiberxavfsizlik bo'yicha minimal talablar. Ro'yxatga olish raqami №3669. – 18.08.2025 y.

voqealar sodir bo’lgandan keyin banklar mijozlar ishonchini sezilarli darajada yo’qotadi, bu esa depozitlar va kredit portfeli hajmiga bevosita salbiy ta‘sir ko’rsatadi[242].

1-jadval

Big Data xavf-xatarlarining tasnifi

Xavf-xatar turi	Asosiy manbalar	Oqibatlari
Kiberxavfsizlik	Kiberhujumlar, phishing, ransomware, DDoS	Moliyaviy yo’qotish, huquqiy javobgarlik
Operatsion	Machine learning xatolari, tizim nosozliklari, outsourcing	Noto’g’ri qarorlar, xizmat uzilishi
Me‘moriy-huquqiy	Qonun talablariga nomuvofiqlik, GDPR, ZRU-547	Jarimalar, litsenziya bekor qilinishi
Obro’ga oid	Ma‘lumotlar oshkor bo’lishi, noto’g’ri foydalanish	Mijozlar ishonchini yo’qotish

Manba: muallif tomonidan BIS Working Papers No.930 asosida tuzilgan.

O’zbekiston Respublikasining me‘yoriy-huquqiy bazasi. O’zbekiston Respublikasida Big Data texnologiyalarini tartibga soluvchi me‘yoriy-huquqiy baza so’nggi yillarda sezilarli darajada rivojlandi. Shunday bo’lsa-da, raqamli transformatsiyaning jadal sur‘atlariga nisbatan qonunchilik tizimini yanada takomillashtirish zarurati saqlanib qolmoqda.

Shaxsiy ma‘lumotlar sohasidagi asosiy huquqiy hujjat – 2019-yil 2-iyulda qabul qilingan ZRU-547-sonli «Shaxsiy ma‘lumotlar to’g’risida»gi qonundir[243]. Mazkur qonun shaxsiy ma‘lumotlarni to’plash, saqlash, qayta ishlash va uzatish tartibini belgilaydi hamda banklarning ma‘lumotlar muhofazasiga oid majburiyatlarini tartibga soladi. Qonunga ko’ra, ma‘lumot subyektining roziligisiz shaxsiy ma‘lumotlarni uchinchi shaxslarga berish taqiqlanadi.

Axborot xavfsizligi sohasida 2025-yil 20-noyabrdan kuchga kirgan O’zbekiston Respublikasi Markaziy banki Boshqaruvi qarori (reg. №3669) tijorat banklari uchun axborot xavfsizligi va kiberxavfsizlik bo’yicha minimal talablarni belgilaydi[244]. Ushbu normativ hujjat quyidagi muhim talablarni o’z ichiga oladi: banklarda axborot xavfsizligi xizmatini yaratish majburiyligi; IT-infratuzilmasini boshqarishni autsorsing qilishga taqiq; ma‘lumotlar va serverlarni faqat bankning o’z ma‘lumotlar markazida yoki Markaziy bank bulutida saqlash talabi; asosiy ma‘lumotlar markazidan kamida 50 km uzoqlikda zaxira ma‘lumotlar markazi mavjudligi; kiber intsidentlar to’g’risida Markaziy bankka darhol xabar berish majburiyligi.

[242] Doerr S., Gambacorta L., Serena J.M. Big data and machine learning in central banking // BIS Working Papers. – 2021. – No.930.

[243] O’zbekiston Respublikasining «Shaxsiy ma‘lumotlar to’g’risida»gi Qonuni. ZRU-547. – 2019-yil 2-iyul.

[244] O’zbekiston Respublikasi Markaziy banki Boshqaruvi qarori. Tijorat banklarining axborot xavfsizligi va kiberxavfsizlik bo’yicha minimal talablar. Ro’yxatga olish raqami №3669. – 18.08.2025 y.

2024-yil 20-sentabrda qabul qilingan ZRU-964-sonli qonun kiberxavfsizlik sohasiga oid qonunchilikka muhim o'zgartishlar kiritdi[245]. Ushbu qonun bank infratuzilmasi kritik axborot infratuzilmasi ob'ektlari sifatida belgilab, ular uchun maxsus himoya rejimi joriy etadi.

RegTech (Regulatory Technology – tartibga solish sohasida texnologiyalardan foydalanish) va SupTech (Supervisory Technology – nazorat sohasida texnologiyalardan foydalanish) yo'nalishida O'zbekiston Respublikasi Markaziy banki 2027-yilgacha ma'lumotlarni boshqarish tizimini joriy etishni rejalashtirayotgani alohida ahamiyat kasb etadi. Ushbu loyiha doirasida Singapur MAS (Monetary Authority of Singapore – Singapur moliyaviy boshqaruv idorasi), Litva, Turkiya va Qozog'iston markaziy banklarining ilg'or tajribasi o'rganilmoqda, KPMG kompaniyasi maslahatchisi sifatida jalb etilgan[246].

