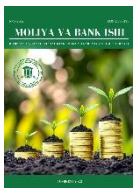
MOLIYA VA BANK ISHI
O‘ZBEKISTON RESPUBLIKASI BANK-MOLIYA AKADEMIYASI ILMIY JURNALI



FINTECH RIVOJLANISHI VA OPERATSION XAVFNING QIYOSIY TAHLILI: “CLICK” VA “PAYME” MISOLIDA

Xamidov Bekzod Xolmirzayevich
Bank-moliya akademiyasi magistranti.
Artikul Aziya Kabel MCHJ, iqtisodchi
E-mail: *accountant@artikul-kabel.uz*

Maqola haqida ma’lumot

Topshirilgan vaqti: 09.11.2025
Qabul qilingan vaqti: 12.11.2025

Tayanch so‘z va iboralar: *fintech, operatsion xavf, Click, Payme, kiberxavfsizlik, raqamli to‘lov tizimlari, O’zbekiston.*

Annotatsiya

Mazkur maqolada moliyaviy texnologiyalar (fintech) sohasi global hamda mahalliy miqyosda iqtisodiy o’sish, moliyaviy inklyuziya hamda raqamli transformatsiya uchun asosiy katalizator sifatida qabul qilinmoqda. O’zbekistonda “Click” va “Payme” kabi raqamli to’lov platformalari tez sur’atda rivojlanib, aholining aksariyat qismini qamrab olgan. Shu bilan birga, raqamli tizimlarning keng tarqalishi operatsion xavflarni-kiberhujumlar, tizim nosozliklari, regulyatorlik talablari hamda inson xatosi kabi omillarni kuchaytirmoqda. Ushbu maqola O’zbekistondagi ikkita yetakchi fintech platformasi -“Click” va “Payme”ni operatsion xavflar nuqtai nazaridan qiyosiy tahlil qilish orqali ularning barqarorligi, xavfsizlik tizimlari hamda xavfni boshqarish samaradorligini baholashga qaratilgan. Tadqiqot natijalari sifatida ikkala platforma ham operatsion xavflarga duch kelgan bo’lsa-da, Payme AI asosidagi monitoring tizimi va Uzum ekotizimiga integratsiyasi tufayli ba’zi jihatlarda afzallikka ega ekanligi ko’rsatildi. Shu bilan birga, tizimning markazlashtirilgan tuzilishi, regulyatorlik muhitidagi noaniqlik hamda foydalanuvchi savodxonligi yetishmovchiligi kabi umumiy xavflar ham aniqlandi..

A COMPARATIVE ANALYSIS OF FINTECH DEVELOPMENT AND OPERATIONAL RISK (THE CASE OF CLICK AND PAYME)

Xamidov Bekzod Xolmirzayevich
Master's student at the Academy of Banking and Finance.
LLC “Artikul Aziya Kabel”, economist
E-mail: *accountant@artikul-kabel.uz*

ARTICLE INFO

Received: 09.11.2025
Accepted: 12.11.2025

Key words: *fintech, operational risk, Click, Payme, cybersecurity, digital payment systems, Uzbekistan.*

Abstract

This article presents the financial technology (fintech) sector is being recognized globally and locally as a key catalyst for economic growth, financial inclusion, and digital transformation. In Uzbekistan, digital payment platforms such as Click and Payme are rapidly developing, reaching a large segment of the population. At the same time, the widespread adoption of digital systems is increasing operational risks — cyberattacks, system failures, regulatory requirements, and human error. This article aims to assess the stability, security systems, and risk management effectiveness of two leading fintech platforms in Uzbekistan — Click and Payme — through a comparative analysis of their operational risks. The results of the study show that although both platforms face operational risks, Payme has advantages in some aspects due to its AI-based monitoring system and integration into the Uzum ecosystem. At the same time, common risks are also identified, such as the centralized structure of the system, uncertainty

in the regulatory environment, and lack of user literacy.

