IQTISODIY TARAQQIYOT VA TAHLIL ILMIY ELEKTRON JURNAL

UO'K: 336.717

BANK XIZMATLARINING RAQAMLI TRANSFORMATSIYASI VA KIBERXAVFSIZLIKNI TA'MINLASH MUAMMOLARI

Mengniyozov Anvar
Termiz davlat universiteti
ORCID: 0009-0003-5137-5398
mengniyozovanvar77@gmail.com

Annotatsiya. *Tadqiqot raqamli bank xizmatlarining jadal rivojlanishi sharoitida O'zbekiston bank tizimining kiberxavfsizligi va barqaror faoliyatini ta'minlash muammolarini o'rganishga bag'ishlangan. Bank sektorining raqamlashtirilishi raqamli banklar va ekotizimlar kabi yangi mahsulot va servislarning paydo bo'lishiga olib kelib, milliy moliyaviy hamda kiberxavfsizlik masalalarining dolzarbligini oshirmoqda. Tadqiqotning maqsadi bank xizmatlarining raqamli transformatsiyasining asosiy yo'nalishlarini kiberxavfsizlik kontekstida tavsiflashdan iborat. Maqolada bank xizmatlarining raqamli transformatsiyasi tushunchasiga doir yondashuvlar tizimlashtirilgan, jahon tajribasi asosida komparativ tahlil o'tkazilgan, O'zbekiston bank tizimidagi kiberxatarlar dinamikasi va ularning obyektlari tahlil qilingan hamda kiberxavfsizlikni kuchaytirishga doir takliflar ishlab chiqilgan. Tadqiqot natijalari bank sektorini davlat tomonidan tartibga solish va barqaror rivojlanish strategiyalarini ishlab chiqishda amaliy ahamiyatga ega.*

Kalit so'zlar: *raqamlashtirish, raqamli transformatsiya, biznes-modellar, kiberxatarlar, bank tizimi, kiberxavfsizlik.*

ЦИФРОВАЯ ТРАНСФОРМАЦИЯ БАНКОВСКИХ УСЛУГ И ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ

Менгниёзов Анвар
Термезский государственный университет

Аннотация. *Настоящее исследование посвящено изучению проблем обеспечения кибербезопасности и устойчивого функционирования банковской системы Республики Узбекистан в условиях стремительного развития цифровых банковских услуг. Цифровизация банковского сектора способствует появлению новых продуктов и сервисов, таких как цифровые банки и финансовые экосистемы, что, в свою очередь, усиливает актуальность вопросов национальной финансовой и кибербезопасности. Целью исследования является характеристика основных направлений цифровой трансформации банковских услуг в контексте обеспечения кибербезопасности. В статье систематизированы теоретические подходы к понятию цифровой трансформации банковских услуг, проведён сравнительный анализ на основе международного опыта, проанализирована динамика киберугроз и их объекты в банковской системе Узбекистана, а также разработаны предложения по усилению мер кибербезопасности. Результаты исследования имеют практическую значимость при разработке механизмов государственного регулирования и стратегий устойчивого развития банковского сектора.*

Ключевые слова: *цифровизация, цифровая трансформация, бизнес-модели, киберугрозы, банковская система, кибербезопасность.*

DIGITAL TRANSFORMATION OF BANKING SERVICES AND CHALLENGES IN ENSURING CYBERSECURITY

Mengniyozov Anvar
Termez State University

Abstract. *This study is devoted to examining the issues of ensuring cybersecurity and the stable functioning of the banking system of Uzbekistan in the context of the rapid development of digital banking services. The digitalization of the banking sector has led to the emergence of new products and services, such as digital banks and financial ecosystems, thereby increasing the relevance of national financial and cybersecurity challenges. The purpose of the research is to characterize the main directions of the digital transformation of banking services within the context of cybersecurity. The article systematizes theoretical approaches to the concept of digital transformation of banking services, conducts a comparative analysis based on international experience, analyzes the dynamics of cyber threats and their target objects within the banking system of Uzbekistan, and develops proposals aimed at strengthening cybersecurity. The research findings have practical significance for the development of state regulation mechanisms and sustainable development strategies in the banking sector.*

Keywords: *digitalization, digital transformation, business models, cyber threats, banking system, cybersecurity.*

Kirish.

XXI asrning uchinchi o‘n yilligida jahon moliya tizimi o‘zining evolyutsion rivojlanishidagi eng keskin burilish nuqtalaridan birini – raqamli transformatsiya jarayonini boshdan kechirmoqda. “Sanoat 4.0” (Industry 4.0) inqilobi ta’sirida an’anaviy bank xizmatlari klassik “mijoz-bank” munosabatlaridan chiqib, murakkab va ochiq raqamli ekotizimlarga aylanib bormoqda. Bugungi kunda bank faoliyati nafaqat moliyaviy resurslarni boshqarish, balki katta hajmdagi ma’lumotlarni (Big Data) qayta ishlash, sun’iy intellekt va blokcheyn texnologiyalarini joriy etish orqali mijozlarga personallashtirilgan xizmatlarni taklif etmoqda.

Biroq, bank xizmatlarining raqamlashtirilishi va masofaviy boshqaruv kanallarining kengayishi (Remote Banking Services) medalyonning ikkinchi tomonini – kiberxavfsizlik muammolarining dolzarblashuvini yuzaga keltirdi. Moliya muassasalarining axborot tizimlari ochiqligining ortishi, “Fintex” kompaniyalarining bozorga kirib kelishi va bulutli texnologiyalarning qo‘llanilishi kiberjinoyatchilik uchun yangi hujum yo’nalishlarini yaratmoqda. Global miqyosda kuzatilayotgan tendensiya shuni ko‘rsatadiki, texnologik taraqqiyot qanchalik tezlashsa, axborot xavfsizligiga tahdidlar ko‘lami va murakkabligi ham shunchalik ortib bormoqda.

Ushbu global jarayonlardan O‘zbekiston iqtisodiyoti ham chetda qolgani yo‘q. Mamlakatimizda so‘nggi yillarda amalga oshirilayotgan keng ko‘lamli islohotlar, xususan, valyuta bozorining liberallashtirilishi va to‘lov tizimlarining rivojlanishi milliy bank tizimini yangi bosqichga olib chiqdi. O‘zbekistonda raqamli banklar (neobanklar), marketpleyslar va mobil to‘lov ilovalarining (Click, Payme va boshqalar) jadal ommalashuvi aholining moliyaviy xizmatlardan foydalanish imkoniyatini keskin oshirdi.

