

MUHANDISLIK

& IQTISODIYOT

ijtimoiy-iqtisodiy, innovatsion texnik,
fan va ta'limga oid ilmiy-amaliy jurnal

2025
oktyabr



**TOSHKENT SHAHRIDAGI TURIN
POLITEXNIKA UNIVERSITETI**

*Xalqaro ilmiy-amaliy onlayn konferensiya
materiallari to'plami*

**“GLOBAL RAQAMLI INTEGRATSIYALASHUV:
2030-YILGACHA YASHIL IQTISODIYOTGA O'TISHDA
TEXNOLOGIK VA INDUSTRIAL SANOATNI RIVOJLANTIRISH
ORQALI MIKRO VA MAKROIQTISODIY BARQAROR
O'SISHNI TA'MINLASH DOLZARBLIGI”**

**“GLOBAL DIGITAL INTEGRATION: THE RELEVANCE OF
ENSURING MICRO AND MACROECONOMIC SUSTAINABLE
GROWTH THROUGH TECHNOLOGICAL AND INDUSTRIAL
DEVELOPMENT IN THE TRANSITION TO A GREEN
ECONOMY BY 2030”**

**«ГЛОБАЛЬНАЯ ЦИФРОВАЯ ИНТЕГРАЦИЯ:
АКТУАЛЬНОСТЬ ОБЕСПЕЧЕНИЯ УСТОЙЧИВОГО
МИКРО- И МАКРОЭКОНОМИЧЕСКОГО РОСТА ЧЕРЕЗ
РАЗВИТИЕ ТЕХНОЛОГИЧЕСКОЙ И ИНДУСТРИАЛЬНОЙ
ПРОМЫШЛЕННОСТИ В ПЕРЕХОДЕ К ЗЕЛЁНОЙ
ЭКОНОМИКЕ К 2030 ГОДУ»**

7-MAXSUS SON



74-91 xalqaro daraja
ISSN: 2992-8982



muhandislik & iqtisodiyot

ijtimoiy-iqtisodiy, innovatsion texnik,
fan va ta'limga oid ilmiy-amaliy jurnal

Elektron nashr.
2025-yil, oktyabr.

Bosh muharrir:

Zokirova Nodira Kalandarovna, iqtisodiyot fanlari doktori, DSc, professor

Bosh muharrir o'rinbosari:

Shakarov Zafar G'afforovich, iqtisodiyot fanlari bo'yicha falsafa doktori, PhD, dotsent

Tahrir hay'ati:

Abduraxmanov Kalandar Xodjayevich, O'z FA akademigi, iqtisodiyot fanlari doktori, professor

Sharipov Kongratbay Avezimbetovich, texnika fanlari doktori, professor

Maxkamov Baxtiyor Shuxratovich, iqtisodiyot fanlari doktori, professor

Abduraxmanova Gulnora Kalandarovna, iqtisodiyot fanlari doktori, professor

Shaumarov Said Sanatovich, texnika fanlari doktori, professor

Turayev Bahodir Xatamovich, iqtisodiyot fanlari doktori, professor

Nasimov Dilmurod Abdulloyevich, iqtisodiyot fanlari doktori, professor

Allayeva Gulchexra Jalgasovna, iqtisodiyot fanlari doktori, professor

Arabov Nurali Uralovich, iqtisodiyot fanlari doktori, professor

Maxmudov Odiljon Xolmirzayevich, iqtisodiyot fanlari doktori, professor

Xamrayeva Sayyora Nasimovna, iqtisodiyot fanlari doktori, professor

Bobonazarova Jamila Xolmurodovna, iqtisodiyot fanlari doktori, professor

Irmatova Aziza Baxromovna, iqtisodiyot fanlari doktori, professor

Bo'taboyev Mahammadjon To'ychiyevich, iqtisodiyot fanlari doktori, professor

Shamshiyeva Nargizaxon Nosirxuja kizi, iqtisodiyot fanlari doktori, professor,

Xolmuxamedov Muhsinjon Murodullayevich, iqtisodiyot fanlari nomzodi, dotsent

Xodjayeva Nodiraxon Abdurashidovna, iqtisodiyot fanlari nomzodi, dotsent

Amanov Otabek Amankulovich, iqtisodiyot fanlari bo'yicha falsafa doktori (PhD), dotsent

Toxirov Jaloliddin Ochil o'g'li, texnika fanlari bo'yicha falsafa doktori (PhD)

Qurbonov Samandar Pulatovich, iqtisodiyot fanlari bo'yicha falsafa doktori (PhD)

Zikriyoyev Aziz Sadulloyevich, iqtisodiyot fanlari bo'yicha falsafa doktori (PhD)