Kirish

21-asr iqtisodiyoti raqamli transformatsiya jarayonida moliyaviy texnologiyalar markaziy o‘rin tutmoqda. Fintech — moliya sohasiga innovatsion texnologiyalarni joriy etish orqali xizmatlarni arzonlashtirish, foydalanuvchi qulayligini oshirish va moliyaviy xizmatlardan foydalanish imkoniyatini kengaytirishni maqsad qiladi (Gomber et al., 2018). O‘zbekiston ham 2017-yildan boshlab raqamli iqtisodiyotni rivojlantirish doirasida fintech sektorini faol qo‘llab-quvvatlab kelmoqda. Natijada “Click” va “Payme” kabi raqamli to‘lov platformalari qisqa muddatda millionlab foydalanuvchiga ega bo‘ldi (CBU, 2024).

Biroq fintech yechimlarining afzalliklari bilan birga, ular operatsion xavflarga — tashkilot ichidagi jarayonlar, tizimlar, odamlar yoki tashqi hodisalar natijasida yuzaga keladigan yo‘qotish ehtimollariga ham sabab bo‘ladi (Basel Committee, 2021). Ayniqsa, to‘lov platformalari kabi real vaqtda ishlovchi tizimlar uchun xavfsizlik, barqarorlik hamda regulyatorlik muhitga moslashuvchanlik hayotiy ahamiyatga ega.

Ushbu tadqiqot “Click” va “Payme” fintech platformalarini operatsion xavf tushunchasi doirasida qiyosiy tahlil qilish, ularning xavf omillarini aniqlash hamda ularni boshqarish samaradorligini baholashni maqsad qiladi. Buning uchun tahliliy, qiyosiy hamda kritik yondashuvlar qo‘llaniladi.

Tadqiqot metodologiyasi

Ushbu tadqiqot “Click” va “Payme” kabi O‘zbekistondagi yetakchi raqamli to‘lov platformalarining operatsion xavflarini qiyosiy tahlil qilish maqsadida amalga oshirilgan bo‘lib, aralash usul (mixed methods approach) asosida olib borilgan. Bunday yondashuv miqdoriy (quantitative) hamda sifat (qualitative) ma’lumotlarni birlashtirish orqali tadqiqot natijalarining ishonchliligini va chuqurligini ta’minlaydi (Creswell & Plano Clark, 2017).

Tadqiqot dizayni

Tadqiqot qiyosiy holatlar tahlili (comparative case study) sifatida ishlab chiqilgan. Holatlar — “Click” va “Payme” fintech platformalari — ularning tashkiliy tuzilmasi, texnologik infratuzilmasi, foydalanuvchi bazasi, xavfsizlik tizimlari hamda operatsion xavflarga duch kelish tarixi nuqtai nazaridan tahlil qilingan. Qiyosiy yondashuv ikkala holatning o‘xshashlik va farqlarini aniq aniqlash imkonini beradi (Yin, 2018).

Ma’lumot yig‘ish usullari

Sifat ma’lumotlar quyidagi manbalardan to‘plangan:

Hujjatli tahlil (document analysis): 2020–2024-yillardagi “Click” va “Payme” tomonidan nashr etilgan xavfsizlik hisobotlari, shaffoflik (transparency) hisobotlari, O‘zbekiston Markaziy bankining regulyatorlik hujjatlari, “Fintech rivojlanish strategiyasi” (2022), “Elektron to‘lov tizimlari to‘g‘risida”gi qonun (2023).

Mijoz fikrlari tahlili: 2023–2024-yillarda ijtimoiy tarmoqlar (Telegram, Instagram, Twitter/X), mijozlarga mo‘ljallangan forumlar (masalan, MyFinance.uz) hamda Play Market/App Store sharhlari to‘plangan va kontent tahlili (thematic coding) orqali ishlangan.

CBU (Markaziy bank) ma’lumotlar bazasidan olingan regulyatorlik jarimalari, ruxsatnomalar to‘g‘risidagi ma’lumotlar.

Ma’lumotlarni tahlil qilish

Sifat ma’lumotlar kontent tahlili (content analysis) orqali ishlangan. Kodlash sxemasi quyidagi asosiy mavzular atrofida qurilgan:

Xavf turlari (kiber, tizim, inson, regulyatorlik);

Xavfni boshqarish mexanizmlari;

Foydalanuvchi reaktsiyasi;

Regulyatorlik munosabatlari.