Shu bilan birga, O‘zbekiston bank-moliya sektorining raqamli makonga jadal integratsiyalashuvi milliy kiberxavfsizlik tizimi oldiga jiddiy vazifalarni qo‘ymoqda. Raqamli infratuzilmaning tezkor rivojlanishi va aholining raqamli savodxonligi darajasi o‘rtasidagi nomutanosiblik, shuningdek, bank mijozlariga nisbatan ijtimoiy muhandislikka (social engineering) asoslangan firibgarlik holatlarining ko‘payishi davlat va xususiy sektor hamkorligida himoya mexanizmlarini takomillashtirishni talab etadi.

Shu nuqtayi nazardan, O‘zbekistonda bank xizmatlarini raqamlashtirish jarayonlarini davlat tomonidan tartibga solishning strategik asoslarini tahlil qilish va xavfsiz raqamli muhitni

yaratish mexanizmlarini ishlab chiqish dolzarb ilmiy-amaliy ahamiyat kasb etadi.

O‘zbekiston Respublikasida milliy iqtisodiyotni raqamli transformatsiya qilish davlat siyosatining ustuvor yo‘nalishi sifatida belgilanishi va bu jarayonning O‘zbekiston Respublikasi Prezidentining 2020-yil 5-oktabrdagi “Raqamli O‘zbekiston – 2030” strategiyasini tasdiqlash va uni samarali amalga oshirish chora-tadbirlari to‘g‘risida”gi PF-6079-son Farmoni hamda “O‘zbekiston – 2030” strategiyasi bilan mustahkamlanishi barcha milliy institutlarni tashkil etish va tartibga solishda sifat jihatidan yangi bosqich boshlanganini anglatadi.

Mazkur strategik hujjatlar mamlakatimizda “Sanoat 4.0” (Industry 4.0) paradigmasini anglash, qabul qilish va unga bosqichma-bosqich o‘tish zaruratini taqozo etdi. Ushbu paradigmaning o‘zagini biznes-jarayonlarning to‘liq raqamlashtirilishi hamda ijtimoiy-iqtisodiy tizimning barcha ishtirokchilari – davlat, biznes va fuqarolar o‘rtasida uzluksiz va integratsiyalashgan axborot makonini shakllantirish tashkil etadi.

Natijada, jadal raqamlashtirish jarayonlari iqtisodiy va raqamli xavfsizlikka (kiberxavfsizlikka) doir yangi chaqiriq va tahdidlarning yuzaga kelishiga sabab bo‘lmoqda. Shu bois, ushbu transformatsiya jarayoni ijtimoiy-iqtisodiy tizimning turli agentlari va ilmiy hamjamiyat tomonidan turlicha baholanmoqda hamda raqamli imkoniyatlar bilan bir qatorda yuzaga keluvchi xatarlarni chuqur tadqiq etishni talab qilmoqda.

Adabiyotlar sharhi.

Raqamli iqtisodiyotga o‘tish va uning bank sohasi faoliyatiga ta’siri akademik doiralar hamda biznes vakillari tomonidan turlicha baholanmoqda.

Bir qator mualliflar bank mahsulotining iqtisodiy qiymatini yaratish va uni mijozga yetkazish jarayonida IT-sohaning roli sezilmas, biroq nihoyatda muhim tarzda monopollashib borayotganini ta’kidlaydilar (amalda raqamlashtirilgan mahsulotlarning ishlash mexanizmi uchun aynan IT sohasi yakka tartibda javobgar bo‘lib, bank esa faqat buyurtmachi va operator vazifasini bajaradi). Ba’zi mutaxassislarning fikricha, bozor pozitsiyalarini saqlab qolish (hatto ularni kengaytirish yoki mustahkamlash) maqsadida bank xizmatlarini raqamli transformatsiya qilish imkoniyatining o‘zi tashqi agentlar uchun ochiq bo‘lgan axborot chegaralarini qayta belgilashni talab etadi (Lebedeva, 2022; Dmitriyeva, 2020). Bu esa bank xizmatlari arxitekturasining xavfsizligi uchun ko‘plab yashirin tahdid va xatarlarni keltirib chiqaradi.

Bank xizmatlarining raqamli transformatsiyasi masalasi mahalliy va xorijiy ilmiy adabiyotlarda turlicha talqin etiladi. Xususan, O‘zbekiston Respublikasi Prezidentining “Raqamli O‘zbekiston – 2030” strategiyasida hamda sohaga oid milliy tadqiqotlarda raqamli transformatsiya – iqtisodiy o‘sishni jadallashtirish, aholiga qulaylik yaratish va shaffoflikni ta’minlashning asosiy drayveri sifatida e’tirof etiladi. Mazkur strategik yondashuvga ko‘ra, raqamli transformatsiya shunchaki yangi texnologiyalarni joriy etish emas, balki iqtisodiy faoliyatni shunday tashkil etish shaklidirki, unda raqamli shakldagi ma’lumotlar (Big Data) ishlab chiqarish va xizmat ko‘rsatishning asosiy omili hisoblanadi. Ularni yig‘ish, qayta ishlash va tahlil qilish orqali bank xizmatlari samaradorligi oshiriladi hamda an’anaviy boshqaruv modellari tubdan o‘zgartiriladi.

Gaysina (2017) bank xizmatlarining raqamli transformatsiyasini bank mahsulotlari va xizmatlarini Internet makonida amalga oshiriladigan start–end raqamli zanjirlar formatiga o‘tkazish jarayoni sifatida talqin qiladi. Muallif ushbu jarayonda texnologik uzluksizlik va raqamli kanallarning ustuvorligini asosiy omil deb hisoblaydi.

Lebedeva (2022) raqamli transformatsiyani bank mahsulotlari va xizmatlarini yaratish, boshqarish, realizatsiya qilish hamda ularga xizmat ko‘rsatish jarayonlari arxitekturasini jismoniy aloqalar o‘rnini bosuvchi raqamli makonga ko‘chirish bilan bog‘laydi. Ushbu yondashuvda bank va mijoz o‘rtasidagi o‘zaro munosabatlar formati tubdan o‘zgarib, raqamli muhit asosiy aloqa maydoniga aylanadi.

Dudin, Shkodinskiy va Usmanov (2021) bank xizmatlarining raqamli

transformatsiyasini Internet paradigmasining axborot izlash vositasidan barcha obyektlar va jarayonlar o‘rtasidagi o‘zaro aloqalarni ta’minlovchi global ekotizimga aylanishi bilan bog‘laydilar. Mualliflar bank faoliyatini amalga oshirish uchun prinsipial jihatdan yangi infratuzilmani shakllantirish zarurligini ta’kidlaydilar.

