

JOURNAL OF DIGITAL LAW AND INNOVATION (JDLI)

LAW • TECHNOLOGY • INNOVATION • JUSTICE

 OPEN
ACCESS

ISSN
3093-9364



OUR FIELDS

- Digital law
- Cybersecurity law
- Artificial intelligence and robotics law
- Intellectual property law
- LegalTech and legal innovations
- E-government and digital public services
- Legal aspects of AgroTech and GreenTech
- Smart city and digital governance



OUR INDEXING

 Google Scholar

 Zenodo

 DOI

 OpenAIRE

 Open Access



AI

! Unauthorized Access

UNAUTHORIZED
ACCESS

SYSTEM
BREACH



CYBER ATTACK



DIGITAL LAW



<https://unireview.uz/index.php/jdli>



Published by
UniLex Global



VOLUME 2

ISSUE 1



AUGUST 2026



“UNILEX GLOBAL” LLC

**Raqamli huquq va innovatsiya
jurnali
Journal of Digital Law and
Innovation**

**August, 2026
VOLUME 2, ISSUE 1**



ADVANCED SCIENCE INDEX



EDITORIAL TEAM

Editor-in-Chief, Tukhtashev Hikmatilla Ismatillaevich - Head of the Department of Legal Sciences, Doctor of Philosophy in Legal Sciences (PhD), TIAME National Research University, Tashkent, Republic of Uzbekistan.

1. **Editorial Board Member Borotov Mirodiljon Xomudjonovich** — Doctor of Legal Sciences, Professor, Head of the Department of Civil Law, International Law and International Organizations, Institute of State and Law of the Academy of Sciences of the Republic of Uzbekistan, Tashkent, Republic of Uzbekistan.
2. **Editorial Board Member Maripova Sevarxon Aribjanovna** — Doctor of Philosophy in Legal Sciences (PhD), Associate Professor, Department of Social Sciences, Cyber University State University, Tashkent, Republic of Uzbekistan.
3. **Editorial Board Member Kaharova Munira Maxamajanovna** — Doctor of Political Sciences (DSc), Researcher, Institute of Criminology of the Republic of Uzbekistan, Tashkent, Republic of Uzbekistan.
4. **Editorial Board Member Yuldashev Mutalib Ibrohimovich** — Doctor of Economic Sciences, Professor, Department of Economics, Tashkent University of Science and Technology, Tashkent, Republic of Uzbekistan.
5. **Editorial Board Member Bafaev Shukhrat Gafurovich** — Doctor of Legal Sciences, Head of the Tashkent City Branch, Center for the Analysis of Democratic Processes, Tashkent, Republic of Uzbekistan.
6. **Editorial Board Member Khodjaeva Aziza Bakhtiyarovna** — Doctor of Philosophy in Legal Sciences (PhD), "Academy of Labor and Social Relations" under the Federation of Trade Unions of the Republic of Uzbekistan, Tashkent, Republic of Uzbekistan.
7. **Editorial Board Member Khudoyberdieva Viloyat Jabbrovanovna** — Candidate of Legal Sciences (PhD), Olmazor District Department of Public Education, Tashkent City, Republic of Uzbekistan.
8. **Editorial Board Member Boboumarova Munira Kurbonovna** — Doctor of Philosophy in Legal Sciences (PhD), Department for Organization of Investigative Activities, Investigation Division, Tashkent City Internal Affairs Department, Tashkent, Republic of Uzbekistan.
9. **Editorial Board Member Usmonov Vosid Muhammadievich** — Doctor of Philosophy in Legal Sciences (PhD), Diplomatic University, Tashkent, Republic of Uzbekistan.
10. **Editorial Board Member Mirzayeva Malika Baxadirovna** — Doctoral Researcher, PhD, Associate Professor, Department of Digital Technologies and Artificial Intelligence, Tashkent Institute of Irrigation and Agricultural Mechanization Engineers – National Research University, Tashkent, Republic of Uzbekistan.
11. **Editorial Board Member Allayorov Tulqin Ruziqulovich** — Doctor of Philosophy in Philology (PhD), Associate Professor, Nizami Named Tashkent State Pedagogical University, Tashkent, Republic of Uzbekistan.
12. **Editorial Board Member Tosheva Maftuna Anvar kizi** — Doctor of Philosophy in Legal Sciences (PhD), Tashkent Institute of Irrigation and Agricultural Mechanization Engineers – National Research University, Tashkent, Republic of Uzbekistan.
13. **Editorial Board Member Askarov Jaloliddin Toychievich** — Doctor of Philosophy in Legal Sciences (PhD), Deputy Head, Department of Business Law, Tashkent State University of Law, Tashkent, Republic of Uzbekistan.
14. **Editorial Board Member Abdixakimov Islombek Bahodir o'g'li** — Master of Law (LL.M), Head of the Artificial Intelligence and Legal Tech Laboratory, Tashkent State University of Law, Tashkent, Republic of Uzbekistan.
15. **Editorial Board Member Kalandarov Aminjon Amondullayevich** — Doctor of Philosophy in Legal Sciences (PhD), Acting Associate Professor, Department of Business Law, Tashkent State University of Law, Tashkent, Republic of Uzbekistan.
16. **Editorial Board Member Hakimov Komil Bakhtiyarovich** — Doctor of Legal Sciences (DSc), Professor, Head of the Department of Criminal Law, Criminology and Anti-Corruption, Tashkent State University of Law, Tashkent, Republic of Uzbekistan.