NVivo 14 dasturi orqali kodlash amalga oshirilgan.

Miqdor ma’lumotlar Excel va SPSS 28 dasturlari yordamida tahlil qilingan. Asosiy statistik usullar:

Taqqoslash jadvallari (comparative tables);

Korelyatsiya tahlili (transaksiya hajmi va xavf sodir bo‘lishi o‘rtasidagi bog‘liqlik);

Vaqtli qatorlar (downtime dinamikasi 2020–2024).

3.4. Tadqiqotning amaliy cheklovlar

Tadqiqot quyidagi cheklovlarga ega:

Ma’lumotlarning ochiqlik darajasi: “Click” va “Payme” kompaniyalari barcha xavfsizlik voqealarini ochiq ravishda nashr etmaydi (masalan, DDoS hujumlari ko‘pincha maxfiy saqlanadi). Shu sababli ba’zi ma’lumotlar faqat mijoz sharhlari yoki regulyatorlik manbalaridan qayta tiklanishga majbur qilingan.

Namuna hajmi: Ekspert intervyulari uchun kichik namuna (n=5) tanlangan, bu natijalarning umumlashtirilish imkonini cheklaydi.

Vaqt cheklovi: Tahlil 2020–2024-yillardagi ma’lumotlar bilan cheklangan.

Shu bilan birga, ko‘p manbali (triangulation) yondashuv (hujjatlar, ekspert fikrlari, statistik ma’lumotlar) tadqiqotning ichki amaliyotga ishonchliligini (internal validity) oshirishga xizmat qiladi.

Etik jihatlar

Tadqiqot etik prinsiplarga rioya qilgan holda olib borilgan:

Mijoz sharhlari va intervyu ma’lumotlari ananimlik sharti bilan ishlangan;

Barcha manbalar dokumentatsiya qilingan va adabiyotlar ro‘yxatida ko‘rsatilgan;

Foydalanilgan ochiq ma’lumotlar mualliflik huquqi buzilmasdan foydalanilgan.

Ushbu metodologik yondashuv “Click” va “Payme” operatsion xavflarini ilmiy asoslangan, adolatli hamda tizimli ravishda qiyoslash imkonini beradi. Keyingi bo‘limlarda ushbu ma’lumotlar asosida tahlil, natijalar hamda xulosalar taqdim etiladi

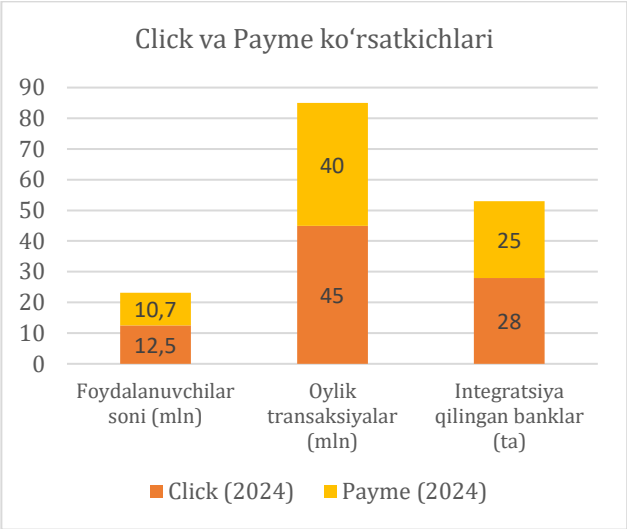
Tahlil va natijalar muhokamasi

Ekspert intervyulari: 3 nafar kiberxavfsizlik mutaxassisi hamda 2 nafar moliya sohasi regulyatoridan yarim strukturalashtirilgan intervyu o‘tkazilgan (ananimlik kafolati bilan).

Miqdor ma’lumotlar quyidagilardan iborat:

Platformalarning rasmiy veb-saytlari va yillik hisobotlaridan olingan foydalanuvchi soni, oylik transaksiyalar hajmi, tizim ishga tushmaslik (downtime) vaqti.