Shunday bo'lsa-da, amaldagi me'yoriy-huquqiy bazaning bir qator muhim bo'shliqlari mavjud:

Big Data texnologiyalari uchun ixtisoslashgan standartlar yo'q;

bulut hisoblash texnologiyalarini tartibga solish to'liq shakllanmagan;

ma'lumotlarni profillashtirish va sun'iy intellekt asosidagi qarorlarga nisbatan talablar yetarli darajada aniq belgilanmagan.

3. Xalqaro tajriba: GDPR va BIS standartlari. Xalqaro amaliyot shuni ko'rsatadiki, rivojlangan davlatlar Big Data texnologiyalarini tartibga solishda ikki yo'nalishda ish olib bormoqda: ma'lumotlarni muhofaza qilishga oid umumiy qonunchilik va bank sektoriga ixtisoslashgan standartlar.

Yevropa Ittifoqida 2018-yildan kuchga kirgan GDPR – General Data Protection Regulation (Shaxsiy ma'lumotlarni muhofaza qilish bo'yicha umumiy reglament) – eng keng qamrovli me'yoriy hujjat hisoblanadi[247]. GDPR ma'lumotlarni "maqsadni cheklash" tamoyili asosida qayta ishlashni talab etadi, ya'ni ma'lumotlar faqat belgilangan maqsad uchun ishlatilishi mumkin. Bank sektorida GDPR katta hajmdagi ma'lumotlarni analitik maqsadlarda foydalanishga jiddiy cheklovlar qo'yadi. Ayniqsa, avtomatlashtirilgan qarorlar (masalan, kredit berish yoki rad etish) ustidan nazorat talabi banklar uchun yangi muvofiqlashuvchi majburiyatlarni yuzaga keltiradi.

BIS Working Papers No.930 ishchi hujjatida katta hajmdagi ma'lumotlardan foydalanishning moliyaviy barqarorlik uchun olib keladigan xavf-xatarlari batafsil tahlil qilingan[248]. BIS ekspertlari xususan quyidagi muammolarni belgilaydi:

model xavfi (AI – Artificial Intelligence, sun'iy intellekt algoritmlari noto'g'ri natijalar berishi mumkin);

---

[245] O'zbekiston Respublikasining kiberxavfsizlikka oid qonunchilikka o'zgartishlar kirituvchi Qonuni. ZRU-964. – 2024-yil 20-sentabr.

[246] O'zbekiston Respublikasi Markaziy banki Boshqaruvi qarori. Tijorat banklarining axborot xavfsizligi va kiberxavfsizlik bo'yicha minimal talablar. Ro'yxatga olish raqami №3669. – 18.08.2025 y.

[247] European Parliament. General Data Protection Regulation (GDPR). Regulation (EU) 2016/679. – Official Journal of the European Union, 2016. – L 119/1.

[248] Doerr S., Gambacorta L., Serena J.M. Big data and machine learning…

ma‘lumotlar sifati muammolari (noto’g’ri ma‘lumotlar asosida kredit baholash);

tizimli xavf (ko’plab banklar bir xil algoritmdan foydalanishi tizimli xatoga olib kelishi mumkin).

Singapur moliyaviy boshqaruv idorasi (MAS) tajribasi alohida ahamiyatga ega. MAS 2019-yilda «FEAT» tamoyillari – Fairness (adolatlilik), Ethics (axloq), Accountability (mas‘uliyat), Transparency (shaffoflik) – ni joriy etib, banklarda sun‘iy intellekt va Big Data texnologiyalarini qo’llashga asoslangan tamoyillar tizimini shakllantirdi[249]. Ushbu yondashuv O’zbekiston uchun ham tatbiq etilishi mumkin bo’lgan samarali model sifatida ko’rilmoqda.

Bazel III – bank sektori uchun kapital va likvidlik talablarini belgillovchi xalqaro standartlar to’plami doirasida operatsion xavf-xatarni boshqarishga oid talablar bank sektorida Big Data tizimlarini joriy etishda hisobga olinishi kerak bo’lgan xalqaro minimumni belgilaydi. Mazkur standartlar axborot xavfsizligi voqealarini operatsion yo’qotishlar sifatida tasniflash va ularni kapital talablari hisobida aks ettirish majburiyatini qo’yadi.

Amalga oshirilgan tahlil asosida O’zbekiston bank sektorida Big Data texnologiyalarini tartibga solishni takomillashtirish bo’yicha quyidagi tavsiyalar ishlab chiqildi.

