AKTUAR MOLIYA VA BUXGALTERIYA HISOBI ILMIY JURNALI

Vol. 6 Issue 06 | **pp.** 159-166 | **ISSN**: 2181-1865
Available online https://finance.tsue.uz/index.php/afa

NAQD PULSIZ TO‘LOV TIZIMLARIDA XAVFSIZLIKNI TA’MINLASH VA ULARNI RIVOJLANTIRISH YO‘NALISHLARI

Niyozov Zuxur Davronovich
Samarqand iqtisodiyot va servis instituti,
“Bank ishi” kafedrasi i.f.n., professor v.b.
Ataboyev Ilhomjon
SamISI, “Bank-moliya xizmatlari” fakulteti talabasi
Raxmatova Nilufar
SamISI, “Bank-moliya xizmatlari” fakulteti talabasi

Annotatsiya. Ushbu maqolada naqd pulsiz to‘lov tizimlarida xavfsizlikni ta’minlashning nazariy va amaliy jihatlari, shuningdek, mazkur tizimlarni yanada rivojlantirish yo‘nalishlari kompleks ravishda tadqiq etilgan. Tadqiqot doirasida O‘zbekistonda elektron to‘lov vositalaridan foydalanish statistikasi tahlil qilinib, naqd pulsiz hisob-kitoblarda yuzaga keladigan asosiy xavf-xatarlar, jumladan, fishing, karta ma’lumotlarini o‘g‘irlash va ijtimoiy muhandislik hujumlari ilmiy asosda tasniflangan. Maqolada tokenizatsiya, ko‘p faktorli autentifikatsiya va kriptografik himoya usullari kabi zamonaviy texnologik yechimlar keng o‘rganilgan. Tadqiqot natijalari asosida O‘zbekiston sharoitiga moslashtirilgan naqd pulsiz to‘lov xavfsizligining kompleks modeli taklif qilinib, tizimni rivojlantirish bo‘yicha amaliy tavsiyalar ishlab chiqilgan.

Kalit so‘zlar: naqd pulsiz to‘lov, elektron to‘lov xavfsizligi, tokenizatsiya, ko‘p faktorli autentifikatsiya, fishing hujumi, 3-D Secure, EMV-chip, PCI DSS, raqamli hamyon, bank kartalari xavfsizligi.

Аннотация. В статье комплексно исследованы теоретические и практические аспекты обеспечения безопасности в системах безналичных платежей, а также направления дальнейшего развития данных систем. В рамках исследования проанализирована статистика использования электронных платежных инструментов в Узбекистане, научно классифицированы основные риски, возникающие при безналичных расчетах, включая фишинг, кражу данных банковских карт и атаки с применением методов социальной инженерии. Рассмотрены современные технологические решения, такие как токенизация, многофакторная аутентификация и методы криптографической защиты. На основе результатов исследования предложена комплексная модель безопасности безналичных платежей, адаптированная к условиям Узбекистана, и разработаны практические рекомендации по развитию системы.

Ключевые слова: безналичные платежи, безопасность электронных платежей, токенизация, многофакторная аутентификация, фишинговая атака, 3-D Secure, EMV-чип, PCI DSS, цифровой кошелек, безопасность банковских карт.

Abstract. This article comprehensively examines the theoretical and practical aspects of ensuring security in cashless payment systems, as well as directions for further development of these systems. The study analyzes statistics on the use of electronic payment instruments in Uzbekistan and scientifically classifies the main risks arising in cashless payments, including phishing, card data theft and social engineering attacks. Modern technological solutions such as tokenization, multi-factor authentication and cryptographic protection methods are also explored. Based on the results, a comprehensive model of cashless payment security adapted to the conditions of Uzbekistan is proposed, and practical recommendations for system development are developed.

Keywords: cashless payment, electronic payment security, tokenization, multi-factor authentication, phishing attack, 3-D Secure, EMV-chip, PCI DSS, digital wallet, bank card security.