RAQAMLI MOLİYAVIY XIZMATLAR TIZIMIDA KIBERXAVFSIZLIKNI TA'MINLASHNING INSTITUTSIONAL VA IQTISODIY MEXANIZMLARI

Sattarov Ulug'bek Umed o'g'li

*“TIQXMMI” Milliy tadqiqot universiteti “Iqtisodiyot”
fakulteti “Buxgalteriya hisobi” ta’lim yo’nalishi talabasi*
<https://orcid.org/0009-0007-9378-5394>

MAQOLA MA'LUMOTI

Kalit so'zlar:

kiberxavfsizlik,
raqamli moliyaviy xizmatlar,
fintex,
moliyaviy barqarorlik,
raqamli risklar,
institutSIONal tartibga solish,
kiberrisklarni sug'urtalash.

ANNO TATSIYA

Maqolada raqamli moliyaviy xizmatlar (internet-banking, mobil to'lov tizimlari, fintex platformalari) sohasida kiberxavfsizlikni ta'minlashning institutsional va iqtisodiy jihatlarini tahlil qilingan. Tadqiqotda kontent-tahlil, qiyosiy tahlil va mantiqiy-tarixiy usullardan foydalanilgan holda raqamlashtirish jarayonida yuzaga keladigan yangi turdagi risklarning iqtisodiy tabiati, ularning moliyaviy barqarorlikka ta'siri hamda ularni boshqarishning institutsional va iqtisodiy mexanizmlari o'rganilgan. Natijalar shuni ko'rsatdiki, kiberxavfsizlik endi texnik emas, balki moliyaviy barqarorlikning ajralmas iqtisodiy omili sifatida qaralishi lozim. Maqola oxirida raqamli moliyaviy xizmatlar sohasida kiberxavfsizlikni ta'minlash bo'yicha amaliy tavsiyalar ishlab chiqilgan.

INSTITUTIONAL AND ECONOMIC MECHANISMS FOR ENSURING CYBERSECURITY IN DIGITAL FINANCIAL SERVICES

ARTICLE INFO

Keywords:

cybersecurity,
digital financial services,
fintech,
financial stability,
digital risks,

ABSTRACT

The article analyzes the institutional and economic aspects of ensuring cybersecurity in digital financial services (internet banking, mobile payment systems, fintech platforms). Using content analysis, comparative analysis, and logical-historical methods, the study examines the economic nature of new risks arising from digitalization, their impact on financial stability, and the institutional and economic

*institutional regulation,
cyber-insurance.*

mechanisms for managing them. The results show that cybersecurity should no longer be viewed as a purely technical issue, but as an integral economic factor of financial stability. The article concludes with practical recommendations for ensuring cybersecurity in the digital financial services sector.