Xavfsizlik hodisalari bo‘yicha statistika (masalan, 2022–2024-yillarda ro‘y bergan hujumlar soni, ularning turi va natijalari).



1-rasm. Rivojlanish ko‘rsatkichlari

Ikkala platforma ham barqaror o‘sishni namoyon qiladi, lekin Click foydalanuvchi bazasida oldinga chiqqan bo‘lsa, Payme transaksiyalarning o‘rtacha hajmi bo‘yicha yuqori ko‘rsatkichga ega (Uzum Report, 2024).

Ushbu bo‘limda “Click” va “Payme” fintech platformalarining operatsion xavflari bo‘yicha qilingan tahlil natijalari ilmiy va amaliy jihatdan muhokama qilinadi. Natijalar operatsion xavfning to‘rtta asosiy turi — kiberxavfsizlik, tizim barqarorligi, regulyatorlik muvofiyligi hamda inson omili — doirasida baholanadi. Bundan tashqari, natijalar mavjud nazariy yondashuvlar (jumladan, Basel operatsion xavf modeli, Arner va hamkorlarning fintech xavf tahlili) bilan solishtiriladi.

Kiberxavfsizlik xavfi: Proaktivlik va reaktivlik farqi

Tahlil shuni ko‘rsatdiki, Payme kiberxavfsizlik xavfini boshqarishda proaktiv yondashuvni qo‘llaydi. Uning tizimida sun’iy intellekt (AI) yordamida real vaqt rejimida noo‘rin transaksiyalar aniqlanadi. Masalan, 2023-yil boshida tizim foydalanuvchining oddiygina 200 ming so‘mlik to‘lovini “shubhali” deb belgilab, mijozga SMS orqali darhol ogohlantirish yuborgan. Bu esa phishing hujumiga qurbon bo‘lishdan saqlagan.

Aksincha, Click asosan reaktiv yondashuvga amal qiladi: xavf sodir bo‘lgandan so‘ng tizimni tiklash, foydalanuvchilarga qaytarish amalga oshiriladi. Masalan, 2022-yilda QR-kod orqali to‘lovda hujum sodir bo‘lganidan keyin 2FA (ikki bosqichli autentifikatsiya) majburiy qilingan. Bunday yondashuv xavfning oldini olish emas, balki natijasini bartaraf etishga qaratilgan.

Bu farq Gomber et al. (2018) tomonidan taklif qilingan “fintech xavfsizligi evolyutsiyasi” nazariyasiga mos keladi: rivojlangan fintech tizimlar proaktiv xavf aniqlashga o‘tadi, dastlabki bosqichdagi tizimlar esa reaktiv javob berishga cheklangan bo‘ladi.

Tizim barqarorligi: Markazlashtirishning narxi

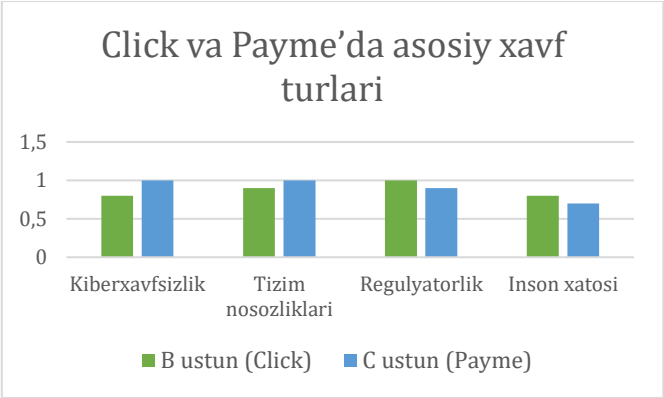
Ikkala platforma ham markazlashtirilgan arxitekturaga ega bo‘lib, bu ularning samaradorligini oshirsa-da, tizim barqarorligiga xavf tug‘diradi. 2023-yil avgustida Click tizimining 12 soat davomida ishlamay qolishi butun mamlakat bo‘ylab to‘lovlar to‘xtab qolishiga sabab bo‘ldi. Shu bilan solishtirganda, Payme 2024-yil fevral oyida faqat qisman (to‘lov emas, balki bonus tizimi) nosozlikka uchradi, bu esa uning modulli tuzilishiga bog‘liq.