Xorijiy tadqiqotlarda mazkur tushuncha yanada kengroq talqin etiladi. Jumladan, Uddin (2020) raqamli transformatsiyani raqamli texnologiyalar salohiyatini bankning moliyaviy mahsulotlari va servislariga integratsiya qilish orqali iqtisodiy qo‘shilgan qiymat yaratishga qaratilgan strategiya sifatida baholaydi. Bu yondashuvda transformatsiya samaradorlik va qiymat yaratish mezonlari bilan chambarchas bog‘liq.

Ghauri (2021) bank xizmatlarining raqamli transformatsiyasini yangi bozor sharoitlari va ishbilarmonlik xulq-atvori paradigmasi doirasida bankning raqobatbardoshligini ta’minlash maqsadida uning xizmatlarini tubdan qayta tashkil etish jarayoni sifatida izohlaydi. Muallif raqamli transformatsiyani majburiy strategik choralar sifatida ko‘radi.

Tripathi (2021) raqamli transformatsiyani uzluksiz axborot makonida xususiy va ommaviy tijorat manfaatlari amalga oshiriladigan yangi tashkiliy-huquqiy va iqtisodiy konstruksiyani shakllantirish jarayoni sifatida talqin qiladi. Bu yondashuv institutsional va huquqiy o‘zgarishlarga alohida urg‘u beradi.

Jibril (2020) esa bank xizmatlarining raqamli transformatsiyasini biznes-jarayonlarni virtual muhitga ko‘chirish bo‘yicha bozor ishtirokchilarining muayyan “kelishuvi” sifatida izohlaydi. Uning fikricha, mazkur jarayonda mahsulot va servislar aniq mijoz talablariga mos holda, smart manufacturing (aqlli ishlab chiqarish) tamoyillari asosida loyihalanadi.

Umuman olganda, keltirilgan adabiyotlar tahlili shuni ko‘rsatadiki, mahalliy olimlar bank xizmatlarining raqamli transformatsiyasini ko‘proq infratuzilmaviy va institutsional jihatlar orqali izohlasalar, xorijiy tadqiqotchilar ushbu jarayonni strategik qayta tashkil etish, raqobatbardoshlik va qiymat yaratish mexanizmlari bilan bog‘laydilar. Mazkur farqlar bank sektorida kiberxavfsizlikni ta’minlash yondashuvlarining ham turlicha shakllanishiga sabab bo‘ladi.

Tadqiqot metodologiyasi.

Mazkur tadqiqot bank xizmatlarining raqamli transformatsiyasi va kiberxavfsizlik muammolarini tahlil qilishga qaratilgan bo‘lib, unda umumilmiy va maxsus ilmiy usullar qo‘llanildi. Nazariy qismda kuzatish, taqqoslash, tahlil va sintez, mantiqiy mushohada yuritish hamda ilmiy adabiyotlarning tanqidiy sharhi orqali bank xizmatlarining raqamli transformatsiyasiga doir yondashuvlar tizimlashtirildi. Tahliliy qismda statistik tahlil va grafik usullaridan foydalanildi. Tadqiqotning yakuniy bosqichida kiberxavfsizlikni kuchaytirishga doir amaliy takliflarni ishlab chiqishda ekspert usulidan foydalanildi.

Tahlil va natijalar muhokamasi.

Ilmiy tadqiqotning nazariy bo‘limi doirasida, shuningdek, jahon amaliyotida qo‘llaniladigan bank xizmatlarini raqamli transformatsiya qilish yondashuvlarining komparativ tavsifi ishlab chiqildi. Mazkur tavsif raqamli muhitda xavfsizlikni ta’minlash kontekstida ushbu yondashuvlarning kuchli va zaif jihatlarini yanada chuqurroq anglash imkonini beradi (1-jadval).

Bank xizmatlarini raqamli transformatsiya qilish yondashuvlarining komparativ tahlili shuni ko‘rsatadiki, bank biznes-jarayonlariga raqamli texnologiyalarning kirib borish darajasi qanchalik yuqori bo‘lsa, bank shunchalik ko‘p turdagi kiberxatarlar ta’siriga duchor bo‘ladi.

Albatta, raqamli iqtisodiyotga o‘tish sharoitida banklarning xavfsiz faoliyat yuritishini ta’minlash faqatgina xakerlik hujumlaridan yoki muhim infratuzilmani himoyalash muammolari bilan cheklanib qolmaydi. Aksincha, mazkur vazifa iqtisodiy, texnologik, kadrlar salohiyati va regulyator xususiyatiga ega bo‘lgan juda keng omillar doirasini tahlil qilishni talab etadi. Biroq yangi davr banklari uchun real va potensial chaqiriqlar hamda tahdidlar

to‘g‘risidagi statistik ma’lumotlarning cheklanganligini inobatga olgan holda (ushbu masala bankni rivojlantirish strategiyasining alohida bo‘limida yoritiladi, biroq tushunarli sabablarga ko‘ra u tijorat siri hisoblanadi), ilmiy tadqiqotda asosiy e’tibor O‘zbekiston bank tizimidagi kiberxatarlarning dinamikasi, tuzilmasi va obyektlari tahliliga, shuningdek bank tizimi regulyator mexanizmlarining nomukammalligi bilan bog‘liq muammolarga qaratiladi.

1-jadval

Bank xizmatlarini raqamli transformatsiya qilish yondashuvlarining komparativ tavsifi

Yondashuv	Asosiy tavsif (umumlashtirilgan)
1. Raqamli kanallarga ega klassik bank	An’anaviy bank biznes-modelini saqlab qolgan holda, raqamli texnologiyalarni qo‘shimcha xizmat kanali sifatida joriy etishga asoslangan yondashuv. Transformatsiya fragmentar xarakterga ega bo‘lib, jismoniy infratuzilma ustuvorligicha qoladi.
2. Klassik bankning raqamli filiali	Bank tarkibida alohida raqamli bo‘linma tashkil etish orqali yangi texnologiyalarni sinovdan o‘tkazish va bosqichma-bosqich joriy etishga yo‘naltirilgan yondashuv. Raqamli va an’anaviy modellarning parallel mavjudligi bilan tavsiflanadi.
3. Raqamli bank brendi	Bank faoliyatini to‘liq qayta formatlashni nazarda tutuvchi, raqamli rebrending va biznes-jarayonlarni tizimli raqamlashtirishga asoslangan yondashuv. Innovatsiyalarni tez joriy etishga yo‘naltirilgan strategik model hisoblanadi.
4. To‘liq raqamli bank	Jismoniy infratuzilmadan voz kechgan holda, greenfield tamoyili asosida to‘liq raqamli bank mahsulotlari va servislarini yaratishga qaratilgan yondashuv. Mijozga yo‘naltirilganlik va texnologik moslashuvchanlik bilan ajralib turadi. (Neobank)
5. Bank raqamli ekotizimi / moliyaviy metakoinot	Bank, moliyaviy va nomoliyaviy servislarni yagona raqamli platformada birlashtiruvchi kompleks model. Mijozning moliyaviy va kundalik ehtiyojlarini qamrab oluvchi ekotizim shakllantirishga yo‘naltirilgan.