Tabayev Azamat Zaripbayevich, iqtisodiyot fanlari bo'yicha falsafa doktori (PhD)

Sxay Lana Aleksandrovna, iqtisodiyot fanlari bo'yicha falsafa doktori (PhD), dotsent

Ismoilova Gulnora Fayzullayevna, iqtisodiyot fanlari nomzodi, dotsent

Djumaniyazov Umrbek Ixamovich, iqtisodiyot fanlari nomzodi, dotsent

Kasimova Nargiza Sabitdjanovna, iqtisodiyot fanlari nomzodi, dotsent

Kalanova Moxigul Baxritdinovna, dotsent

Ashurzoda Luiza Muxtarovna, iqtisodiyot fanlari bo'yicha falsafa doktori (PhD)

Sharipov Sardor Begmaxmat o'g'li, iqtisodiyot fanlari bo'yicha falsafa doktori (PhD)

Sharipov Botirali Roxataliyevich, iqtisodiyot fanlari nomzodi, professor

Tursunov Ulug'bek Sativoldiyevich, iqtisodiyot fanlari doktori (DSc), dotsent

Bauyetdinov Majit Janizaqovich, Toshkent davlat iqtisodiyot universiteti dotsenti, PhD

Botirov Bozorbek Musurmon o'g'li, Texnika fanlari bo'yicha falsafa doktori (PhD)

Sultonov Shavkatjon Abdullayevich, Kimyo fanlari doktori, (DSc)

Jo'raeva Malohat Muhammadovna, filologiya fanlari doktori (DSc), professor.

muhandislik & iqtisodiyot

ijtimoiy-iqtisodiy, innovatsion texnik,
fan va ta'limga oid ilmiy-amaliy jurnal

- 05.01.00 – Axborot texnologiyalari, boshqaruv va kompyuter grafikasi
- 05.01.01 – Muhandislik geometriyasi va kompyuter grafikasi. Audio va video texnologiyalari
- 05.01.02 – Tizimli tahlil, boshqaruv va axborotni qayta ishlash
- 05.01.03 – Informatikaning nazariy asoslari
- 05.01.04 – Hisoblash mashinalari, majmualari va kompyuter tarmoqlarining matematik va dasturiy ta'minoti
- 05.01.05 – Axborotlarni himoyalash usullari va tizimlari. Axborot xavfsizligi
- 05.01.06 – Hisoblash texnikasi va boshqaruv tizimlarining elementlari va qurilmalari
- 05.01.07 – Matematik modellash
- 05.01.11 – Raqamli texnologiyalar va sun'iy intellekt
- 05.02.00 – Mashinasozlik va mashinashunoslik
- 05.02.08 – Yer usti majmualari va uchish apparatlari
- 05.03.02 – Metrologiya va metrologiya ta'minoti
- 05.04.01 – Telekommunikatsiya va kompyuter tizimlari, telekommunikatsiya tarmoqlari va qurilmalari. Axborotlarni taqsimlash
- 05.05.03 – Yorug'lik texnikasi. Maxsus yoritish texnologiyasi
- 05.05.05 – Issiqlik texnikasining nazariy asoslari
- 05.05.06 – Qayta tiklanadigan energiya turlari asosidagi energiya qurilmalari
- 05.06.01 – To'qimachilik va yengil sanoat ishlab chiqarishlari materialshunosligi
- 05.08.03 – Temir yo'l transportini ishlatish
- 05.09.01 – Qurilish konstruksiyalari, bino va inshootlar
- 05.09.04 – Suv ta'minoti. Kanalizatsiya. Suv havzalarini muhofazalovchi qurilish tizimlari
- 10.00.06 – Qiyosiy adabiyotshunoslik, chog'ishtirma tilshunoslik va tarjimashunoslik
- 10.00.04 – Yevropa, Amerika va Avstraliya xalqlari tili va adabiyoti
- 08.00.01 – Iqtisodiyot nazariyasi
- 08.00.02 – Makroiqtisodiyot
- 08.00.03 – Sanoat iqtisodiyoti
- 08.00.04 – Qishloq xo'jaligi iqtisodiyoti
- 08.00.05 – Xizmat ko'rsatish tarmoqlari iqtisodiyoti
- 08.00.06 – Ekonometrika va statistika
- 08.00.07 – Moliya, pul muomalasi va kredit
- 08.00.08 – Buxgalteriya hisobi, iqtisodiy tahlil va audit
- 08.00.09 – Jahon iqtisodiyoti
- 08.00.10 – Demografiya. Mehnat iqtisodiyoti
- 08.00.11 – Marketing
- 08.00.12 – Mintaqaviy iqtisodiyot
- 08.00.13 – Menejment
- 08.00.14 – Iqtisodiyotda axborot tizimlari va texnologiyalari
- 08.00.15 – Tadbirkorlik va kichik biznes iqtisodiyoti
- 08.00.16 – Raqamli iqtisodiyot va xalqaro raqamli integratsiya
- 08.00.17 – Turizm va mehmonxona faoliyati

