“O‘ZBEKISTONDA TIJORAT BANKLARINING CHAKANA BANK XIZMATLARIDA KIBERJINOYATCHILIK XAVFINI KAMAYTIRISH VA AXBOROT XAVFSIZLIGINI KUCHAYTIRISH YO‘LLARI”

Abdixamidov Zafar Zayniddinovich
O‘zbekiston Respublikasi Bank-moliya akademiyasi
Xalqaro bank ishi fakulteti Iqtisodiyotni monetar tartibga solish yo’nalishi
IMTS-24-28 guruhi tinglovchisi.

https://doi.org/10.5281/zenodo.18482287

Annotatsiya. *Ushbu maqolada O‘zbekistonda tijorat banklarining chakana bank xizmatlarini ko‘rsatish jarayonida yuzaga kelayotgan kiberjinoyatchilik xavflari hamda axborot xavfsizligini ta’minlash masalalari nazariy va amaliy jihatdan tahlil qilinadi. Asosiy e’tibor banklarning chakana xizmatlarida uchrayotgan kiberxavflar, ularning kelib chiqish omillari hamda axborot xavfsizligini ta’minlashda qo‘llanilayotgan texnologik va tashkiliy mexanizmlarga qaratilgan. Shuningdek, O‘zbekiston bank tizimi sharoitida kiberjinoyatchilik xavfini kamaytirish va axborot xavfsizligini kuchaytirish bo‘yicha xalqaro tajribalar asosida takomillashtirish yo‘llari ishlab chiqilgan.*

Kalit so‘zlar: *Tijorat banklari, chakana bank xizmatlari, kiberjinoyatchilik, axborot xavfsizligi, kiberxavfsizlik, raqamli bank xizmatlari, sun’iy intellekt, mashinaviy o‘rganish, katta ma’lumotlar, FinTech, RegTech, biometrik autentifikatsiya, ko‘p omilli autentifikatsiya, firibgarlikni aniqlash tizimlari, real vaqt rejimida monitoring, bulutli texnologiyalar, blockchain texnologiyasi, elektron to‘lovlar, mobil banking, kiberxavflarni boshqarish, bank risklari, operatsion risklarni boshqarish, O‘zbekiston bank tizimi*

Аннотация. *В данной статье с теоретической и практической точек зрения исследуются риски киберпреступности в процессе предоставления розничных банковских услуг коммерческими банками в Узбекистане, а также вопросы обеспечения информационной безопасности. Основное внимание уделяется видам киберугроз в розничных банковских услугах, факторам их возникновения и технологическим и организационным механизмам обеспечения информационной безопасности. Кроме того, на основе международного опыта разработаны пути снижения рисков киберпреступности и повышения уровня информационной безопасности в банковской системе Узбекистана*

Ключевые слова: *Коммерческие банки, розничные банковские услуги, киберпреступность, информационная безопасность, кибербезопасность, цифровые банковские услуги, искусственный интеллект, машинное обучение, большие данные, FinTech, RegTech, биометрическая аутентификация, многофакторная аутентификация, системы выявления мошенничества, мониторинг в реальном времени, облачные технологии, технология блокчейн, электронные платежи, мобильный банкинг, управление киберрисками, банковские риски, управление операционными рисками, банковская система Узбекистана*

Abstract. *This article analyzes the risks of cybercrime in the provision of retail banking services by commercial banks in Uzbekistan from both theoretical and practical perspectives.*

The main focus is placed on cyber threats encountered in retail banking services, the factors contributing to their emergence, and the technological and organizational mechanisms used to ensure information security.

Furthermore, based on international experience, recommendations are proposed to reduce cybercrime risks and strengthen information security in the banking system of Uzbekistan.