Manba: *muallif tomonidan tayyorlangan.*

Ilmiy tadqiqot muammosini yoritishda foydalanilgan statistik ma’lumotlar bazasini shakllantirishda rasmiy va verifikatsiyadan o‘tgan axborot manbalariga tayanildi. Xususan, statistik axborotning asosiy manbalari sifatida O‘zbekiston Respublikasi Markaziy bankining bank tizimi barqarorligi va raqamli moliyaviy xizmatlar rivoji bo‘yicha yillik tahliliy hisobotlari*, Ichki ishlar vazirligi Kiberxavfsizlik markazining rasmiy statistikasi, shuningdek, “CERT-UZ” (Kiberxavfsizlik hodisalariga qarshi kurashish markazi)ning milliy segmentdagi kiberxatarlar dinamikasiga oid umumlashtiruvchi sharhlari va davriy byulletenlari xizmat qildi.

2-jadvalda 2021–2024 yillar davomida O‘zbekiston bank tizimida kuzatilgan kiberxatarlar (kiberhujumlar) dinamikasi aks ettirilgan. Jadvalda keltirilgan ma’lumotlardan ko‘rinib turibdiki, tahlil qilinayotgan davrda O‘zbekiston bank tizimi tobora ko‘proq kiberhujumlarga duch kelgan. Xususan, 2021-yildan boshlab tizimli ahamiyatga ega banklarga nisbatan kiberhujumlar faolligining oshgani kuzatiladi. Bu holatni kiberhujumlarni amalga oshiruvchi subyektlar tomonidan bank tizimini izdan chiqarish, jamiyatda vahima kayfiyatini shakllantirish hamda yirik banklar top-menejmentini obro‘sizlantirish maqsadidagi harakatlar natijasi sifatida ham baholash mumkin. Ikkinchi muhim jihat sifatida fintex vakillariga nisbatan kiberhujumlar sonining jadal o‘sishi qayd etiladi. Umuman olganda, bu holat mijozlarning klassik banklardan ko’ra o‘zaro munosabatlarda nisbatan moslashuvchan qoidalarga amal qiladigan va regulyator cheklovlariga kamroq duch keladigan nobank kredit-moliya tashkilotlarini (NKMT) afzal ko‘rayotganligi bilan bog‘liq global tendensiyani aks ettiradi. Aynan shu holat ularning kriminal elementlar uchun ma’lum darajada “nomaqbul”, biroq jozibador obyektga aylanishiga sabab bo‘lmoqda.

2-jadval

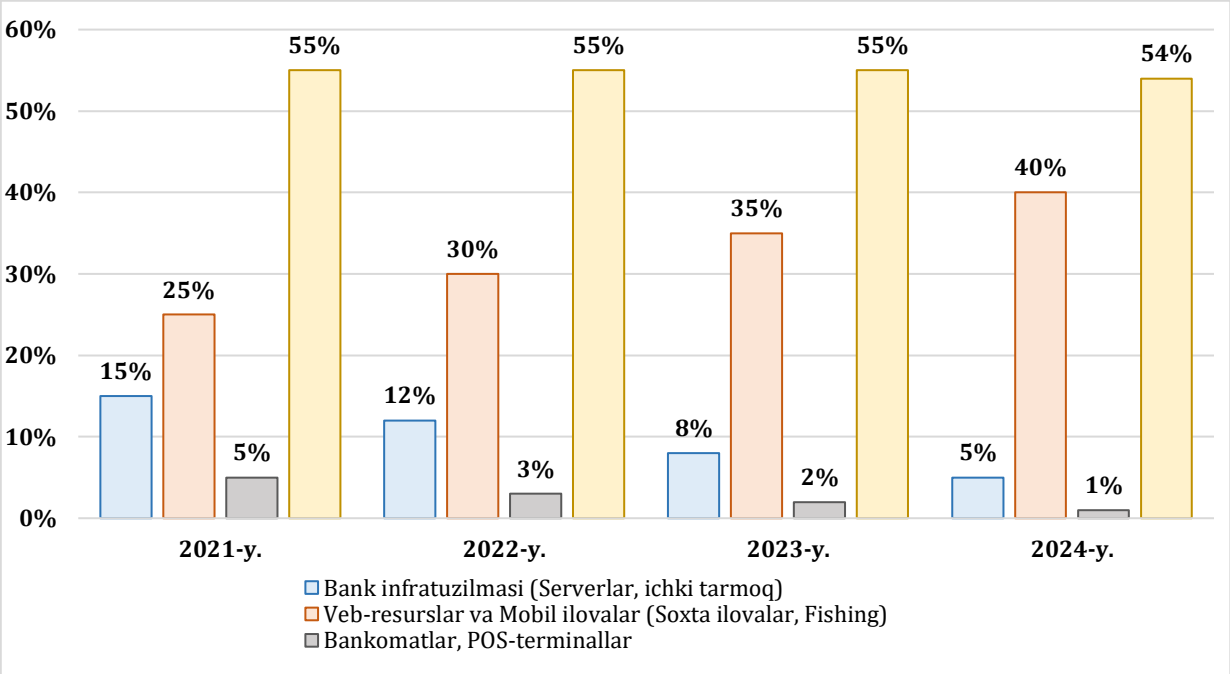
O‘zbekiston bank-moliya tizimida kiberxatarlar va kiberjinoyatlar dinamikasi (2021–2024 yillar)