Ma'lumot uchun, OAK

Rayosatining 2024-yil 28-avgustdagi 360/5-son qarori bilan "Dissertatsiyalar asosiy ilmiy natijalarini chop etishga tavsiya etilgan milliy ilmiy nashrlar ro'yxati"ga texnika va iqtisodiyot fanlari bo'yicha "Muhandislik va iqtisodiyot" jurnali ro'yxatga kiritilgan.

Muassis: "Tadbirkor va ishbilarmon" MChJ

Hamkorlarimiz:

1. Toshkent shahridagi G.V.Plexanov nomidagi Rossiya iqtisodiyot universiteti
2. Toshkent davlat iqtisodiyot universiteti
3. Toshkent irrigatsiya va qishloq xo'jaligini mexanizatsiyalash muhandislari instituti" milliy tadqiqot universiteti
4. Islom Karimov nomidagi Toshkent davlat texnika universiteti
5. Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti
6. Toshkent davlat transport universiteti
7. Toshkent arxitektura-qurilish universiteti
8. Toshkent kimyo-texnologiya universiteti
9. Jizzax politexnika instituti



MUNDARIJA

ASSESSING RISKS IN BANKING ACTIVITIES TO ENHANCE THE EFFICIENCY OF FINANCIAL SERVICES	21
Saidov Jasurbek Latipbayevich	
MECHANISMS OF THE IMPACT OF STATE BUDGET REVENUES AND EXPENDITURES ON ECONOMIC GROWTH.....	24
Sheraliyev Nurbek Jumanazarovich	
O'QUVCHI VA TALABALARDA HUQUQIY MADANIYATINI TA'LIM JARAYONIDA YUKSALTIRISHNING ASOSIY YO'NALISHLARI VA TAMOIYILLARI	27
Mansurova Zilola Akromxonovna	
O'ZBEKISTON BANK TIZIMIDA FINTECH INNOVATSIYALARINING RIVOJI VA ULARNING SANOAT-QURILISH SEKTORIDAGI TRANSFORMATSION TA'SIRI	30
Muzayyana Beknazarova	
TURIZM SOHASIDA RAQOBAT AFZALLIKLARINI YARATISHDA MARKETINGNING ROLI	33
Shaymanov To'liqin Mahmayusupovich	
O'ZBEKISTONDA DAVLAT BUDJETI IJROSINI RAQAMLASHTIRISHNING FISKAL INTIZOM VA SHAFFOFLIKKA TA'SIRI	37
Tangrieva Farida Abdulkarimovna	
OLIY TA'LIM MUASSASALARIDA SUN'IY INTELLEKTNI TATBIQ ETISH ORQALI BOSHQARUV SAMARADORLIGINI OSHIRISH	41
Radjabov Bunyod Abdullilovich	
XXI-ASRDA JAHON IQTISODIYOTINING RIVOJLANISH BOSQICHLARI VA ASOSIY DRAYVERLARI	45
Jalolov Umidjon Xudoyberdi o'g'li, Yegamberdiyev Shuxrat Satimbayevich	
XALQARO RAQAMLI INTEGRATSIYA JARAYONIDA O'ZBEKISTON ISHTIROKI	48
Muyassarzoda Fayziyeva	
ФИНАНСОВЫЙ КОНТРОЛЬ КАК КЛЮЧЕВОЙ ИНСТРУМЕНТ ОБЕСПЕЧЕНИЯ НАЦИОНАЛЬНЫХ ИНТЕРЕСОВ И ФИНАНСОВОЙ БЕЗОПАСНОСТИ УЗБЕКИСТАНА	52
Турсунбоева Нилуфар Отабековна	
ФИНАНСОВАЯ ГРАМОТНОСТЬ И ИНВЕСТИЦИИ	55
Ягудин Дмитрий Рустамович	
YANGI O'ZBEKISTON SHAROITIDA BARQAROR TURIZM RIVOJI: GLOBAL TAJRIBA VA MILLIY YONDASHUVLAR.....	57
Xamdullayeva Gulhoyo Ergash qizi	
RAQAMLI TEXNOLOGIYALAR YORDAMIDA TO'QIMACHILIK KORXONALARIDA INVESTITSION QARORLARNI OPTIMALLASHTIRISH	59
Rustambekov Djasur Askarovich	
KORXONA POTENSIALINING MOHIYATI VA TUZILMASIGA OID NAZARIY HAMDA ILMIY YONDASHUVLAR TAHLILI.....	61
Djalilov Sardor Sadillovovich	
XALQARO IQTISODIYOTNING GLOBAL DAROMAD TENGSIZLIKLARINI SHAKLLANTIRISHDAGI ROLI: SAVDO SIYOSATLARI VA REDISTRIBYUTSIYA MEKANIZMLARINING TAQQOSLAYDIGAN TAHLILI	64
Kurolov Maksud Obidovich	
SURXONDARYO VILOYATIDA INVESTITSIYA VA YHM O'RTASIDAGI O'ZARO BOG'LIQLIK.....	73
Zaripova Muqaddas Jumaniyozovna, Normurodov Asliddin Alijon o'g'li	
SUN'IY INTELLEKT VA AVTOMATLASHTIRISHNING MEHNAT BOZORI DINAMIKASIGA TA'SIRI	77
Akmalbek Najimov Umid o'g'li, Dinara Ishmanova	
ПРАКТИКА И АНАЛИЗ КРЕДИТОВАНИЯ ПРОИЗВОДИТЕЛЕЙ СЕЛЬСКОХОЗЯЙСТВЕННОЙ ПРОДУКЦИИ	81
Шамшетьева Гульраушан	