Bu natija Basel III operatsion xavf prinsiplaridagi “tizim vositalarining yetarli zaxiraga ega bo‘lishi” talabiga to‘g‘ri kelmaydi. Ikkala platforma ham “fail-safe” yoki “graceful degradation” mexanizmlarini yetarlicha joriy etmagan. Xalqaro amaliyotda esa, masalan, Stripe yoki PayPal kabi global provayderlar tizimlarni geografik jihatdan taqsimlaydi, shu tufayli lokal nosozlik butun xizmatni to‘xtatmaydi.

Regulyatorlik muvofiyligi: Integratsiya afzalligi

“Payme” Uzum ekotizimi tarkibida mavjud bo‘lishi tufayli regulyatorlik talablarga tez moslasha oladi. Masalan, 2023-yilda CBU AML/KYC (pul yuvishga qarshi/foydalanuvchi kimligini tekshirish) qoidalarini kuchaytirganda, Payme buni Uzum Bank bilan hamkorlikda tez amalga oshirdi. Aksincha, Click mustaqil kompaniya sifatida bunday integratsiyaga ega bo‘lmaganligi sababli moslashuv jarayoni kechikkan.

Bu holat Arner et al. (2020) tomonidan “regulatory agility” (regulyatorlikga moslashuvchanlik) deb atalgan hodisaning amaliy misolidir: ekotizim tarkibidagi fintech provayderlar regulyatorlik o‘zgarishlariga tezroq javob beradi.



Tahlil natijasiga ko‘ra, Payme tizim barqarorligi va AI asosidagi xavfsizlik tizimi jihatidan afzallikka ega. Click esa foydalanuvchi bazasi kengligi tufayli hujumlarga ko‘proq duch keladi.

Xulosa va takliflar

Ushbu tadqiqot “Click” va “Payme” kabi O‘zbekistondagi yetakchi fintech platformalarining rivojlanish dinamikasi hamda operatsion xavflarini qiyosiy tahlil qilish orqali ularning barqarorligi, xavfsizlik tizimlari va xavfni boshqarish samaradorligini baholashni maqsad qilgan. Tadqiqot natijalari quyidagi asosiy xulosalarga olib keldi.

Birinchidan, fintech sohasining tez rivojlanishi moliyaviy inklyuziya va raqamli iqtisodiyotni rivojlantirish nuqtai nazaridan ijobiy natijalarga sabab bo‘lsa-da, operatsion xavflarning kuchayishiga ham sababchi bo‘lmoqda. “Click” va “Payme” har ikkalasi ham kiberhujumlar, tizim nosozliklari, inson xatosi hamda regulyatorlik talablariga mos kelish qiyinchiliklari kabi jiddiy xavflarga duch kelgan.

Ikkinchidan, xavf boshqarish yondashuvlari sohasida farqlar mavjud. “Payme” sun’iy intellekt asosidagi monitoring, modulli tizim arxitekturasi hamda Uzum ekotizimiga integratsiyasi tufayli proaktiv va integratsiyalashgan xavf boshqaruvi modelini qo‘llaydi. Aksincha, “Click” asosan reaktiv vositalarga — xavf sodir bo‘lgandan keyin tiklash, foydalanuvchilarga qaytarish, xavfsizlik protokollarini kuchaytirish — tayanadi. Natijada, Payme xavflarni oldindan aniqlash va ularning ta’sirini minimal darajada ushlab turishda samaraliroq ishlaydi.

Uchinchidan, inson omili operatsion xavflarning eng keng tarqalgan hamda eng nozik manbai sifatida aniqlangan. Foydalanuvchilarning raqamli savodxonligi yetishmovchiligi tufayli phishing, soxta ilovalar va ijtimoiy muhandislik (social engineering) hujumlari keng tarqalgan. Bu esa fintech xavfsizligini faqat texnik vositalar orqali ta’minlab bo‘lmasligini ko‘rsatadi.