Ko‘rsatkichlar	2021 y.	2022 y.	2023 y.	2024 y.
1. O‘zbekiston axborot makonida qayd etilgan umumiy kiberhujumlar soni, mln dona	**~5,5**	**~8,0**	**11,2**	**12,0+**
Jumladan:				
1.1. Davlat va bank sektoriga yo‘naltirilgan hujumlar ulushi (taxminiy)	Yuqori	Yuqori	Yuqori	Yuqori
2. Qayd etilgan kiberjinoyatlar soni (bank kartalari va moliya bilan bog‘liq), dona	**~2 500**	**~4 000**	**~8 000**	**58 800***
Jumladan:				
2.1. Bank kartalari bilan bog‘liq jinoyatlar ulushi (jami kiberjinoyatlar ichida)	~90%	90%+	95%	98%
3. Kiberjinoyatlar oqibatida yetkazilgan moddiy zarar miqdori, mlrd so‘m	**~100**	**~250**	**~400**	**603**
Jumladan:				
3.1. Fuqarolar va bank mijozlari ko‘rgan zarar (2021–2024 jami: 1,9 trln so‘m)	–	–	–	603
4. Bank sektorining raqamli himoyalanganlik indikatorlari				
4.1. Global kiberxavfsizlik indeksi (GCI) bo‘yicha o‘rni	70+	80+	94	89 (T2 guruhi)
4.2. Hujumlarning asosiy vektori (bank mijozlariga nisbatan)	Ijtimoiy muhandislik	Ijtimoiy muhandislik	Telegram/ APK viruslar	Soxta havolalar va dasturlar (60%)
5. Raqamli savodxonlik va gigiyena				
5.1. Firibgarlik qurbonlari orasida moliyaviy savodxonlik yetishmasligi darajasi	Yuqori	Yuqori	Yuqori	Yuqori

Manba: *muallif tomonidan tayyorlangan.*

Kiberhujumlar sonining ortishi bilan banklarga yetkazilgan moliyaviy zarar hajmi ham oshib bormoqda. Shu bilan birga, 2021-yildan boshlab bunday hujumlardan keyin banklarning normal faoliyatini tiklash xarajatlari deyarli besh baravar oshgani, shuningdek mijozlar ishonchi va bank imijining yo‘qotilishi bilan bog‘liq bilvosita yo‘qotishlar to‘rt baravar ko‘payganini alohida ta’kidlash lozim. Bundan tashqari, mazkur holatlar bank regulyatori e’tiborining kuchayishiga va rejadan tashqari kompleks tekshiruvlarning o‘tkazilishiga olib kelgan. O‘zbekiston bank tizimidagi zaif nuqtalarni aniqlash maqsadida 2021–2024 yillar davomida kiberhujumlar obyektlarining tuzilmasi ko‘rib chiqildi (1-rasm).

Keltirilgan ma’lumotlarga ko‘ra, tahlil qilinayotgan davrda O‘zbekiston bank sektoriga uyushtirilgan kiberhujumlar arxitekturasida tub burilish (transformatsiya) jarayoni kuzatilmoqda. Xususan, kiberjinoyatchilarning e’tibori “qiyin nishonlar” dan (bank serverlari) “oson o‘ljalar”ga (mijozlar va ularning gadjetlariga) ko‘chgani yaqqol namoyon bo‘lmoqda.



1-rasm. O‘zbekiston bank tizimida kiberhujumlar obyektlari tuzilmasi (2021–2024 yillar), % hisobida

Manba: *muallif tomonidan tayyorlangan.*

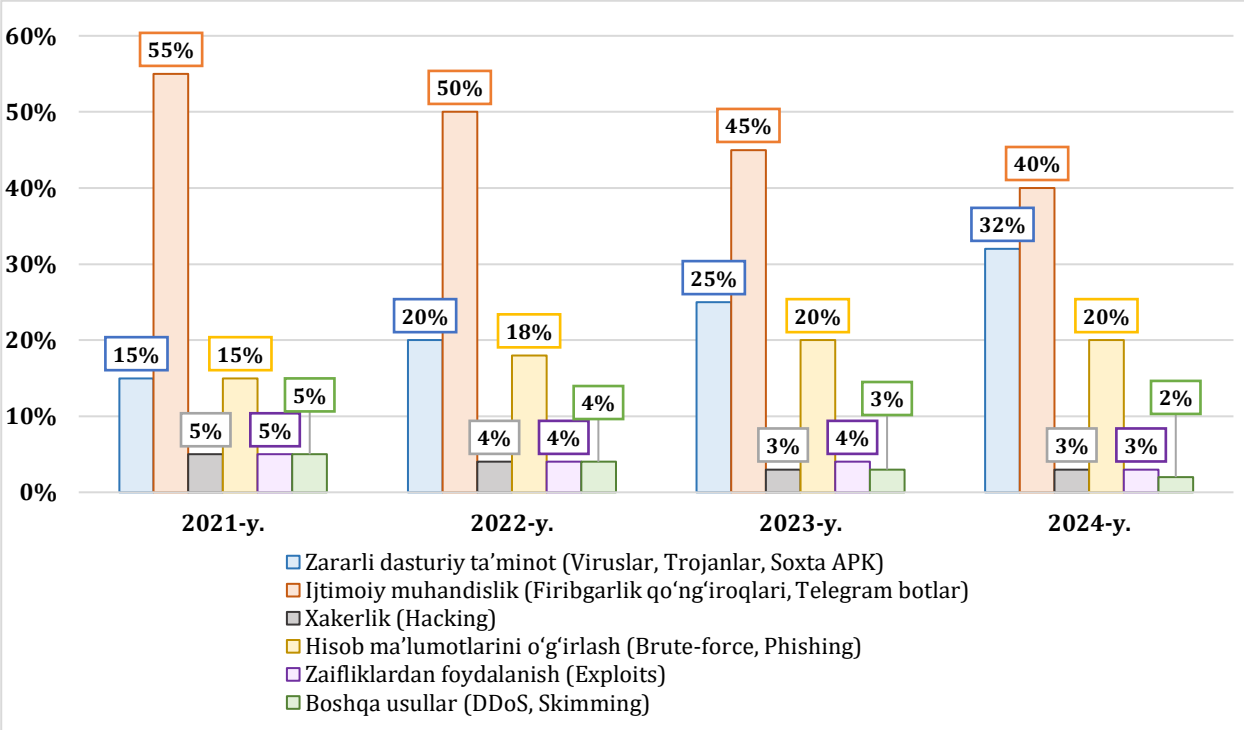
Birinchidan, bank infratuzilmasi (serverlar va ichki tarmoqlar)ga to‘g‘ridan-to‘g‘ri qaratilgan hujumlar ulushi keskin qisqarish tendensiyasiga ega. Agar 2021-yilda umumiy hujumlarning 15 foizi banklarning himoya tizimlarini buzib kirishga qaratilgan bo‘lsa, 2024-yilga kelib bu ko‘rsatkich 3 barobarga kamayib, 5 foizni tashkil etgan. Bu holat mahalliy banklarning kiberhimoya tizimlari (Firewall, DLP, SOC markazlari) mustahkamlanganini va jinoyatchilar uchun bankning markaziy serverlarini buzish iqtisodiy jihatdan qimmat va samarasiz bo‘lib borayotganini anglatadi.