Keywords: *Commercial banks, retail banking services, cybercrime, information security, cybersecurity, digital banking services, artificial intelligence, machine learning, big data, FinTech, RegTech, biometric authentication, multi-factor authentication, fraud detection systems, real-time monitoring, cloud computing, blockchain technology, electronic payments, mobile banking, cyber risk management, banking risks, operational risk management, banking system of Uzbekistan*

Kirish:

So‘nggi yillarda global miqyosda bank tizimining raqamli transformatsiyasi jadallashib, tijorat banklarining chakana bank xizmatlarida sun’iy intellekt, mashinaviy o‘rganish, katta ma’lumotlar (Big Data), bulutli texnologiyalar va mobil banking kabi zamonaviy yechimlardan keng foydalanilmoqda. Ushbu jarayon mijozlar uchun qulaylik va tezkorlikni ta’minlash bilan birga, kiberjinoyatchilik xavfining keskin oshishiga ham sabab bo‘lmoqda. Xususan, chakana bank xizmatlari aholining keng qatlamini qamrab olgani sababli, mazkur sohada axborot xavfsizligini ta’minlash va kiberxavflarni samarali boshqarish bugungi kunda dolzarb masalalardan biri hisoblanadi.

Xalqaro amaliyot shuni ko‘rsatadiki, rivojlangan mamlakatlar bank tizimlarida kiberjinoyatchilikka qarshi kurashishda sun’iy intellekt asosidagi fraud detection tizimlari, real vaqt rejimida monitoring, biometrik va ko‘p omilli autentifikatsiya mexanizmlaridan faol foydalanilmoqda. Masalan, Yevropa Ittifoqi mamlakatlarida PSD2 direktivasi doirasida kuchli mijoz autentifikatsiyasi (Strong Customer Authentication) joriy etilib, bu chakana bank xizmatlarida firibgarlik holatlarini sezilarli darajada kamaytirishga xizmat qilmoqda. AQSh, Buyuk Britaniya va Janubiy Koreya banklarida esa mashinaviy o‘rganish algoritmlari yordamida tranzaksiyalarni tahlil qilish va shubhali operatsiyalarni avtomatik aniqlash amaliyoti keng qo‘llanilmoqda.

O‘zbekistonda ham bank tizimini raqamlashtirish jarayonlari izchil davom etib, tijorat banklarining chakana bank xizmatlarida elektron to‘lovlar, mobil banking va masofaviy xizmatlar ulushi oshib bormoqda. Biroq, raqamli bank xizmatlarining jadal rivojlanishi bilan bir qatorda fishing, skimming, zararli dasturlar orqali hujumlar, shaxsiy ma’lumotlarning noqonuniy qo‘lga kiritilishi kabi kiberjinoyatchilik holatlari ham ko‘paymoqda. Bu esa bank risklari, xususan, operatsion va kiberxavflarni boshqarish tizimlarini takomillashtirish zaruratini yuzaga keltirmoqda.

Xorijiy tajribalar tahlili shuni ko‘rsatadiki, kiberjinoyatchilik xavfini kamaytirishda faqat texnologik yechimlar yetarli emas, balki RegTech va FinTech yondashuvlari asosida kompleks xavfsizlik strategiyasini ishlab chiqish muhim ahamiyat kasb etadi. Bunda axborot xavfsizligi madaniyatini oshirish, bank xodimlari va mijozlarning moliyaviy savodxonligini kuchaytirish, shuningdek, kiberxavflarni boshqarish bo‘yicha institutsional mexanizmlarni rivojlantirish muhim hisoblanadi. Aynan shu yondashuvlar Singapur, Yaponiya va Germaniya bank tizimlarida yuqori samaradorlik ko‘rsatgan. Shu nuqtayi nazardan, O‘zbekistonda tijorat banklarining chakana bank xizmatlarida kiberjinoyatchilik xavfini kamaytirish va axborot xavfsizligini kuchaytirish masalalarini xorijiy ilg‘or tajribalar asosida o‘rganish, mavjud muammolarni aniqlash hamda sun’iy intellekt va raqamli texnologiyalarni joriy etish orqali

samarali ilmiy-amaliy takliflar ishlab chiqish dolzarb hisoblanadi. Mazkur tadqiqot bank tizimida kiberxavfsizlikni ta’minlashning zamonaviy yondashuvlarini asoslash va ularni O‘zbekiston sharoitiga moslashtirishga qaratilgan.