Birinchi tavsiya – ixtisoslashgan me‘yoriy hujjatlar ishlab chiqish. Amaldagi me‘yoriy-huquqiy bazani to’ldirish maqsadida tijorat banklarida Big Data va sun‘iy intellekt texnologiyalarini qo’llashga oid alohida qo’llanma ishlab chiqish tavsiya etiladi. Mazkur hujjat data governance (ma‘lumotlarni boshqarish – ma‘lumotlarning to’g’riligi, xavfsizligi va sifatini ta‘minlash tizimlari), model xavfini boshqarish va algoritmik qarorlar ustidan nazorat talablarini o’z ichiga olishi kerak. Singapur MAS ning «FEAT» tamoyillari mazkur yo’nalishdagi asosiy metodologik manba sifatida tatbiq etilishi mumkin.

Ikkinchi tavsiya – RegTech va SupTech tizimini jadal rivojlantirish. Markaziy bankning 2027-yilgacha amalga oshirishni rejalashtirayotgan ma‘lumotlarni boshqarish tizimi doirasida real vaqt rejimida bank faoliyatini nazorat qilish imkoniyatlarini kengaytirish zarur. Ayniqsa, banklarning Big Data infratuzilmasidan foydalanishini masofadan monitoring qilish va kiber holatlarni darhol aniqlash mexanizmlarini ishga tushirish ustuvor vazifa hisoblanadi.

Uchinchi tavsiya – ma‘lumotlar lokalizatsiyasi talablarini aniqlashtirish. Markaziy bankning reg. №3669-sonli qarori ma‘lumotlarni faqat bankning o’z ma‘lumotlar markazida yoki Markaziy bank bulutida saqlash talabini o’rnatgan. Biroq cloud computing texnologiyalarining turli shakllari (xususiy, jamoat, gibrid bulut) uchun aniq texnik va huquqiy talablarni belgilovchi qo’shimcha yo’riqnomalar ishlab chiqish maqsadga muvofiqdir.

To’rtinchi tavsiya – axborot xavfsizligi bo’yicha kadrlar salohiyatini oshirish. Tijorat banklarida Big Data tizimlarini samarali boshqarish uchun ixtisoslashgan

249 Monetary Authority of Singapore. Principles to Promote Fairness, Ethics, Accountability and Transparency (FEAT) in the Use of Artificial Intelligence and Data Analytics in Singapore's Financial Sector. – Singapore: MAS, 2019. – 22 p.

mutaxassislar tayyorlash dasturlari va sertifikatlash mexanizmlarini joriy etish tavsiya etiladi. Xususan, CISO (Chief Information Security Officer – axborot xavfsizligi bo'yicha bosh direktor) lavozimi uchun malaka talablarini belgilovchi normativ hujjat qabul qilish va ularni muntazam attestatsiyadan o'tkazish tizimini shakllantirish zarur.

Mazkur tadqiqot natijalari shuni ko'rsatadiki, O'zbekiston tijorat banklarida Big Data texnologiyalarini qo'llash hajmining tez o'sishi 2020-2024 yillar davomida masofaviy bank xizmatlari foydalanuvchilari sonining 10,1 milliondan 43,6 millionga yetishi – tartibga solish tizimini yanada takomillashtirishni talab etadi. Kiberxavfsizlik, operatsion, me'yoriy-huquqiy va obro'ga oid xavf-xatarlar o'zaro bog'liq bo'lib, ularni kompleks boshqarish zaruriyati mavjud.

Amaldagi me'yoriy-huquqiy baza – ZRU-547, reg. №3669 va ZRU-964 hujjatlari – muhim asosni shakllantirgan bo'lsa-da, Big Data va sun'iy intellektga ixtisoslashgan standartlar, bulut texnologiyalari va profillashtirish bo'yicha talablar hali to'liq ishlab chiqilmagan. Singapur MAS va BIS standartlarining ilg'or tajribasi asosida ixtisoslashgan qo'llanmalar ishlab chiqish, RegTech/SupTech tizimini jadal rivojlantirish va axborot xavfsizligi kadrlar salohiyatini oshirish – O'zbekiston bank sektori uchun ustuvor yo'nalishlar sifatida belgilanishi maqsadga muvofiqdir.

ЦИФРОВАЯ ТРАНСФОРМАЦИЯ СИСТЕМЫ ГОСУДАРСТВЕННЫХ ЗАКУПОК: ПРОБЛЕМЫ И ПЕРСПЕКТИВЫ

Ризакулов Шерзод Шермуратович
Доцент кафедры финансы и цифровой экономики Ташкентского государственного экономического университета

В современных условиях развития цифровой экономики важным направлением реформирования государственного управления является внедрение цифровых технологий в систему государственных закупок. Государственные закупки выступают одним из ключевых инструментов эффективного использования бюджетных средств, стимулирования конкуренции и развития предпринимательской среды. В этой связи цифровая трансформация закупочных процессов приобретает стратегическое значение для повышения прозрачности, эффективности и подотчетности государственных расходов.

В мировой практике внедрение электронных систем закупок позволило значительно повысить открытость закупочных процедур, обеспечить доступность информации для участников рынка и минимизировать коррупционные риски. Использование цифровых платформ способствует автоматизации процедур планирования, проведения тендеров, заключения контрактов и мониторинга исполнения