ИНСТИТУЦИОНАЛЬНЫЕ И ЭКОНОМИЧЕСКИЕ МЕХАНИЗМЫ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ В СИСТЕМЕ ЦИФРОВЫХ ФИНАНСОВЫХ УСЛУГ

ИНФОРМАЦИЯ СТАТЬИ

Ключевые слова:

кибербезопасность,
цифровые финансовые
услуги,
финтех,
финансовая стабильность,
цифровые риски,
институциональное
регулирование,
киберстрахование.

АННОТАЦИЯ

В статье анализируются институциональные и экономические аспекты обеспечения кибербезопасности в сфере цифровых финансовых услуг (интернет-банкинг, системы мобильных платежей, финтех-платформы). С использованием методов контент-анализа, сравнительного и логико-исторического анализа исследована экономическая природа новых рисков, возникающих в процессе цифровизации, их влияние на финансовую стабильность, а также институциональные и экономические механизмы управления ими. Результаты показывают, что кибербезопасность следует рассматривать не как чисто техническую, а как неотъемлемую экономическую составляющую финансовой стабильности. В заключение статьи разработаны практические рекомендации по обеспечению кибербезопасности в сфере цифровых финансовых услуг.

KIRISH

So'nggi o'n yillikda moliyaviy xizmatlar sohasi jadal sur'atlarda raqamlashtirilmoqda: mobil to'lov ilovalari, internet-banking tizimlari, elektron hamyonlar va fintex platformalari an'anaviy bank xizmatlarining o'rnini tobora ko'proq egallamoqda. Ushbu jarayon moliyaviy xizmatlarga kirish imkoniyatini kengaytirib, tranzaksiya xarajatlarini kamaytirsada, shu bilan birga yangi turdagi zaifliklarni — kiberhujumlar, ma'lumotlar sizib chiqishi, moliyaviy firibgarlik kabi risklarni — vujudga keltirmoqda. Bu holat mavzuning yuqori dolzarbligini belgilaydi.

Mavzuning o'rganilish darajasi bo'yicha xalqaro miqyosda Moliyaviy barqarorlik kengashi (FSB), Bazel bank nazorati qo'mitasi, Xalqaro valyuta fondi va Butunjahon iqtisodiy forumi kabi tashkilotlar kiberxavfsizlik va moliyaviy barqarorlik o'rtasidagi bog'liqlikni faol o'rganmoqda. Shu bilan birga, kiberrisklarni iqtisodiy rag'batlantirish mexanizmlari, xususan sug'urta instituti orqali boshqarish masalalari C. Biener, M. Eling, N. Kshetri kabi tadqiqotchilarning ishlarida yoritilgan. Rivojlanayotgan iqtisodiyotlar, jumladan O'zbekiston sharoitida esa ushbu masalaning institutsional-huquqiy jihatlari yetarlicha tadqiq etilmagan, bu esa ushbu maqolaning ilmiy yangiligini belgilaydi.

Shuni ta'kidlash joizki, kiberxavfsizlik muammosi endilikda alohida davlatlar chegarasidan chiqib, transchegaraviy tavsifga ega bo'lib bormoqda: zamonaviy to'lov tizimlari va moliyaviy infratuzilmalarning o'zaro integratsiyalashuvi tufayli bitta mamlakatdagi kiberhujum boshqa mamlakatlarning moliyaviy barqarorligiga ham ta'sir ko'rsatishi mumkin. Bu jihat mavzuni nafaqat milliy, balki global moliyaviy barqarorlik nuqtai nazaridan ham dolzarb qiladi.

Tadqiqotning maqsadi — raqamli moliyaviy xizmatlar tizimida kiberxavfsizlikni ta'minlashning institutsional va iqtisodiy mexanizmlarini tahlil qilish hamda milliy sharoitga mos amaliy tavsiyalar ishlab chiqishdan iborat.

TADQIQOT METODOLOGIYASI

Tadqiqotda kontent-tahlil, mantiqiy-tarixiy tahlil, qiyosiy tahlil hamda tizimli yondashuv usullaridan foydalanildi. Xalqaro moliyaviy tashkilotlarning me'yoriy hujjatlari va tahliliy hisobotlarini o'rganishda kontent-tahlil usuli; kiberrisklarning iqtisodiy tabiatini ochib berishda sabab-oqibat tahlili; turli mamlakatlarning tartibga solish tajribasini solishtirishda qiyosiy tahlil usuli qo'llanildi. Tadqiqot sifat tavsifiga (qualitative) ega bo'lib, institutsional-iqtisodiy tahlilga asoslangan.