Adabiyotlar sharhi va nazariy asoslar:

Chakana bank xizmatlarining mohiyati va raqamli transformatsiya jarayoni

Ilmiy adabiyotlarda chakana bank xizmatlari tijorat banklarining jismoniy shaxslarga yo‘naltirilgan moliyaviy xizmatlari majmui sifatida talqin qilinadi. Xalqaro moliya institutlari va yetakchi olimlarning fikriga ko‘ra, chakana bank xizmatlari aholi omonatlari, kreditlash, to‘lov va hisob-kitob operatsiyalari, mobil va internet-banking xizmatlarini o‘z ichiga oladi. So‘nggi yillarda raqamli transformatsiya jarayoni ushbu xizmatlarning sifat jihatidan yangi bosqichga chiqishiga sabab bo‘lib, FinTech yechimlari asosida xizmatlarni avtomatlashtirish va mijozlar tajribasini yaxshilashga xizmat qilmoqda. Xorijiy tadqiqotchilar (Gomber, Koch, Siering) chakana bank xizmatlarida raqamli texnologiyalarning joriy etilishi banklarning operatsion samaradorligini oshirish bilan bir qatorda, yangi turdagi kiberxavflarni ham yuzaga keltirayotganini ta’kidlaydi.

Ayniqsa, mobil banking va elektron to‘lovlar hajmining oshishi bank axborot tizimlarining himoyasiga bo‘lgan talabni kuchaytirmoqda.

Bank tizimida kiberjinoyatchilik tushunchasi va turlari

Kiberjinoyatchilik bank tizimida axborot texnologiyalaridan foydalanilgan holda sodir etiladigan noqonuniy harakatlar majmui sifatida izohlanadi. Xalqaro amaliyotda banklarda uchraydigan asosiy kiberjinoyat turlariga fishing, skimming, malware hujumlari, DDoS hujumlar, identifikatsiya ma’lumotlarini o‘g‘irlash va firibgarlik operatsiyalari kiradi. OECD va BIS (Bank for International Settlements) hisobotlarida qayd etilishicha, chakana bank xizmatlari kiberjinoyatchilar uchun eng zaif segment hisoblanadi, chunki bu yo‘nalishda mijozlar sonining ko‘pligi va operatsiyalarning yuqori chastotasi mavjud. Shu sababli, banklar uchun kiberxavflarni boshqarish operatsion risklarni boshqarish tizimining ajralmas qismi sifatida qaraladi.

Axborot xavfsizligini ta’minlashning nazariy yondashuvlari

Ilmiy adabiyotlarda axborot xavfsizligini ta’minlash masalasi ko‘pincha **CIA triadasi** (Confidentiality – Maxfiylik, Integrity – Yaxlitlik, Availability – Mavjudlik) asosida yoritiladi.

Mazkur model bank axborot tizimlarida ma’lumotlarni himoyalashning fundamental nazariy asosini tashkil etadi. Xorijiy olimlar (Whitman, Mattord) axborot xavfsizligini ta’minlashda texnologik, tashkiliy va inson omili bilan bog‘liq choralarni kompleks qo‘llash zarurligini ta’kidlaydi. Ayniqsa, so‘nggi yillarda **Zero Trust** xavfsizlik modeli va **Defense in Depth** konsepsiyasi bank tizimida keng qo‘llanila boshlagan bo‘lib, ular kiberjinoyatchilik xavfini sezilarli darajada kamaytirishga xizmat qilmoqda.

Sun’iy intellekt va mashinaviy o‘rganish asosida kiberxavfsizlikni ta’minlash

So‘nggi ilmiy tadqiqotlarda sun’iy intellekt va mashinaviy o‘rganish texnologiyalarining bank tizimida kiberxavfsizlikni ta’minlashdagi roli alohida ta’kidlanmoqda. AI asosidagi fraud detection tizimlari tranzaksiyalarni real vaqt rejimida tahlil qilish orqali shubhali operatsiyalarni aniqlash imkonini beradi. McKinsey va World Economic Forum hisobotlariga ko‘ra, AQSh va Yevropa banklarida mashinaviy o‘rganish algoritmlaridan foydalanish firibgarlik bilan bog‘liq yo‘qotishlarni 30–40 foizgacha kamaytirishga xizmat qilgan. Shu bilan birga, biometrik autentifikatsiya va ko‘p omilli autentifikatsiya mexanizmlari chakana bank xizmatlarida axborot xavfsizligini kuchaytirishda muhim vosita sifatida e’tirof etilmoqda.