Kirish

Zamonaviy iqtisodiyot sharoitida naqd pulsiz to‘lov tizimlari nafaqat qulay va tezkor hisob-kitob vositasi, balki davlat moliyaviy siyosatining strategik tarkibiy qismi sifatida ham muhim ahamiyat kasb etmoqda. Raqamli texnologiyalar rivojlanishi, internet va mobil aloqa infratuzilmasining kengayishi natijasida elektron to‘lovlar global moliyaviy tizimning asosiy yo‘nalishlaridan biriga aylandi. Ayniqsa, COVID-19 pandemiyasi davrida masofaviy xizmatlarga bo‘lgan ehtiyojning ortishi dunyo miqyosida naqd pulsiz iqtisodiyotga o‘tish jarayonini sezilarli darajada jadallashtirdi. Jahon bankining 2022-yilgi ma’lumotlariga ko‘ra, o‘rta va past daromadli mamlakatlarda elektron to‘lovlardan foydalanish darajasi 2017-yildagi 35 foizdan 2021-yilda 57 foizga yetgan [14]. Bu ko‘rsatkich raqamli moliyaviy xizmatlarning global iqtisodiyotdagi o‘rni tobora ortib borayotganini ko‘rsatadi.

O‘zbekistonda ham so‘nggi yillarda naqd pulsiz to‘lov tizimlarini rivojlantirish davlat iqtisodiy siyosatining ustuvor yo‘nalishlaridan biriga aylandi. Mamlakatda bank tizimini modernizatsiya qilish, raqamli iqtisodiyotni rivojlantirish va moliyaviy xizmatlar ommabopligini oshirish bo‘yicha amalga oshirilayotgan islohotlar elektron to‘lovlar hajmining keskin oshishiga sabab bo‘ldi. O‘zbekiston Respublikasi Markaziy banki ma’lumotlariga ko‘ra, naqd pulsiz to‘lovlarning umumiy to‘lovlar hajmidagi ulushi 2019-yildagi 34 foizdan 2023-yilda 68 foizga yetgan [2]. Shu bilan birga, UzCard va HUMO tizimlari orqali muomaladagi bank kartalari soni 30 milliondan oshgan bo‘lib, mobil banking va onlayn to‘lov xizmatlari orqali amalga oshirilayotgan tranzaksiyalar hajmi har yili barqaror ravishda o‘sib bormoqda.

Naqd pulsiz to‘lov tizimlarining kengayishi iqtisodiy samaradorlikni oshirish, yashirin iqtisodiyot ulushini qisqartirish, moliyaviy shaffoflikni ta’minlash va aholining moliyaviy xizmatlardan foydalanish imkoniyatlarini kengaytirishda muhim rol o‘ynamoqda. Elektron to‘lovlar orqali tranzaksiyalar tezligi ortishi, operatsion xarajatlarning kamayishi va biznes jarayonlarining avtomatlashtirilishi iqtisodiy faoliyat samaradorligiga ijobiy ta’sir ko‘rsatmoqda. Ayniqsa, kichik biznes va elektron tijorat rivojida raqamli to‘lov tizimlari asosiy infratuzilma vazifasini bajarmoqda.

Biroq raqamli moliyaviy xizmatlarning jadal rivojlanishi bilan bir qatorda yangi xavf-xatarlar ham yuzaga kelmoqda. Kiberjinoyatchilikning murakkablashuvi, firibgarlik sxemalarining ko‘payishi va foydalanuvchi ma’lumotlariga noqonuniy kirish holatlari bank tizimi xavfsizligini ta’minlash masalasini dolzarb muammoga aylantirmoqda. O‘zbekiston Kiberxavfsizlik markazining 2023-yilgi hisobotiga ko‘ra, moliyaviy sektordagi kiberhujumlar soni 2022-yilga nisbatan oshgan bo‘lib, ularning asosiy qismi to‘lov tizimlari va bank kartalariga qaratilgan [9]. Mazkur holat bank tizimida axborot xavfsizligini kuchaytirish va zamonaviy himoya mexanizmlarini joriy etish zaruratini yanada oshirmoqda.