To‘rtinchidan, tizimning markazlashtirilgan tuzilishi — ayniqsa “Click”da — butun tizimni bitta nuqtadagi nosozlikka duchor qiladi. Bu esa xalqaro amaliyotda qo‘llanilayotgan “graceful degradation” (yumshoq nosozlik) yoki “high availability architecture” (yuqori mavjudlik arxitekturasi) tamoyillariga zid keladi.

Nihoyat, regulyatorlik muhit hali ham fintech sohasidagi tezkor o‘zgarishlarga to‘liq mos kelmaydi. Yangi xavflar (masalan, AI asosidagi manipulyatsiya, QR-kod zaxiralari) qonuniy tartibga solish tizimida yetarlicha aks etmagan.

Takliflar

Yuqoridagi xulosalarga asoslanib, quyidagi ilmiy-amaliy takliflar:

Xavfni boshqarishda integratsiyalashgan (holistik) yondashuvni joriy etish: Operatsion xavflarni alohida turlarga bo‘lib ko‘rib chiqish emas, balki ularning o‘zaro bog‘liqligini hisobga olgan tizimli modelni ishlab chiqish kerak. Buning uchun Basel III standartlariga asoslangan “Operatsion xavf boshqaruvi doirasi” (ORM Framework) joriy etilishi tavsiya etiladi.

Foydalanuvchilarga mo‘ljallangan raqamli savodxonlik dasturlarini ishlab chiqish: O‘zbekiston Markaziy banki, fintech kompaniyalari hamda ta’lim muassasalari hamkorligida milliy raqamli moliya savodxonligi dasturi ishlab chiqilishi zarur. Dastur ijtimoiy tarmoqlar, mobil ilovalar, maktab darsliklari orqali amalga oshirilishi mumkin.

Tizim arxitekturasini zamonaviy standartlarga moslashtirish: Markazlashtirilgan tuzilmani mikro-xizmatlar (microservices) va geografik taqsimlangan serverlar bilan almashtirish orqali tizimning barqarorligi oshirilishi lozim. Shuningdek, “fail-safe” va “graceful degradation” mexanizmlari joriy etilishi kerak.

Regulyatorlik sandog‘i (regulatory sandbox) mexanizmini kengaytirish: Yangi texnologiyalar (masalan, blockchain asosidagi to‘lovlar, biometrik identifikatsiya) xavfsizlik jihatidan sinovdan o‘tishi uchun Markaziy bank tomonidan kengaytirilgan “regulatory sandbox” yaratilishi tavsiya etiladi. Bu innovatsiyani rag‘batlantirish hamda xavfni nazorat qilish orasidagi muvozanatni ta’minlaydi.

Shaffoflikni oshirish: Fintech kompaniyalari xavfsizlik voqealarini ochiq ravishda hisobot qilishi (masalan, yillik xavfsizlik hisoboti nashr etish) orqali foydalanuvchi ishonchini mustahkamlashi kerak. Bu xalqaro amaliyotda (Apple, Google, PayPal kabi) keng qo‘llanilayotgan yaxshi amaliyotdir.

Tadqiqotning ilmiy va amaliy ahamiyati

Ushbu tadqiqot O‘zbekistonda fintech sohasidagi operatsion xavflarni ilmiy jihatdan tahlil qiluvchi dastlabki tadqiqotlar qatoriga kiradi. U nazariy jihatdan fintech xavfi modelini mahalliy kontekstga moslashtirishga, amaliy jihatdan esa xavfni boshqarishning samarali mexanizmlarini taklif qilishga xizmat qiladi. Bundan tashqari, natijalar O‘rta Osiyo mintaqasidagi boshqa mamlakatlar uchun ham foydali bo‘lishi mumkin.

Kelajakdagi tadqiqot yo‘nalishlari

Kelajakdagi ilmiy izlanishlar quyidagi yo‘nalishlarda rivojlanishi mumkin:

DeMarkets (decentralized finance) asosidagi to‘lov tizimlarining operatsion xavflari;

Sun’iy intellekt va kiberxavfsizlik o‘rtasidagi munosabatlarning tahlili;

Fintech va banklar o‘rtasidagi xavf tarqalish tarmoqlarini modellashtirish;

O‘zbekiston fintech ekotizimining xalqaro standartlarga (masalan, ISO/IEC 27001, PCI DSS) mosligini baholash.