Xalqaro amaliyotni o'rganishda asosiy manba sifatida Moliyaviy barqarorlik kengashining kiberinsidentlar to'g'risida hisobot berish bo'yicha tavsiyalari [1], Bazel bank nazorati qo'mitasining operatsion barqarorlik tamoyillari [2] hamda Yevropa Markaziy bankining moliyaviy bozor infratuzilmalari uchun kiber-chidamlilik bo'yicha kutilmalari [7] tahlil qilindi. Ushbu me'yoriy hujjatlar tartibga soluvchi institutlarning kiberxavfsizlikka nisbatan yondashuvidagi umumiy tamoyillarni aniqlash imkonini berdi, bu esa tadqiqotning institutsional tahlil qismi uchun metodologik asos vazifasini o'tadi.

TAHLIL VA NATIJALAR

1. Raqamli moliyaviy risklarning iqtisodiy tabiati. Tadqiqot natijalariga ko'ra, kiberxavfsizlik bilan bog'liq risklarni ikki asosiy guruhga ajratish mumkin: to'g'ridan-to'g'ri moliyaviy zarar (mablag'larning o'g'irlanishi, firibgarlik operatsiyalari) va bilvosita iqtisodiy zarar (mijozlar ishonchining pasayishi, tashkilot obro'siga putur yetishi, huquqiy javobgarlik xarajatlari). Bilvosita zararlar ko'pincha to'g'ridan-to'g'ri moliyaviy yo'qotishlardan ham yuqori bo'ladi, chunki ishonchni tiklash uzoq muddatli va qimmat jarayondir. Bundan tashqari, moliyaviy tizimning o'zaro bog'liqligi tufayli bitta muassasadagi kiberhujum tizimli risk (systemic risk) shakliga o'tishi mumkin.

IMFning moliyaviy barqarorlik bo'yicha hisobotida [3] ta'kidlanishicha, moliyaviy tizimning yuqori darajada o'zaro bog'liqligi sharoitida bitta yirik kiberhujum global miqyosda tizimli beqarorlikni keltirib chiqarishi mumkin, chunki zamonaviy to'lov infratuzilmalari biri-biri bilan chambarchas bog'langan. Butunjahon iqtisodiy forumining kiberxavfsizlik bo'yicha global sharhida [5] ko'rsatilishicha, moliya sektori boshqa tarmoqlarga nisbatan kiberhujumlarning eng ko'p nishoniga aylangan sohalardan biri hisoblanadi, bu esa bilvosita zararlarning — ayniqsa obro'-e'tibor yo'qotilishi va mijozlar bazasining qisqarishi — nisbiy ulushini yanada oshiradi.

2. Institutsional tartibga solish mexanizmlari. Tadqiqot jarayonida kiberxavfsizlikni ta'minlashning quyidagi institutsional mexanizmlari aniqlandi: markaziy bank va moliyaviy nazorat organlari tomonidan minimal kiberxavfsizlik standartlarini majburiy tartibda joriy etish; moliyaviy tashkilotlar uchun majburiy audit va stress-test tizimini kiberrisklar bo'yicha ham qo'llash; insidentlar to'g'risida hisobot berish tizimini (mandatory incident reporting) yaratish; davlat-xususiy sektor hamkorligi asosida kiberxavfsizlik markazlarini (CERT/CSIRT) rivojlantirish. Bunday institutsional infratuzilma alohida tashkilotlarning individual harakatlariga qaraganda ancha samaraliroq ekanligi aniqlandi.