Mazkur maqolaning asosiy maqsadi O‘zbekistondagi naqd pulsiz to‘lov tizimlarida xavfsizlikni ta’minlashning hozirgi holati, mavjud muammolari va rivojlanish istiqbollarini ilmiy-tahliliy jihatdan o‘rganishdan iborat. Tadqiqot davomida milliy to‘lov tizimining amaldagi holati baholanadi, bank tizimidagi asosiy xavfsizlik tahdidlari tahlil qilinadi hamda xalqaro tajriba asosida amaliy tavsiyalar ishlab chiqiladi.

Adabiyotlar tahlili

Naqd pulsiz to‘lov tizimlari va ularning xavfsizligini ta’minlash masalalari so‘nggi yillarda iqtisodiyot, axborot texnologiyalari va moliya sohalaridagi ilmiy tadqiqotlarning muhim yo‘nalishlaridan biriga aylandi. Mavjud ilmiy tadqiqotlarning aksariyati to‘lov tizimlarini rivojlantirish yoki xavfsizlik masalalarini alohida yo‘nalish sifatida o‘rganishga qaratilgan bo‘lib, ushbu ikki omilning o‘zaro bog‘liqligini kompleks tarzda tahlil qiluvchi ilmiy ishlar hali yetarli darajada shakllanmagan.

O‘zbekistonlik olimlar orasida A. Xoliqovning “Elektron to‘lov tizimlari va ularning xavfsizligi” nomli monografiyasi ushbu sohadagi muhim ilmiy ishlardan biri hisoblanadi [4]. Muallif elektron to‘lov tizimlari infratuzilmasini texnologik nuqtai nazardan tahlil qilib, O‘zbekistondagi bank kartalari tizimlarida uchraydigan xavfsizlik zaifliklarini tizimli ravishda tasniflagan. Tadqiqotning asosiy afzalligi shundaki, unda UzCard va HUMO tizimlari faoliyatidagi autentifikatsiya hamda foydalanuvchi identifikatsiyasi bilan bog‘liq muammolar amaliy misollar orqali ochib berilgan.

S. Mirzayevning “Naqd pulsiz to‘lovlarda firibgarlikning oldini olish” nomli ilmiy maqolasida O‘zbekiston tijorat banklarida uchrayotgan amaliy xavfsizlik muammolari tadqiq etilgan [5]. Muallif to‘lov kartalari bilan bog‘liq eng ko‘p uchraydigan firibgarlik usullarini tasniflab, skimming va phishing hujumlari dominant tahdid sifatida shakllanayotganini ilmiy asoslaydi. Shu bilan birga, tadqiqot asosan mavjud tahdidlarni tavsiflash bilan cheklanib, kompleks himoya tizimlarini shakllantirish bo‘yicha strategik yondashuvlarni yetarlicha qamrab olmagan.

G. Yusupova tomonidan olib borilgan “Raqamli to‘lovlar ekotizimida iste’molchilar ishonchi” nomli tadqiqot mavzuga ijtimoiy-iqtisodiy nuqtai nazardan yondashgani bilan ajralib turadi [6]. Tadqiqot natijalariga ko‘ra, foydalanuvchilarning elektron to‘lov tizimlariga bo‘lgan ishonch darajasi moliyaviy savodxonlik va xavfsizlik bo‘yicha bilimlar bilan bevosita bog‘liq. Bu esa texnologik rivojlanish bilan bir qatorda foydalanuvchilar ishonchini shakllantirish masalasi ham muhim ekanligini ko‘rsatadi.

Xalqaro ilmiy adabiyotlarda ham to‘lov tizimlari xavfsizligi masalasi keng o‘rganilgan. Ross Andersonning “Security Engineering” asarida to‘lov tizimlari xavfsizligining fundamental tamoyillari, identifikatsiya mexanizmlari va kiberhimoya

arxitekturasi chuqur ilmiy asosda bayon qilingan [10]. Muallif xavfsizlik tizimlarini faqat texnologik himoya vositalari orqali emas, balki inson omili, iqtisodiy manfaatlar va boshqaruv mexanizmlari bilan uzviy bog‘liq holda ko‘rib chiqadi.