AHOLI DAROMADLARI O'SISHI VA INFLYATSIYA DARAJASI O'RTASIDAGI BOG'LIQLIK	83
G'ayratova Zilola G'anijon qizi, Ibragimov G'anijon G'ayratovich	
KORXONALARDA MAHSULOT SAVDOSIGA OID MA'LUMOTLARNI TAHLIL QILISHNING ZAMONAVIY INTELEKTUAL YONDASHUVLARI	86
Baydullayeva Dildora Tuylibayevna, Baydullayev Ruslan Tuylibayevich	
ELEKTRON TIJORATNING MILLIY IQTISODIYOTGA TA'SIRI VA RIVOJLANISH ISTIQBOLLARI	90
Toxirov Shodibek Jo'ra o'g'li	
RAQOBATBARDOSH ELEKTROTEXNIKA MAHSULOTLARI ISHLAB CHIQUVISHDA TEXNOLOGIK MODERNIZATSIYA VA INVESTITSIYA SIYOSATINING O'RNI	93
Jalolov Abbasxon Ravshanxon	
RAQAMLI TEXNOLOGIYALAR VA SUN'IIY INTELLEKT ASOSIDA BUXGALTERIYA HISOB VA AUDIT TIZIMLARINI AVTOMATLASHTIRISHNING METODOLOGIK ASOSLARI	97
To'laganov Ziyovuddin Kamolitdin o'g'li	
THE IMPACT OF EXTERNAL DEBT, INVESTMENT ACTIVITY, AND CAPITAL FORMATION PROCESSES ON EXPORT VOLUME AND ECONOMIC GROWTH DYNAMICS IN CENTRAL ASIAN COUNTRIES	102
Tojiqulova Sitora Sobirjon qizi	
HUMAN CAPITAL AND DIGITAL TRANSFORMATION: DRIVERS OF SUSTAINABLE ECONOMIC DEVELOPMENT	108
Hamrokulov Mirabbos Ortiqovich	
YEVROPA ITTIFOQI DAVLATLARI SOLIQ SIYOSATINI USTUVOR JIHATLARINI MARKAZIY OSIYO MAMLAKATLARIDA QO'LLASH ORQALI SOLIQ TIZIMINI TAKOMILLASHTIRISH	110
Hakimov Feruz Xurshid o'g'li	
KAPITAL TUZILMASINI OPTIMALLASHTIRISH ORQALI TIJORAT BANKLARINING MOLIYAVIY BARQARORLIGINI OSHIRISH KONSEPSIYASI	114
Turdibayev Abdulaziz Abduvaxidovich	
O'ZBEKISTONNING 12 YILLIK TA'LIM TIZIMIGA QAYTISH ISLOHOTI	118
Ashurov Abdulaziz Rustamovich, Olimov Anvarjon Atamirzayevich, Mahmudov Ziyoviddin Shamsiddinovich, Ishmuratov Baxodir Xusanovich	
MAMLAKATNING XALQARO BAHOLASH TIZIMLARIDAGI MAVQEINI YAXSHILASHDA IQTISODIY MUSTAHKAMLIKNING AHAMIYATI	123
Berdibekova Dilfuza Xoldorbekovna	
XALQARO SAVDODA MARKETING ROLI: EKONOMETRIK MODELLASHTIRISH	125
Qurolov Maqsud Obitovich	
BANK RISKLARINING BANK FAOLIYATIGA TA'SIRI VA ULARNI BOSHQARISHNI TAKOMILLASHTIRISH YO'LLARI	130
B.Izbosarov, N.Hakimova	
OZIY-OVQAT XAVFSIZLIGI MASALASINING JAHON IQTISODIYOTIDA TUTGAN O'RNI	132
Abdusamatov Barkamol Rustamjon o'g'li	
DYUZDO SPORTIDA MALAKALI SPORTCHILARNI TAYYORLASH JARAYONIDA TAKTIK TAYYORGARLIKNING NAZARIY ASOSLARI VA AMALIY AHAMIYATI	135
Tangriyev Abdullo Tovashovich	
SANOATDA QO'SHILGAN QIYMAT HAJMINI OSHIRISH	138
Mamurjonova Ruxshonabegim Farxodovna	
O'ZBEKISTONDA OLIY TA'LIM BOSHQARUVI UCHUN SUN'IIY INTELLEKTNING KENGAYTIRILGAN BASHORATLI TAHLILI	142
Esanova Shohida O'tkirovna	
PROSPECTS OF USING CREDIT CARDS IN COMMERCIAL BANKS OF THE REPUBLIC OF UZBEKISTAN	146
Mamatova Sevara Ilhom qizi	
O'ZBEKISTONDA EKSPORTNI SUG'URTALASH MEKANIZMLARINI YANADA KENGAYTIRISH YO'NALISHLARI	151
Xalilova Feruza Jamolovna	