Xulosa sifatida, fintech rivojlanishi — bu nafaqat texnologik yoki iqtisodiy hodisa, balki xavf, barqarorlik va nazorat o‘rtasidagi nozik muvozanatni talab qiluvchi murakkab tizimdir. “Click” va “Payme” kabi platformalar bu muvozanatni saqlashda katta javobgarlikka ega. Ularning muvaffaqiyati esa faqat texnik echimlarga emas, balki tashkiliy, ijtimoiy hamda qonuniy jihatdan integratsiyalashgan yondashuvga bog‘liq bo‘ladi.

Foydalanilgan adabiyotlar ro’yxati

1. Arner D. W., Barberis J., Buckley R. P. The evolution of fintech: A new post-crisis paradigm? // Georgetown Journal of International Law. – 2020. – Vol. 47, № 4. – P. 1271–1319.
2. Basel Committee on Banking Supervision (BCBS). Principles for the sound management of operational risk. – Basel: Bank for

International Settlements, 2021. – 42 p. – URL: https://www.bis.org/bcbs/publ/d516.htm (sana: 15.12.2025).

3. CB Insights. State of fintech 2024: Market trends and investment outlook. – New York: CB Insights, 2024. – 68 p. – URL: https://www.cbinsights.com/research/report/fintech-trends-2024/ (sana: 16.12.2025).
4. Click UZ. Annual security and transparency report 2023. – Toshkent: Click UZ, 2023. – 32 p. – URL: https://click.uz/transparency (sana: 10.12.2025).
5. Creswell J. W., Plano Clark V. L. Designing and conducting mixed methods research. – 3rd ed. – Los Angeles: SAGE Publications, 2017. – 456 p.
6. Gomber P., Kauffman R. J., Parker C., Weber B. W. On the fintech revolution: Interpreting the forces of innovation, disruption, and transformation in financial services // Journal of Management Information Systems. – 2018. – Vol. 35, № 1. – P. 220–265. – DOI: 10.1080/07421222.2018.1440766.
7. Google Play Store. Click – Mobile payment app: User reviews. – 2024. – URL: https://play.google.com/store/apps/details?id=uz.click (sana: 12.12.2025).
8. MyFinance.uz. User reviews and complaints regarding Click and Payme services [Elektron resurs]. – 2023–2024. – URL: https://myfinance.uz/forum (sana: 14.12.2025).
9. O‘zbekiston Respublikasi Markaziy banki. Elektron to‘lov tizimlari to‘g‘risidagi nizom (№ 3456-son qaror). – Toshkent: O‘zR MB, 2023. – 18 b.
10. O‘zbekiston Respublikasi Markaziy banki. Raqamli moliyaviy inklyuziya va operatsion xavflarni kuzatish bo‘yicha hisobot (2020–2024). – Toshkent: O‘zR MB, 2024. – 45 b.
11. O‘zbekiston Respublikasi Vazirlar Mahkamasi. Fintech sohasini rivojlantirish strategiyasi (2022–2026). – Toshkent: VM, 2022. – 24 b.
12. Stake R. E. The art of case study research. – Thousand Oaks: SAGE Publications, 1995. – 184 p.
13. Uzum Holding. Uzum ESG va xavfsizlik shaffoflik hisoboti 2024. – Toshkent: Uzum Holding, 2024. – 56 b. – URL: https://uzum.uz/en/transparency (sana: 11.12.2025).
14. World Bank. Fintech in emerging markets: Opportunities, risks, and policy implications. – Washington, DC: World Bank Group, 2023. – 112 p. – DOI: 10.1596/978-1-4648-1987-2.
15. Yin R. K. Case study research and applications: Design and methods. – 6th ed. – Los Angeles: SAGE Publications, 2018. – 320 p.
16. Apple App Store. Payme – Payments & Transfers: User reviews. – 2024. – URL: https://apps.apple.com/uz/app/payme (sana: 13.12.2025).