Europolning 2022-yilgi hisobotida Yevropa va Markaziy Osiyo mintaqasidagi karta firibgarligi tendensiyalari tahlil qilinib, transmilliy kiberjinoyatchilikning kuchayishi to‘lov tizimlari uchun asosiy tahdidlardan biri sifatida baholangan [12]. Bank for International Settlements tomonidan tayyorlangan hisobotda esa raqamli valyutalar va tokenizatsiya mexanizmlarining xavfsizlik imkoniyatlari tahlil qilingan [11]. Ushbu manbalar O‘zbekiston sharoitida milliy to‘lov tizimlari xavfsizligini takomillashtirishda muhim metodologik asos bo‘lib xizmat qiladi.

Tahlil qilingan ilmiy adabiyotlar shuni ko‘rsatadiki, O‘zbekiston sharoitiga xos bo‘lgan qator omillar, xususan, aholining moliyaviy savodxonlik darajasi, hududlar kesimida raqamli infratuzilmaning notekis rivojlanganligi, internet qamrovi bilan bog‘liq muammolar hamda milliy to‘lov tizimlarining o‘ziga xos texnologik xususiyatlari alohida kompleks tadqiqotni talab qiladi.

Tadqiqot metodologiyasi

Tadqiqotda tizimli tahlil, qiyosiy tahlil, statistik usullar va amaliy case-study metodlaridan majmuaviy foydalanildi. Tadqiqot 2019–2023-yillarni qamrab oluvchi besh yillik davr uchun amalga oshirildi. Statistik tahlilda O‘zbekiston Respublikasi Markaziy banki, O‘zbekiston Kiberxavfsizlik markazi, PCI Security Standards Council, Europol va Jahon banki ma’lumotlariga tayangan holda qiyosiy baholash amalga oshirildi [2; 9; 12; 13; 14].

Xavfsizlik tizimlari tahlilida PCI DSS v4.0, ISO/IEC 27001:2022 va O‘zbekiston Markaziy bankining “Bank tizimida axborot xavfsizligi talablari to‘g‘risida”gi 2021-yil 10-maydagi 13/1-sonli Yo‘riqnomasi metodologik asos sifatida qo‘llanildi [1; 13].

Tahlil va natijalar

2019–2023-yillar davomida O‘zbekistonda naqd pulsiz to‘lovlar tizimida kuzatilgan o‘sish dinamikasi quyidagi jadvalda aks ettirilgan:

1-jadval

O‘zbekistonda naqd pulsiz to‘lovlar dinamikasi (2019–2023)

Ko‘rsatkich	2019	2020	2021	2022	2023
Bank kartalari soni (mln)	17,2	20,1	24,5	27,8	30,6
POS-terminallar soni (ming)	42	56	71	83	90
Naqd pulsiz to‘lovlar ulushi (%)	34	44	52	61	68
Mobil to‘lovlar hajmi (trln	28	67	112	198	310

so‘m)					
Karta firibgarligi holatlari (ming)	8,4	11,2	18,6	26,3	34,7

Manba: O‘zbekiston Respublikasi Markaziy banki va O‘zbekiston Kiberxavfsizlik markazi ma’lumotlari asosida mualliflar tomonidan tuzilgan.

1-jadvaldan ko‘rinib turibdiki, naqd pulsiz to‘lovlarning o‘sishi bilan parallel ravishda karta firibgarligi holatlari ham keskin ortgan: 2019-yildagi 8,4 ming holatdan 2023-yilda 34,7 ming holatga, ya’ni 4,1 barobarga oshgan. Bu ko‘rsatkich xavfsizlik muammosining qanchalik dolzarb ekanligini yaqqol ko‘rsatadi.