Ikkinchidan, kiberhujumlarning og‘irlik markazi veb-resurslar va mobil ilovalarga (soxta ilovalar, fishing) siljigan. Tahlil davrida ushbu yo‘nalishdagi hujumlar ulushi 25 foizdan (2021 y.) 40 foizga (2024 y.) o‘sgan. Bu O‘zbekistonda masofaviy bank xizmatlari ommalashuvi fonida yuzaga kelgan bo‘lib, xakerlar rasmiy ilovalarning soxta nusxalarini (Fake APK) tarqatish va fishing saytlar orqali foydalanuvchilarni aldash yo‘lini tanlamoqda.

Uchinchidan, eng xavotirli tendensiya – bu shaxsiy ma’lumotlar va mijoz hisoblariga qaratilgan “Ijtimoiy muhandislik” (Social engineering) hujumlarining mutlaq dominantligidir. 2021–2024 yillar davomida bu ko‘rsatkich barqaror ravishda yuqori (54–55 foiz) bo‘lib turibdi. Bu shuni ko‘rsatadiki, O‘zbekistonda kiberxavfsizlikning eng zaif bo‘g‘ini texnologiya emas, balki inson omilidir. Jinoyatchilar murakkab kodlar yozish o‘rniga, fuqarolarning ishonuvchanligidan va raqamli savodxonligi pastligidan foydalanib, kodlarni o‘zlariga aytishga majburlash (vishing) yoki soxta havolalarga kiritish (smishing) usullarini qo‘llamoqda.

To‘rtinchidan, bankomatlar va POS-terminallarga qaratilgan hujumlar (skimming) deyarli yo‘qolish arafasida (2021-yildagi 5 foizdan 2024-yilda 1 foizgacha tushgan). Naqd pul muomalasining qisqarishi va raqamli to‘lovlarning rivojlanishi jinoyatchilar uchun bankomatlarni jismoniy buzish yoki ularga qurilma o‘rnatishni foydasiz mashg‘ulotga aylantirdi.

2-rasmda banklarga qarshi kiberhujumlarni amalga oshirishda eng ko‘p qo‘llaniladigan vositalar tuzilmasini aks ettiruvchi diagramma keltirilgan bo‘lib, u bank menejmenti va regulyator uchun asosiy e’tibor nuqtalari (xavf zonalari)ni aniqlash imkonini beradi.



2-rasm. 2020–2024 yillarda banklarga kiberhujumlarni amalga oshirishda qo'llanilgan instrumentlar tuzilmasi, %

Manba: *muallif tomonidan tayyorlangan.*

Keltirilgan ma'lumotlardan ko'rinib turibdiki, O'zbekiston banklari va ularning mijozlari uchun asosiy tahdid manbai ijtimoiy muhandislik (Social engineering) usullari hisoblanadi. Tahlil qilinayotgan davrda ushbu instrument barcha hujumlarning o'rtacha 47,5 foizini (2021-yilda 55 foizdan 2024-yilda 40 foizgacha) tashkil etgan.

Ikkinchi o'rinda zararli dasturiy ta'minot (Malware, xususan soxta mobil ilovalar va troyanlar) turadi. E'tiborli jihati shundaki, ushbu tahdid turi dinamik o'sish tendensiyasiga ega bo'lib, 2021-yildagi 15 foizdan 2024-yilda 32 foizgacha ko'tarilgan. Uchinchi o'rinda esa hisob ma'lumotlarini o'g'irlash (fishing va brute-force) usullari (20 %) qayd etilgan bo'lib, klassik xakerlik hujumlari (hacking) ulushi juda past darajada (3 %) qolmoqda.

Tahlil qilinayotgan davrda O'zbekiston Respublikasi Markaziy banki va "Kiberxavfsizlik markazi" (CERT-UZ) tomonidan moliya tizimining xavfsizligini ta'minlash yo'nalishida qator institutsional choralar ko'rildi. Xususan, "Kiberxavfsizlik to'g'risida"gi Qonunning qabul qilinishi bilan banklarga nisbatan axborot xavfsizligi bo'yicha minimal talablar kuchaytirildi hamda bank ilovalarida biometrik identifikatsiya (Face-ID) tizimlari keng joriy etildi.

Shu bilan birga, bank tizimida an'anaviy "dushmanni tashqarida ushlab turish" (perimeter himoyasi) modeli O'zbekiston sharoitida ham o'z samaradorligini qisman yo'qotmoqda. Bunga sabab – raqamli xizmatlarning ommaviylashuvi va ijtimoiy muhandislikning dominantligidir. Bugungi kunda jinoyatchilar bankning kuchli himoyalangan serverlarini buzish o'rniga, mijozning shaxsiy mobil qurilmalarini (gadjetlarini) nishonga olmoqdalar. Bu esa kiberxavfsizlikni ta'minlashda texnik choralardan ko'ra, aholining "raqamli gigiyenasi" va moliyaviy savodxonligini oshirish masalasini birinchi o'ringa olib chiqmoqda.

Shu bilan birga, bank tizimida zaif jihatlar hanuzgacha yetarlicha mavjud. Shundan kelib chiqib, mualliflar quyidagi takliflarni amalga oshirishni maqsadga muvofiq deb hisoblaydilar:

O'zbekistonda tizimli ahamiyatiga ega banklar bilan hamkorlikda banklar faoliyatining axborot xavfsizligini ta'minlash bo'yicha milliy himoya liniyasini yaratish tashabbusini amalga oshirishi lozim. Mazkur tizim Buyuk Xitoy fayrvoli analogi sifatida faoliyat yuritib, ma'lum to'lov evaziga barcha banklarni ulash imkonini beradi. Bu banklarga xususiy axborot xavfsizligi

tizimlariga bo‘lgan xarajatlarni qisqartirish imkonini beradi. Bunday tizimning asosiy afzalligi axborot makonidagi barcha dolzarb chaqiriq va tahdidlar bo‘yicha real vaqt rejimida axborot almashinuvi, shuningdek barcha hujumlar faktlarini qayd etish imkoniyatidir. G.Grefning fikriga ko‘ra, moliyaviy bo‘lmagan sektor kompaniyalarining 80,0 foizdan ortig‘i kiberhujumlar faktini yashiradi, bu esa keyinchalik bank tizimiga tarqalishi mumkin, banklarning o‘zi ham har beshinchi muvaffaqiyatli hujumni oshkor etmaydi.