УЯЗВИМОСТИ В ПЛАТЕЖНЫХ ОРГАНИЗАЦИЯХ РЕСПУБЛИКИ УЗБЕКИСТАН	155
Садыков Азиз Миршарапович	



УЯЗВИМОСТИ В ПЛАТЕЖНЫХ ОРГАНИЗАЦИЯХ РЕСПУБЛИКИ УЗБЕКИСТАН

Садыков Азиз Миршарапович

Банковско-Финансовая Академия Республики Узбекистан

Независимый исследователь,

a.sadikov@atmos.uz,

Аннотация. В работе анализируются ключевые уязвимости платёжных организаций Узбекистана в условиях ускоренной цифровизации. Исследование охватывает технологические, операционные, комплаенс-риски и человеческий фактор, а также предлагает комплекс мер по их минимизации. Особое внимание уделено киберугрозам, росту мошенничества и необходимости усиления кибербезопасности.

Ключевые слова: платёжные организации, кибербезопасность, цифровизация, уязвимости, AML/CFT, мошенничество.

Annotatsiya. Maqolada O'zbekistondagi to'lov tashkilotlarining raqamlashtirish jarayonida yuzaga kelayotgan asosiy zaifliklari tahlil qilinadi. Tadqiqot texnologik, operatsion, komplayens va inson omili bilan bog'liq xatarlarni o'rganadi hamda ularni kamaytirish bo'yicha takliflar beradi. Kiberxavfsizlik tahdidlari va firibgarlik holatlarining o'sishi alohida yoritilgan.

Kalit so'zlar: to'lov tashkilotlari, kiberxavfsizlik, raqamlashtirish, zaifliklar, AML/CFT, firibgarlik.

Abstract. This paper examines the key vulnerabilities of payment organizations in Uzbekistan amid rapid digitalization. The study highlights technological, operational, compliance-related and human-factor risks, and proposes a set of measures to mitigate them. Special attention is given to cyber threats, fraud growth, and the need to strengthen cybersecurity frameworks.

Keywords: payment organizations, cybersecurity, digitalization, vulnerabilities, AML/CFT, fraud.

ВВЕДЕНИЕ

Цифровизация финансовых услуг в Узбекистане развивается высокими темпами: растёт проникновение мобильного интернета, расширяется электронная коммерция, активно используются мобильные кошельки и платёжные сервисы. Массовый переход транзакций в цифровую среду создаёт новые возможности для экономического роста и финансовой инклюзии, но одновременно увеличивает поверхность атаки для злоумышленников и усложняет управление рисками платёжных организаций.

Центральный банк в ежегодных отчётах по финансовой стабильности фиксирует устойчивую тенденцию роста безналичных расчётов, а национальные центры реагирования на киберинциденты систематически отмечают увеличение количества попыток атак и выявленных уязвимостей в интернет-ресурсах. Эти два факта — ускоренная цифровизация и усиление киберугроз — формируют актуальный контекст для исследования уязвимостей платёжной экосистемы Узбекистана.

Текущее состояние платёжной экосистемы Узбекистана.