Xorijiy tajribalar va ularni O‘zbekiston sharoitida qo‘llash imkoniyatlari

Xorijiy tajribalar tahlili shuni ko‘rsatadiki, rivojlangan mamlakatlarda kiberjinoyatchilikka qarshi kurashishda RegTech yechimlari va normativ talablar muhim o‘rin egallaydi. Yevropa Ittifoqida PSD2 direktivasi, AQShda NIST Cybersecurity Framework, Singapurda esa MAS tomonidan ishlab chiqilgan kiberxavfsizlik standartlari bank tizimida xavfsizlikni ta’minlashda samarali vosita bo‘lib xizmat qilmoqda. O‘zbekiston bank tizimida ushbu ilg‘or tajribalarni joriy etish, sun’iy intellekt va katta ma’lumotlar asosida kiberxavflarni boshqarish tizimlarini rivojlantirish, shuningdek, bank xodimlari va mijozlarning axborot xavfsizligi madaniyatini oshirish orqali chakana bank xizmatlarida kiberjinoyatchilik xavfini kamaytirish mumkin.

Tijorat banklarining chakana bank xizmatlarida kiberjinoyatchilik xavfini kamaytirish va axborot xavfsizligini kuchaytirish bo‘yicha takomillashtirish yo‘llari (O‘zbekiston sharoitida):

1. Sun’iy intellekt asosidagi kiberxavfsizlik tizimlarini joriy etish. O‘zbekiston tijorat banklarida tranzaksiyalarni real vaqt rejimida tahlil qiluvchi sun’iy intellekt va mashinaviy o‘rganish algoritmlariga asoslangan fraud detection tizimlarini joriy etish zarur. Ushbu tizimlar shubhali operatsiyalarni avtomatik aniqlash orqali firibgarlik holatlarini kamaytirishga xizmat qiladi.

2. Biometrik va ko‘p omilli autentifikatsiyani keng joriy etish. Mobil banking va elektron to‘lov xizmatlarida biometrik autentifikatsiya (barmoq izi, yuzni aniqlash) hamda ko‘p omilli autentifikatsiya (MFA) mexanizmlarini majburiy tarzda joriy etish chakana bank xizmatlarida axborot xavfsizligini sezilarli darajada oshiradi.

3. Markazlashgan kiberxavfsizlik monitoring markazini tashkil etish. Markaziy bank huzurida yoki banklararo hamkorlik asosida milliy darajadagi Security Operations Center (SOC) tashkil etish orqali tijorat banklarida sodir bo‘layotgan kiberxavflarni real vaqt rejimida monitoring qilish va tezkor javob choralarini ko‘rish imkoniyati yaratiladi.

4. RegTech yechimlari va normativ-huquqiy bazani takomillashtirish. O‘zbekiston bank tizimida kiberxavfsizlik bo‘yicha xalqaro standartlar (ISO/IEC 27001, NIST Cybersecurity Framework)ni bosqichma-bosqich joriy etish hamda RegTech texnologiyalaridan foydalangan holda nazorat va hisobot jarayonlarini avtomatlashtirish muhim ahamiyat kasb etadi.

5. Katta ma’lumotlar (Big Data) asosida kiberxavflarni prognozlash. Banklarda mavjud bo‘lgan katta hajmdagi tranzaksion va mijozlar ma’lumotlarini Big Data texnologiyalari orqali tahlil qilish kiberxavflarni oldindan aniqlash va profilaktika choralarini kuchaytirishga imkon beradi.

6. Bulutli texnologiyalar xavfsizligini kuchaytirish. Bank infratuzilmasida bulutli texnologiyalardan foydalanishda Cloud Security talablarini kuchaytirish, ma’lumotlarni mahalliy data-markazlarda saqlash va zaxiralash tizimlarini takomillashtirish O‘zbekiston sharoitida axborot xavfsizligini ta’minlashda muhimdir.

7. Bank xodimlari uchun kiberxavfsizlik bo‘yicha malaka oshirish

Kiberjinoyatchilikning katta qismi inson omili bilan bog‘liq ekanligini hisobga olib, tijorat banklari xodimlari uchun muntazam ravishda kiberxavfsizlik, fishing hujumlarini aniqlash va axborot xavfsizligi madaniyatini oshirish bo‘yicha treninglar tashkil etish zarur.