Olib borilgan tadqiqotlar va xorijiy tajriba tahlili shuni ko‘rsatmoqdaki, O‘zbekistonda bank xizmatlarining jadal raqamlashtirilishi sharoitida kiberxavfsizlikni ta’minlashga yangicha va tizimli yondashuv zarur. Xorijiy bank tizimlari misolida ko‘rilgan amaliyotlarni milliy iqtisodiyotimiz xususiyatlaridan kelib chiqib tatbiq etish bir qator ijobiy natijalarni berishi mumkin.

Avvalo, bank tizimida resurslardan samarali foydalanish maqsadida kiberxavfsizlik xizmatlarini autsorsing asosida ko‘rsatish amaliyotini kengaytirish maqsadga muvofiqdir. Hozirgi kunda kichik banklar va mikromoliya tashkilotlari uchun o‘zlarining mustaqil va qimmatbaho himoya markazlarini tashkil etish iqtisodiy jihatdan og‘irlik qilmoqda. Shu bois, yirik tijorat banklari yoki IT-Park rezidentlari negizida shakllangan kuchli xavfsizlik markazlari (Security Operations Center) orqali bozorning boshqa ishtirokchilariga “xizmat sifatida xavfsizlik” modelini taklif etish, sohada himoya darajasini birxillashtirishga va xarajatlarni optimallashtirishga xizmat qiladi.

Shu bilan birga, texnologik suverenitetni ta’minlash masalasi ham dolzarb bo‘lib turibdi. Xorijiy himoya vositalariga to‘liq qaramlikni kamaytirish uchun AKT sohasida import o‘rnini bosish dasturlari doirasida milliy kiberxavfsizlik startaplarini va “Fintex” loyihalarini moliyaviy qo‘llab-quvvatlash lozim. Buning uchun “Aloqabank” venchur jamg‘armasi, “UzVC” va boshqa institutlar imkoniyatlarini birlashtirib, istiqbolli mahalliy loyihalarni davlat buyurtmalari orqali rag‘batlantirish tizimini yo‘lga qo‘yish kerak. Bu nafaqat xavfsizlikni oshiradi, balki mamlakat ichida kuchli IT-ekotizim shakllanishiga turtki beradi.

Yana bir muhim jihat – bu sohada davlat nazorati va rag‘batlantirish mexanizmlarining uyg‘unligidir. Bank sektori subyektlari uchun kiberxavfsizlik bo‘yicha minimal majburiy talablarni qat’iylashtirish va eng muhimi, ularning ijrosini baholovchi aniq nazorat indikatorlarini (KPI) joriy etish zarur. Agar Markaziy bank tomonidan banklarning kiberhimoyalanganlik reytingi muntazam e’lon qilib borilsa, bu banklar o‘rtasida sog‘lom raqobatni yuzaga keltirib, ularni xavfsizlikka investitsiya kiritishga undaydi.

Nihoyat, kelajak istiqbollarini inobatga olgan holda, strategik ahamiyatga ega moliyaviy operatsiyalarda shaffoflikni ta’minlash uchun Markaziy bankning “Raqamli so‘m” platformasidan foydalanishni sinovdan o‘tkazish lozim. Blokcheyn texnologiyasiga asoslangan ushbu mexanizm yirik davlat xaridlari va investitsiya mablag‘larining harakatini to‘liq nazorat qilish imkonini beradi, bu esa o‘z navbatida kiberfiribgarlik va korrupsiya xatarlarini minimallashtirishda samarali vosita bo‘lib xizmat qiladi. Mazkur takliflarning kompleks tarzda amalga oshirilishi milliy bank tizimining barqarorligini oshirishga mustahkam zamin yaratadi.

Xulosa va takliflar.

Raqamli transformatsiya sharoitida O‘zbekiston bank sektorining xavfsizligini ta’minlash masalasi murakkab va ko‘p qirrali xususiyatga ega bo‘lib, mazkur tadqiqot doirasida uning fundamental yo‘nalishlaridan faqat bittasi – banklarning kiberxavfsizligi masalasi ko‘rib chiqildi. Aynan ushbu yo‘nalish zamonaviy sharoitda tobora keng ko‘lam kasb etib bormoqda.

Raqamli iqtisodiyotga o‘tish va uning bank sohasiga ta’siri IT-soha tomonidan samarali transformatsiya jarayonlaridagi rolning sezilmas, biroq nihoyatda muhim darajada monopollashuvi sababli bir ma’noli baholanmayapti.

O‘zbekiston bank sektorining xavfsiz faoliyat yuritish strategiyasini tahlil qiladigan bo‘lsak, uning asosiy xususiyatlari markazlashgan nazorat va texnologik ta’minotning o‘ziga xosligida namoyon bo‘ladi. Xususan, butun moliya bozori bo‘yicha yuzaga kelayotgan chaqiriq

va tahdidlarni monitoring qilish vazifasi yagona institutsional muvofiqlashtiruvchi organlar – O‘zbekiston Respublikasi Markaziy banki hamda “Kiberxavfsizlik markazi” (CERT-UZ) hamkorligida amalga oshirilishiga alohida urg‘u beriladi.

Shuningdek, strategiyaning yana bir muhim jihati shundaki, tizim ahamiyatiga ega bo‘lgan yirik tijorat banklari hamda bank tizimining muhim infratuzilma obyektlari barqarorligini ta’minlashda, asosan, xalqaro standartlarga javob beruvchi va sinovdan o‘tgan tayyor axborot xavfsizligi mahsulotlarini xarid qilishga hamda ularni joriy etishga ustuvorlik beriladi. Bu yondashuv banklarga murakkab himoya tizimlarini noldan yaratishga vaqt sarflamasdan, jahon tajribasida o‘zini oqlagan yechimlar orqali xavfsizlik perimetrini tezkor mustahkamlash imkonini beradi.