1. Инфраструктура и участники. Платёжная экосистема включает банки, платёжные организации, операторов эквайринга, процессинговые центры и fintech-компании. Национальные проекты и крупные игроки расширяют охват услуг: POS-терминалы, интернет-эквайринг, мобильные платежи, коммунальные и образовательные платежи. Однако частые интеграции с внешними провайдерами и API усложняют обеспечение единого уровня безопасности¹.

2. Регулирование и надзор. Центральный банк в отчётах о финансовой стабильности выделяет риски цифровизации и вопросы устойчивости платёжной инфраструктуры. Регулятор внедряет

¹ https://cbu.uz/en/financial-stability/?utm_source

макропруденциальные меры и требования к контролю операций. Параллельно профильные органы кибербезопасности осуществляют мониторинг и устранение уязвимостей.

3. Киберобстановка. По данным национальных служб (UzCERT и др.) наблюдается устойчивый рост количества попыток кибератак и выявленных уязвимостей в доменной зоне .uz. Финансовый сектор относится к числу наиболее атакуемых. Ежегодно фиксируются миллионы попыток атак и тысячи уязвимостей.

Проблемы и уязвимости. Ниже представлен систематизированный анализ уязвимостей, разделённых по четырём ключевым категориям: технологические, операционные, комплаенс-риски и человеческий фактор.

1) Технологические уязвимости.

а) Уязвимости веб-приложений и API.

– Описание: недостаточная валидация входных данных (SQL-инъекции), уязвимости XSS, слабая аутентификация, незащищённые сессии, открытые административные интерфейсы. Активное использование API создаёт риски компрометации цепочки интеграций.

– Последствия: кража персональных данных, утечка реквизитов карт, подмена транзакций, несанкционированный доступ в административные панели.

– Пример: национальные отчёты регулярно фиксируют «критические» уязвимости в веб-ресурсах государственных и частных структур, что указывает на аналогичные риски в финансовом секторе².

б) Устаревшее ПО и некорректный патч-менеджмент.

– Описание: использование устаревших ОС, серверов и библиотек; несвоевременная установка обновлений.

– Последствия: эксплуатация известных эксплойтов, массовые компрометации. Национальные службы отмечают, что значительная доля атак связана с непропатченными узлами³.

с) Уязвимости интеграции с эквайринговыми шлюзами.

– Описание: ошибки в реализации 3-D Secure, некорректная обработка повторных запросов (idempotency), слабая проверка цифровых подписей.

– Последствия: двойные списания, replay-атаки, манипуляции статусами транзакций, рост chargeback-ов.

2) Операционные уязвимости.

а) Недостаточный контроль доступа и управления привилегиями.

– Описание: нерегулярная ротация ключей/паролей, отсутствие MFA на всех админ-аккаунтах, слабый аудит.

– Последствия: захват администраторских учётных записей, внутренние злоупотребления, незамеченные изменения конфигураций.

б) Недостаточная автоматизация мониторинга транзакций.

– Описание: ручной анализ аномалий, отсутствие real-time AML-моделей и автоматических правил детекции.

– Последствия: позднее выявление мошенничества, использование сервисов для отмывания средств.

с) Ошибки в процедурах dispute/chargeback.

– Описание: размытые регламенты, слабая верификация возвратов.

– Последствия: финансовые потери, рост мошенничества со стороны мерчантов.

3) Комплаенс-риски (AML/CFT).

– Описание: при массовом онлайн-КУС и росте трансграничных операций возможны поверхностные проверки клиентов и бенефициаров. Особенно рискованны операции нерезидентов и сложных корпоративных структур.

– Последствия: использование сервисов для легализации преступных доходов, штрафы и санкции регуляторов и международных организаций⁴.

4) Человеческий фактор и мошенничество с клиентами.

– Описание: фишинг, вредоносные приложения, социальная инженерия («Hello, Mom» и другие локальные схемы). Клиенты передают коды подтверждения или устанавливают трояны.

– Последствия: прямые кражи средств, компрометация аккаунтов. Национальные отчёты фиксируют значительный рост жалоб, связанных именно с фрод-схемами.

2 https://infocom.uz/en/news/ozbekistonda-kiberxavfsizlik-rivojlanish-darajasining-tahlili?utm_source

3 https://kun.uz/en/news/2025/02/03/over-12-million-cyberattacks-recorded-in-uzbekistan-in-2024?utm_source

4 www.fatf-gafi.org/en/publications/Mutualevaluations/Mutualevaluationofuzbekistan.html?utm_source



Таблица 1. Классификация уязвимостей и примерные последствия

Категория уязвимости	Конкретный пример	Возможные последствия
Технологические	SQL-инъекция в API мерчанта	Утечка PII, компрометация токенов карт
Инфраструктурные	Необновлённый веб-сервер (CVE-эксплойт)	Массовое взломанное узло, RCE
Операционные	Отсутствие MFA у админов	Захват админпанели, изменение транзакций
Комплаенс (AML/CFT)	Поверхностный KYC при онлайн-реестрации	Использование аккаунтов для отмывания средств
Человеческий фактор	Фишинговая рассылка пользователям	Кража кодов подтверждения, потеря средств

Последствия уязвимостей.