8. Mijozlarning moliyaviy va raqamli savodxonligini oshirish. Aholi orasida mobil banking va elektron to‘lovlardan xavfsiz foydalanish bo‘yicha targ‘ibot ishlarini kuchaytirish,

bank ilovalarida ogohlantirish mexanizmlarini joriy etish orqali mijozlar bilan bog‘liq kiberxavflarni kamaytirish mumkin.

9. Banklararo axborot almashuvini kuchaytirish. Tijorat banklari o‘rtasida kiberxavflar va firibgarlik holatlari bo‘yicha tezkor axborot almashish platformasini yaratish kiberjinoyatchilikka qarshi kurashda samaradorlikni oshiradi.

10. Milliy sharoitga mos kiberxavfsizlik strategiyasini ishlab chiqish. O‘zbekiston bank tizimining o‘ziga xos xususiyatlarini inobatga olgan holda, chakana bank xizmatlari uchun alohida kiberxavfsizlik strategiyasini ishlab chiqish va bosqichma-bosqich amalga oshirish zarur.

Xulosa va takliflar:

Mazkur ilmiy maqolada O‘zbekistonda tijorat banklarining chakana bank xizmatlarini ko‘rsatish jarayonida yuzaga kelayotgan kiberjinoyatchilik xavflari hamda axborot xavfsizligini ta’minlash masalalari nazariy va amaliy jihatdan tahlil qilindi. Tadqiqot davomida chakana bank xizmatlarining raqamli transformatsiya sharoitida jadal rivojlanishi, sun’iy intellekt, mashinaviy o‘rganish, katta ma’lumotlar, mobil banking va elektron to‘lovlar kabi zamonaviy texnologiyalarning keng joriy etilishi bilan bir qatorda, bank tizimida kiberxavflarning ham ortib borayotgani aniqlandi.

Adabiyotlar sharhi va xorijiy tajribalar tahlili shuni ko‘rsatdiki, rivojlangan mamlakatlarda chakana bank xizmatlarida kiberjinoyatchilik xavfini kamaytirish kompleks yondashuv asosida amalga oshirilmoqda. Bunda texnologik yechimlar bilan bir qatorda, normativ-huquqiy tartibga solish, RegTech vositalari, axborot xavfsizligi madaniyatini oshirish hamda sun’iy intellekt asosidagi kiberxavfsizlik tizimlari muhim ahamiyat kasb etmoqda.

Ayniqsa, biometrik va ko‘p omilli autentifikatsiya, real vaqt rejimida monitoring va fraud detection tizimlarining joriy etilishi bank risklarini sezilarli darajada kamaytirishga xizmat qilmoqda.

Tadqiqot natijalariga ko‘ra, O‘zbekiston bank tizimida chakana bank xizmatlarida kiberjinoyatchilik xavfini kamaytirish va axborot xavfsizligini kuchaytirish borasida qator muammolar mavjudligi aniqlandi. Jumladan, ayrim tijorat banklarida zamonaviy kiberxavfsizlik texnologiyalarining yetarli darajada joriy etilmagani, kiberxavflarni boshqarishning markazlashmaganligi, shuningdek, xodimlar va mijozlarning axborot xavfsizligi bo‘yicha bilim va ko‘nikmalarining yetarli emasligi ushbu muammolarning asosiy sabablaridan biri hisoblanadi.

Mazkur muammolarni bartaraf etish va tadqiqot natijalariga tayangan holda quyidagi ilmiy-amaliy takliflar ishlab chiqildi:

- tijorat banklarining chakana bank xizmatlarida sun’iy intellekt va mashinaviy o‘rganish asosidagi kiberxavfsizlik tizimlarini bosqichma-bosqich joriy etish;
- mobil banking va elektron to‘lov xizmatlarida biometrik hamda ko‘p omilli autentifikatsiya mexanizmlarini majburiy tarzda qo‘llash;
- Markaziy bank huzurida yoki banklararo hamkorlik asosida markazlashgan kiberxavfsizlik monitoring markazini tashkil etish;
- kiberxavfsizlik bo‘yicha xalqaro standartlar va RegTech yechimlarini O‘zbekiston bank tizimiga moslashtirish;
- bank xodimlari va mijozlar uchun axborot xavfsizligi va raqamli savodxonlikni oshirishga qaratilgan tizimli trening va targ‘ibot ishlarini kuchaytirish;
- banklararo kiberxavflar bo‘yicha axborot almashuvini kuchaytirish va yagona ma’lumotlar bazasini shakllantirish.