O‘tkazilgan tadqiqotlar natijasida naqd pulsiz to‘lov tizimlarida uchraydigan xavf-xatarlarni uchta asosiy guruhga ajratish mumkinligi aniqlandi: texnik tahdidlar, ijtimoiy muhandislik tahdidlari hamda tashkiliy va tartibga solish bilan bog‘liq xavflar. Ushbu tahdidlarning har biri bank tizimi barqarorligi va foydalanuvchilar mablag‘lari xavfsizligiga turli darajada salbiy ta’sir ko‘rsatadi.

Birinchi guruh — texnik tahdidlar bo‘lib, ular to‘lov infratuzilmasining texnologik zaifliklaridan foydalanishga asoslanadi. Mazkur tahdidlar qatoriga skimming, zararli dasturlar (malware), man-in-the-middle hujumlari hamda SQL-inyeksiya usullari kiradi. O‘zbekiston Kiberxavfsizlik markazining 2023-yilgi hisobotiga ko‘ra, texnik tahdidlar moliyaviy sektordagi umumiy kiberinsidentlarning salmoqli qismini tashkil etadi [9]. Bu bank infratuzilmasida zamonaviy himoya mexanizmlarini joriy etish zarurati yuqori ekanligini ko‘rsatadi.

Ikkinchi guruh — ijtimoiy muhandislik tahdidlari hisoblanadi. Ushbu tahdidlar inson omiliga ta’sir qilish orqali maxfiy ma’lumotlarni qo‘lga kiritishga qaratilgan bo‘lib, phishing, smishing, vishing va pretexting kabi usullarni o‘z ichiga oladi. Ayniqsa, moliyaviy savodxonlik darajasi past bo‘lgan foydalanuvchilar ushbu tahdidlarga ko‘proq moyil hisoblanadi.

Uchinchi guruh — tashkiliy va tartibga solish bilan bog‘liq xavflardir. Ushbu toifadagi tahdidlar banklarning ichki boshqaruv tizimlari va nazorat mexanizmlaridagi kamchiliklardan kelib chiqadi. Jumladan, bank xodimlari tomonidan ma’lumotlarning ruxsatsiz oshkor etilishi, IT-autsorsing kompaniyalari bilan ishlashdagi xavfsizlik zaifliklari hamda me’yoriy-huquqiy talablarning to‘liq bajarilmasligi asosiy muammolar sifatida qayd etiladi.

Jahon amaliyotida naqd pulsiz to‘lovlar xavfsizligini ta’minlash uchun ilg‘or texnologik yechimlardan keng foydalanilmoqda. Birinchi muhim texnologiya — tokenizatsiya hisoblanadi. Ushbu texnologiya karta ma’lumotlarini tranzaksiya vaqtida noyob bir martalik token bilan almashtirishga asoslanadi. Natijada haqiqiy karta rekvizitlari savdogar tizimlarida saqlanmaydi va ma’lumotlar o‘g‘irlanishi xavfi sezilarli darajada kamayadi.

Ikkinchi texnologik yechim — ko‘p faktorli autentifikatsiya (MFA) tizimidir. Mazkur tizim foydalanuvchi shaxsini bir vaqtning o‘zida bir nechta mustaqil omillar

orqali tasdiqlashni nazarda tutadi. OTP-parollar, biometrik autentifikatsiya va apparat xavfsizlik kalitlari ushbu yo‘nalishdagi eng samarali vositalar hisoblanadi.

Muhim texnologik yechimlardan yana biri 3-D Secure 2.0 protokolidir. Ushbu xalqaro standart onlayn karta to‘lovlari xavfsizligini ta’minlash maqsadida ishlab chiqilgan bo‘lib, tranzaksiyalarni real vaqt rejimida risk darajasi bo‘yicha tahlil qiladi. Xalqaro tajriba 3-D Secure 2.0 versiyasiga o‘tish onlayn firibgarlik holatlarini sezilarli kamaytirishini ko‘rsatmoqda [12; 13].