1. Финансовые потери. Прямые списания средств, рост количества возвратов (chargeback), штрафы регулятора, а также расходы на компенсации клиентам. По данным национальных служб, увеличение числа мошеннических операций и фрод-инцидентов приводит к существенному росту экономических потерь в платёжном сегменте.

2. Репутационные риски. Потеря доверия клиентов и партнёров, снижение качества пользовательского опыта, переход мерчантов к конкурентам и, как следствие, долгосрочное сокращение доли рынка.

3. Регуляторные последствия. Усиление надзорных проверок, введение дополнительных требований к капиталу и резервам, административные санкции, а в отдельных случаях — временное ограничение или приостановление деятельности. Центральный банк в рамках политики финансовой стабильности подчёркивает критическую важность контроля системных рисков.

4. Системные риски. Крупные инциденты могут негативно влиять на доступность платёжной инфраструктуры, нарушать непрерывность обслуживания, снижать доверие к безналичным расчётам и приводить к макроэкономическим эффектам, затрагивающим экономическую активность в целом.

Методы и инструменты решения. Решения сгруппированы по четырём направлениям: технические, организационно-процессные, регуляторно-институциональные и просветительские.

Технические меры (направлены на непосредственное снижение уязвимости)

1. Управление уязвимостями. Внедрение регулярных автоматизированных сканирований безопасности, проведение обязательных внешних и внутренних пентестов не реже одного раза в год, создание программ bug bounty для критически важных компонентов⁵.

2. Современные архитектурные подходы: Zero Trust (контроль доступа по минимальным привилегиям), разнесение сетей (сегментация), изоляция критичных сервисов.

3. Защита API и web-слоя: WAF, rate-limiting, проверка idempotency, защита от replay-атак, TLS-практики, подписанные и защищённые сообщения между сервисами⁶.

4. Харденинг и патч-менеджмент: централизованный процесс обновлений, критические патчи — в течение SLA (например, 48–72 часа для критичных CVE).

5. Аутентификация и управление ключами: обязательный MFA для всех административных и клиентских операций; HSM для хранения секретов, ротация ключей и журналирование доступа.

Операционные и процессные меры

1. Автоматизация мониторинга транзакций (real-time AML/Fraud). Внедрение решений класса SIEM и EDR, а также антифрод-систем с использованием ML-моделей позволяет осуществлять постоянный анализ транзакций и поведения пользователей. Интеграция с AML-case-management обеспечивает единый цикл обработки подозрительных операций. Реал-тайм скоринг повышает эффективность раннего выявления аномалий и оперативной блокировки мошеннических действий.

2. Чёткие регламенты incident response и BCP. Разработка и внедрение плейбуков, процедур эскалации и уведомления регулятора, а также регулярные учения (tabletop-тренировки и DR-упражнения) повышают готовность организаций к реагированию на инциденты. Такой подход снижает время восстановления сервисов и минимизирует ущерб.

3. Управление третьими сторонами (third-party risk management). Формирование стандартов безопасности для внешних провайдеров: включение требований по SLA, обязательным аудитам,

⁵ https://infocom.uz/en/news/ozbekistonda-kiberxavfsizlik-rivojlanish-darajasining-tahlili?utm_source

⁶ https://assets.kpmg.com/content/dam/kpmg/uz/pdf/2024/Fintech%20UZ_Payments_POS%20Financing_BNPL-final.pdf?utm_source

предоставлению pentest-отчётов, сертификатов SOC-2 или аналогичных. Периодическая ревизия интеграций и контроль цепочек поставок позволяют предотвратить проникновение уязвимостей через сторонние сервисы.

Регуляторно-институциональные меры

1. Единые требования по кибер-инцидентам и обмен индикаторами компрометации. Установление обязательной отчётности по серьёзным инцидентам кибербезопасности и создание централизованного механизма обмена IOC (Indicators of Compromise) через профильные национальные центры (UzCERT и др.). Это способствует повышению коллективной устойчивости финансового сектора, ускоряет идентификацию угроз и укрепляет национальную систему реагирования на киберугрозы⁷.

2. Усиление AML/CFT контроля: адаптация risk-based подхода с учётом особенностей цифровых продуктов, проверка бенефициаров, усиленный мониторинг трансграничных потоков в высокорисковых сегментах.