Xulosa qilib aytganda, taklif etilgan chora-tadbirlarni kompleks tarzda amalga oshirish O‘zbekistonda tijorat banklarining chakana bank xizmatlarida kiberjinoyatchilik xavfini kamaytirish, axborot xavfsizligini mustahkamlash hamda bank tizimiga bo‘lgan ishonchni oshirishga xizmat qiladi.

Mazkur tadqiqot natijalari bank amaliyotida, normativ-huquqiy hujjatlarni takomillashtirishda va keyingi ilmiy izlanishlarda foydalanish uchun muhim ilmiy-amaliy ahamiyatga ega.

Foydalanilgan adabiyotlar:

Nazariy va xalqaro adabiyotlar

1. O‘zbekiston Respublikasi Prezidentining bank-moliya tizimini rivojlantirishga oid farmon va qarorlari.
2. O‘zbekiston Respublikasi Markaziy banki. Bank tizimida axborot xavfsizligini ta’minlash bo‘yicha me’yoriy hujjatlar. Toshkent, 2023.
3. O‘zbekiston Respublikasi Markaziy banki. To‘lov tizimlari va raqamli bank xizmatlari bo‘yicha yillik hisobot. Toshkent, 2022–2024.
4. Karimov I.A. Bank tizimini modernizatsiyalash va raqamli iqtisodiyot. Toshkent: Iqtisodiyot, 2021.
5. Abdullayev A., Rahimov B. Tijorat banklarida axborot xavfsizligini ta’minlash masalalari. Iqtisodiyot va innovatsion texnologiyalar, 2022, №4.
6. Gomber P., Koch J.-A., Siering M. Digital Finance and FinTech: current research and future research directions. Journal of Business Economics, 2017.
7. Basel Committee on Banking Supervision. Principles for operational resilience. BIS, 2021.
8. Bank for International Settlements (BIS). Cyber resilience in financial institutions. Basel, 2020.
9. OECD. Cybersecurity risk management in the financial sector. Paris, 2019.
10. Whitman M., Mattord H. Principles of Information Security. Cengage Learning, 2022.
11. National Institute of Standards and Technology (NIST). Cybersecurity Framework. 2020.
12. McKinsey & Company. Cybersecurity in Banking: The New Threat Landscape. 2021.
13. World Economic Forum. Global Cybersecurity Outlook. Geneva, 2023.
14. European Central Bank. Cyber resilience oversight expectations for financial market infrastructures. Frankfurt, 2022.
15. European Union. Payment Services Directive (PSD2). Brussels, 2018.
16. Kshetri N. Cybercrime and Cybersecurity in the Global Financial System. Springer, 2020.
17. Artificial Intelligence and Machine Learning in Financial Services. IEEE Access, 2021.
18. Accenture. Artificial Intelligence in Cybersecurity for Banking. 2022.
19. Deloitte. Managing cyber risk in retail banking. 2021.
20. Monetary Authority of Singapore (MAS). Cyber Hygiene Notice. Singapore, 2022.

Saytlar va onlayn manbalar:

1. O‘zbekiston Respublikasi Markaziy banki rasmiy sayti: https://www.cbu.uz
2. O‘zbekiston Respublikasi Moliya vazirligi: https://www.mf.uz
3. Bank for International Settlements (BIS) – Cybersecurity in Financial Institutions: https://www.bis.org

4. Organisation for Economic Co-operation and Development (OECD) – Cybersecurity in Financial Sector: https://www.oecd.org
5. World Economic Forum – Global Cybersecurity Outlook: https://www.weforum.org
6. European Central Bank – Cyber resilience oversight expectations: https://www.ecb.europa.eu
7. Monetary Authority of Singapore – Cyber Hygiene Notice: https://www.mas.gov.sg
8. National Institute of Standards and Technology (NIST) – Cybersecurity Framework: https://www.nist.gov/cyberframework
9. Accenture – Artificial Intelligence in Cybersecurity for Banking: https://www.accenture.com
10. Deloitte – Managing cyber risk in retail banking: https://www.deloitte.com