Olib borilgan tadqiqotlar natijalaridan kelib chiqqan holda, bank xizmatlarining raqamli transformatsiyasi sharoitida kiberxavfsizlikni ta’minlash samaradorligini oshirish maqsadida quyidagi takliflarni ilgari surish maqsadga muvofiq hisoblanadi:

1. O‘zbekiston Respublikasi Markaziy banki huzurida bank-moliya sektori uchun ixtisoslashgan yagona Muvofiqlashtiruvchi markaz (Fin-CERT.UZ) faoliyatini takomillashtirish.

2. Bank sektori subyektlari (shu jumladan, mikromoliya tashkilotlari va fintex-kompaniyalar) uchun axborot xavfsizligi bo‘yicha majburiy minimal talablarni (O‘z DSt ISO/IEC 27001 standarti asosida) qat’iylashtirish.

3. Kichik banklar va kredit tashkilotlari uchun axborot xavfsizligi xarajatlarini optimallashtirish maqsadida, yirik davlat banklari yoki ixtisoslashgan IT-park rezidentlari negizida “Xizmat sifatida kiberxavfsizlik” (Security as a Service) modelini rivojlantirish.

4. Bank xavfsizligini ta’minlashda xorijiy vendorlarga qaramlikni kamaytirish maqsadida, kiberxavfsizlik yechimlarini (antifrod tizimlari, biometrik identifikatsiya, shifrlash vositalari) ishlab chiquvchi milliy IT-kompaniyalarni grantlar va soliq imtiyozlari orqali rag‘batlantirish.

5. Ijtimoiy muhandislikka (firibgarlikka) qarshi kurashishning eng samarali yo‘li sifatida, Markaziy bank va tijorat banklari hamkorligida “Raqamli moliyaviy savodxonlik” milliy dasturini amalga oshirish.

6. Strategik ahamiyatga ega to‘lovlar va budjet mablag‘lari harakati shaffofligini ta’minlash maqsadida, blokcheyn texnologiyasiga asoslangan milliy raqamli valyuta (“Raqamli so‘m”) platformasini bosqichma-bosqich sinovdan o‘tkazish va amaliyotga joriy etish.

Maqolada ilgari surilgan takliflarni amaliyotga joriy etish banklarning raqamlashtirish bilan bog‘liq chaqiriq va tahdidlardan himoyalanishini ta’minlash bo‘yicha amaldagi xavfsizlik tizimining zaif jihatlarini bartaraf etishga sezilarli darajada xizmat qilishi mumkin.

Adabiyotlar/Литература/References:

Dmitrieva, G.S. (2020) ‘Цифровые технологии в банковском секторе экономики.’ Известия Санкт-Петербургского государственного экономического университета, № 7, С. 49–54.

Dudin, M.N., Shkodinskiy, S.V. and Usmanov, D.I. (2021) ‘Ключевые тенденции и закономерности развития цифровых бизнес-моделей банковских сервисов в Индустрии 4.0.’ Финансы: теория и практика, № 25(5), С. 59–78.

Gaysina, D.V. (2017) ‘Transformation of Modern Business Models into Ecosystems.’ Design. Busin. Architect., pp. 215–223.

Ghauri, F.A. (2021) ‘Why Financial Sectors Must Strengthen Cybersecurity.’ International Journal of Computer Science and Information Security (IJCSIS), № 19(7).

Gontar, L.O. (2021) ‘Смарт-подходы в цифро-финансовой экосистеме: финтех в условиях применения цифровых платформ и умного контроля.’ E-Management, № 4(2), С. 44–50.

Jibril, A.B., Kwarteng, M.A., Chovancova, M. and Denanyoh, R. (2020) ‘Customers’ perception of cybersecurity threats toward e-banking adoption and retention: A conceptual study.’

Proceedings of the 15th International Conference on Cyber Warfare and Security (ICCWS), pp. 270–276.

Kosarev, V.E. (2020) 'О цифровой эволюции банков в направлении необанков.' Финансовые рынки и банки, № 3, С. 56–61.

Lebedeva, I.A. (2022) 'Цифровая трансформация банковского сектора России: возможности и риски для банков и их клиентов.' Социальные новации и социальные науки, № 1, С. 74–85.

O'zbekiston Respublikasi Prezidenti farmoni (2020) "Raqamli O'zbekiston-2030" strategiyasini tasdiqlash va uni samarali amalga oshirish chora-tadbirlari to'g'risida, PF-6079-son, 2020-yil 5-oktyabr.

Omelehina, N.V. (2017) 'Финансовый суверенитет государства: к постановке проблемы исследования правовой идентификации.' Финансовое право, № 4, С. 12–21.

O'zbekiston Respublikasi Markaziy banki (2024) Moliyaviy barqarorlik sharhi.

Ryabicheva, O.I. (2021) 'Цифровизация розничных банковских услуг в российской федерации на современном этапе.' Журнал прикладных исследований, № 6-9, С. 896–905.

Sokolinskaya, N.Э. and Zinovyeva, E.A. (2020) 'Анализ готовности российских коммерческих банков к цифровизации экономики в условиях трансформации мирового рынка.' Финансовые рынки и банки, № 4, С. 50–57.

Tripathi, S. and Gupta, M. (2021) 'A holistic model for Global Industry 4.0 readiness assessment.' Benchmarking, № 28(10), pp. 3006–3039.

Uddin, M.H., Mollah, S. and Ali, M.H. (2020) 'Does cyber tech spending matter for bank stability?' International Review of Financial Analysis, № 72.

Urazova, S.A. (2021) 'Цифровая трансформация банковских систем как основа перехода к новому периоду их эволюции.' Финансовые исследования, № 2(71), С. 55–66.

Vakulyk, O., Petrenko, P., Kuzmenko, I., Pochtovyi, M. and Orlovskyi, R. (2020) 'Cybersecurity as a component of the national security of the state.' Journal of Security and Sustainability Issues, № 9(3), pp. 775–784.

Zverkova, T.N. (2018) 'Региональные банки и FinTech: противостояние или партнерство.' Финансы и кредит, № 24(12), С. 2771–2782.

Алонцева, В.Р. (2018) 'Оценка состояния цифрового банкинга в РФ.' Международный журнал гуманитарных и естественных наук, № 5(2), С. 88–91.

Андреева, О.В. (2014) 'Технологический и финансовый суверенитет Российской Федерации: проблемы, противоречия, механизмы обеспечения.' Journal of Economic Regulation (Вопросы регулирования экономики), № 4(5), С. 126–135.

Шкодинский, С.В., Дудин, М.Н. и Усманов, Д.И. (2021) 'Анализ и оценка киберугроз национальной финансовой системе России в цифровой экономике.' Финансовый журнал, № 13(3), С. 38–53.