Tadqiqot davomida sun’iy intellekt asosidagi firibgarlikni aniqlash tizimlari (Fraud Detection Systems — FDS) ham alohida tahlil qilindi. Ushbu tizimlar tranzaksiyalarni real vaqt rejimida kuzatib, odatiy bo‘lmagan faoliyatni avtomatik ravishda aniqlaydi va bloklaydi. O‘zbekistonda bunday tizimlar hozircha asosan yirik banklar tomonidan joriy etilmoqda, ularning keng ommalashmaganligi esa xavfsizlik bo‘yicha farqni oshirmoqda.

2-jadval

Xavfsizlik yechimlari va ularning tatbiq etilish darajasi (2023)

Texnologiya / yechim	Xalqaro qo‘llanish darajasi	O‘zbekiston darajasi	Farq
EMV-chip kartalari	96%	78%	-18%
3-D Secure 2.0	74%	0% (1.0 ishlatiladi)	-74%
Tokenizatsiya (raqamli hamyon)	68%	12%	-56%
AI-asosli FDS tizimlari	81%	18%	-63%
Biometrik autentifikatsiya	55%	9%	-46%
ISO/IEC 27001 sertifikatsiyasi	91%	47%	-44%

Manba: PCI SSC, O‘zbekiston Respublikasi Markaziy banki va Europol ma’lumotlari asosida mualliflar tomonidan tuzilgan.

2-jadvalda ko‘rsatilganidek, O‘zbekistonda xavfsizlik texnologiyalaridan foydalanish darajasi xalqaro ko‘rsatkichlardan sezilarli darajada orqada qolmoqda. Eng katta tafovut AI-asosli FDS tizimlari va 3-D Secure 2.0 protokoli bo‘yicha kuzatilmoqda. Bu ikki yo‘nalish eng ustuvor investitsiya obyekti sifatida ko‘rib chiqilishi lozim.

Xulosa va takliflar

Tadqiqot natijalari shuni tasdiqlaydiki, O‘zbekistonda naqd pulsiz to‘lovlar tizimi jadal rivojlanayotgan bo‘lsa-da, xavfsizlik tizimining rivojlanish sur’ati to‘lov infratuzilmasining o‘sish sur’atidan orqada qolmoqda. Bu holat karta firibgarligi holatlarining 2019–2023-yillar davomida 4,1 barobar oshishida o‘z ifodasini topgan. Ushbu nomutanosiblikni bartaraf etish va naqd pulsiz to‘lov tizimini barqaror rivojlantirish uchun quyidagi kompleks tavsiyalar taklif etiladi:

1. Barcha muomaladagi HUMO va UzCard kartalarini 2026-yilga qadar to‘liq EMV-chip va NFC texnologiyasiga o‘tkazish hamda magnit tasmali kartalarni muomaladan chiqarish bo‘yicha O‘zbekiston Respublikasi Markaziy banki tomonidan majburiy tartib o‘rnatilishi maqsadga muvofiq.

2. Onlayn karta to‘lovlarida 3-D Secure 2.0 protokolini joriy etishni barcha tijorat banklari uchun majburiy talabga aylantirish va Markaziy bank tomonidan bu borada monitoring tizimini yo‘lga qo‘yish zarur.

3. Sun’iy intellekt asosidagi firibgarlikni aniqlash tizimlarini (FDS) joriy etishda kichik va o‘rta banklarga texnik yordam ko‘rsatish maqsadida Markaziy bank huzurida yagona milliy FDS platformasini tashkil etish maqsadga muvofiq. Bu alohida tizim qurishga qodir bo‘lmagan kichik banklar uchun ham foydali bo‘ladi.

4. To‘lov karta ma’lumotlarini himoya qilish uchun tokenizatsiya texnologiyasini barcha mobil to‘lov ilovalari va internet-bankingda standart holga keltirish bo‘yicha me’yoriy hujjat qabul qilinishi lozim.

5. Maktab va oliy ta’lim muassasalari dasturlariga “Raqamli moliyaviy xavfsizlik” kursini kiritish, aholi orasida fishing va ijtimoiy muhandislik hujumlariga qarshi profilaktik kampaniyalarni yiliga kamida ikki marta o‘tkazish tavsiya etiladi.