Образовательные и превентивные меры

1. Обучение сотрудников: регулярные тренинги по информационной безопасности, фишинг-тестирование, обучение команд реагированию на инциденты.

2. Просветительские кампании для клиентов: повышение цифровой грамотности, инструкции по безопасному использованию мобильных приложений и карт (государственно-частные инициативы). Национальные медиа и сервисы уже информируют о популярных схемах мошенничества.

Таблица 2. План внедрения защитных мер

Приоритет	Мера	Временной горизонт	KPI (пример)
Высокий	MFA для админов и клиентов; real-time транзакционный мониторинг	0–3 мес	% аккаунтов с MFA, среднее время обнаружения фрода
Средний	Пентесты + баг-баунти; WAF и SIEM	3–6 мес	Кол-во найденных уязвимостей до и после
Средний	Процесс управления патчами и HSM	3–6 мес	Среднее время на установку крит. патча
Низкий	Public awareness кампании	6–12 мес	Доля фишинг-инцидентов в общем объёме жалоб

ВЫВОДЫ И РЕКОМЕНДАЦИИ

Рост цифровых платежей повышает доступность и удобство, но одновременно увеличивает риск системных инцидентов и мошенничества. Динамика количества атак и уязвимостей подтверждает необходимость приоритетного внимания к информационной безопасности.

Уязвимости носят разноуровневый характер: от кодовых ошибок и непатченных сервисов до слабых организационных процессов и недостатков в AML/CFT. Эффективная защита требует синергии технических, организационных и регуляторных мер.

Централизованные механизмы обмена индикаторами и оперативное уведомление регулятора существенно снижают риски распространения инцидента и позволяют координировать меры по защите.

Платёжные организации в Республике Узбекистан находятся на этапе активной цифровой трансформации, что требует модернизации как технических решений, так и процессов управления рисками. Ключ к устойчивой и безопасной экосистеме — комплексный подход: внедрение современных мер кибербезопасности (Zero Trust, WAF, SIEM, HSM), усиление AML/CFT-процедур с риск-ориентированным подходом, повышение квалификации персонала и цифровой грамотности клиентов, а также обеспечение взаимодействия на уровне «регулятор — частный сектор — национальные центры киберзащиты». Своевременное применение предложенных мер позволит снизить финансовые, репутационные и системные риски и сохранить доверие к безналичным платёжным инструментам.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Центральный банк Республики Узбекистан — Financial Stability Report, annual reports and press releases (2023–2024).
2. UzCERT / Cybersecurity Center — прогноз угроз и отчёты по инцидентам (2024–2025).
3. Материалы национальных СМИ и аналитики по кибербезопасности (Kun.uz, Yuz.uz) — данные о количестве кибератак и росте мошенничества.

⁷ https://uzcert.uz/en/forecast-of-major-cyber-threats-in-uzbekistan-for-2025/?utm_source



4. KPMG — Fintech & Payments in Uzbekistan (аналитический обзор по развитию платежей и рискам), 2023–2024.
5. FATF / EAG — материалы по оценке системы AML/CFT и рекомендации для стран региона (Mutual Evaluation materials).
6. Visa — аналитические материалы по электронным платежам и рискам внедрения (региональные обзоры).

muhandislik **& iqtisodiyot**

ijtimoiy-iqtisodiy, innovatsion texnik,
fan va ta'limga oid ilmiy-amaliy jurnal

Ingliz tili muharriri: Feruz Hakimov

Musahhih: Zokir Alibekov

Sahifalovchi va dizayner: Iskandar Islomov

2025

© Materiallar ko'chirib bosilganda "Muhandislik va iqtisodiyot" jurnali manba sifatida ko'rsatilishi shart. Jurnalda bosilgan material va reklamalardagi dalillarning aniqligiga mualliflar ma'sul. Tahririyat fikri har vaqt ham mualliflar fikriga mos kelamasligi mumkin. Tahririyatga yuborilgan materiallar qaytarilmaydi.

"Muhandislik va iqtisodiyot" jurnali 26.06.2023-yildan
O'zbekiston Respublikasi Prezidenti Adminstratsiyasi huzuridagi
Axborot va ommaviy kommunikatsiyalar agentligi tomonidan
№S-5669245 reyestr raqami tartibi bo'yicha ro'yxatdan o'tkazilgan.
Litsenziya raqami: №095310.

**Manzilimiz: Toshkent shahri Yunusobod
tumani 15-mavze 19-uy**





+998 93 718 40 07



<https://muhandislik-iqtisodiyot.uz/index.php/journal>



t.me/yait_2100