6. O‘zbekiston Respublikasi Iqtisodiyot va moliya vazirligi hamda Kiberxavfsizlik markazi hamkorligida moliyaviy kiberfavqulodda vaziyatlar markazi (Financial-CERT) tashkil etilib, banklar o‘rtasida tahdidlar to‘g‘risidagi ma’lumot almashishning real vaqtli platformasi ishga tushirilishi zarur.

Ushbu tadqiqotning keyingi yo‘nalishlari sifatida markaziy bank raqamli valyutasining (CBDC) xavfsizlik arxitekturasini o‘rganish va biometrik autentifikatsiya texnologiyalarining O‘zbekiston foydalanuvchilari tomonidan qabul qilinishini tahlil qilish tavsiya etiladi.

Foydalanilgan adabiyotlar ro‘yxati

1. O‘zbekiston Respublikasi Markaziy banki. O‘zbekiston Respublikasi Markaziy bankining 2021-yil 10-maydagi 13/1-sonli “Bank tizimida axborot xavfsizligi talablari to‘g‘risida”gi Yo‘riqnomasi. — Toshkent: O‘zbekiston Markaziy banki, 2021.

2. O‘zbekiston Respublikasi Markaziy banki. O‘zbekiston Respublikasi Markaziy bankining 2023-yilgi yillik statistik to‘plami. — Toshkent: O‘zbekiston Markaziy banki, 2024. — 162 b.

3. O‘zbekiston Respublikasi Prezidentining 2020-yil 28-apreldagi PQ-4699-sonli “O‘zbekiston Respublikasida elektron tijorat va to‘lov tizimlarini yanada rivojlantirish chora-tadbirlari to‘g‘risida”gi Qarori. — Toshkent, 2020.

4. Xoliqov A. Elektron to‘lov tizimlari va ularning xavfsizligi. — Toshkent: TATU nashriyoti, 2020. — 260 b.

5. Mirzayev S. Naqd pulsiz to‘lovlarda firibgarlikning oldini olish // Axborot texnologiyalari muammolari. — Toshkent, 2021. — №2. — B. 67–81.

6. Yusupova G. Raqamli to‘lovlar ekotizimida iste’molchilar ishonchi // Moliya va bank ishi. — Toshkent, 2022. — №1. — B. 34–47.

7. Toshmatov N., Ergashev B. Bank kartalari xavfsizligida tokenizatsiya texnologiyasining ahamiyati // Iqtisodiyot va innovatsion texnologiyalar. — Toshkent, 2023. — №3. — B. 95–108.

8. Hasanov R. Naqd pulsiz hisob-kitoblar va moliyaviy inklyuzivlik: O‘zbekiston tajribasi // O‘zbekiston iqtisodiyoti jurnali. — Toshkent, 2022. — №4. — B. 56–70.

9. O‘zbekiston Kiberxavfsizlik markazi. 2023-yil moliyaviy kiberxavfsizlik holati to‘g‘risida hisobot. — Toshkent, 2024. — 72 b.

10. Anderson R. Security Engineering: A Guide to Building Dependable Distributed Systems. 3rd ed. — Hoboken: Wiley, 2020. — 1200 p.

11. Bank for International Settlements. Central Bank Digital Currencies: Foundational Principles and Core Features. — Basel: BIS, 2021. — 57 p.

12. Europol. Internet Organised Crime Threat Assessment (iOCTA): Payment Card Fraud. — The Hague: Europol, 2022. — 88 p.

13. PCI Security Standards Council. PCI DSS v4.0 Requirements and Testing Procedures. — Wakefield: PCI SSC, 2022. — 360 p.

14. World Bank. The Global Findex Database 2021: Financial Inclusion, Digital Payments, and Resilience in the Age of COVID-19. — Washington D.C.: World Bank, 2022. — 160 p.

15. Financial Action Task Force. Digital Transformation of AML/CFT for Operational Agencies. — Paris: FATF, 2022. — 68 p.