Bazel bank nazorati qo'mitasining tamoyillariga ko'ra [2], operatsion chidamlilik faqat texnik infratuzilmani mustahkamlash bilan emas, balki tashkilotning boshqaruv jarayonlarini kiberxavflarga moslashtirish orqali ta'minlanadi. FSBning tavsiyalariga muvofiq [1], insidentlar to'g'risida hisobot berishning yagona standartlashtirilgan formati turli yurisdiksiyalar o'rtasidagi ma'lumot almashinuvini osonlashtiradi va tizimli risklarni erta aniqlash imkonini beradi. ECB tajribasida [7] moliyaviy bozor infratuzilmalari uchun belgilangan kiber-chidamlilik kutilmalari uch bosqichli yondashuvga — oldini olish, aniqlash va tiklanish — asoslangan bo'lib, bu model boshqa mintaqalar uchun ham amaliy ahamiyatga ega. OECDning bank sektoridagi raqamli buzilish bo'yicha tahlilida [6] ta'kidlanishicha, tartibga solishning ortiqcha qattiqligi innovatsion fintex-yechimlarning bozorga kirishini sekinlashtirishi mumkin, shu sababli institutsional mexanizmlar moslashuvchan bo'lishi lozim.

3. Iqtisodiy rag'batlantirish vositalari. Tadqiqot shuni ko'rsatdiki, faqat majburiy me'yorlar bilan cheklanish kifoya qilmaydi. Kiberxavfsizlikka investitsiya kiritishni rag'batlantiruvchi iqtisodiy vositalar sifatida quyidagilar aniqlandi: kiberxavfsizlik bo'yicha xarajatlarni soliq bazasidan chegirish; kiberrisklarni sug'urtalash bozorini rivojlantirish;

xavfsizlik standartlariga rioya qilgan tashkilotlar uchun litsenziyalash jarayonini soddalashtirish. Kiberrisklarni sug'urtalash instituti tashkilotlarni profilaktik choralarga investitsiya kiritishga iqtisodiy jihatdan undaydi, chunki sug'urta mukofoti xavfsizlik darajasiga bog'liq bo'ladi.

Biener, Eling va Wirfsning empirik tadqiqotiga ko'ra [8], kiberrisklarning barcha turlari bir xil darajada sug'urtalanishi mumkin emas — ayniqsa korrelyatsiyalashgan (bir vaqtda ko'p tashkilotni qamrab oluvchi) hujumlar tufayli yuzaga keladigan zararlar an'anaviy aktuar modellarga yaxshi sig'maydi. Kshetri [9] kiberrisklarni sug'urtalash bozorining rivojlanishi tashkilotlarni faqat zararni qoplash emas, balki xavfsizlik amaliyotlarini standartlashtirishga ham undashini ko'rsatadi, chunki sug'urta kompaniyalari mukofot stavkalarini xavfsizlik auditi natijalariga bog'laydi. Ashrafning rivojlanayotgan bozorlar bo'yicha tadqiqotida [10] ta'kidlanishicha, bunday iqtisodiyotlarda kiberrisklarni boshqarish ko'pincha me'yoriy talablarga rasman rioya qilish darajasida qolib ketadi, amaliy xavfsizlik madaniyati esa yetarlicha shakllanmagan bo'ladi — bu xulosa O'zbekiston sharoiti uchun ham dolzarbdir.

4. Milliy amaliyot va institutsional infratuzilma. O'zbekiston Respublikasi Markaziy bankining to'lov tizimlarida axborot xavfsizligini ta'minlash bo'yicha me'yoriy hujjatlari [12] milliy darajada dastlabki texnik-huquqiy asosni yaratgan bo'lsa-da, ular asosan minimal xavfsizlik talablarini belgilash bilan cheklangan va iqtisodiy rag'batlantirish elementlarini o'z ichiga olmaydi. Muallifning oldingi tadqiqotida [11] ko'rsatilganidek, moliyaviy institutlarning kiberxavfsizligini ta'minlash muammosi ko'p jihatdan kadrlar tayyorgarligi va institutsional monitoring tizimining yetishmasligi bilan bog'liq, bu esa ushbu maqolada taklif etilayotgan kompleks yondashuvning zarurligini yana bir bor tasdiqlaydi.

MUHOKAMA

Tadqiqot natijalarini xalqaro tajriba bilan solishtirganda shuni ta'kidlash mumkinki,

rivojlangan moliyaviy bozorlarga ega mamlakatlarda (AQSH, Yevropa Ittifoqi davlatlari) kiberxavfsizlik bo'yicha institutsional infratuzilma — CERT/CSIRT markazlari, majburiy insident hisobotini berish tizimlari va kiberrisklarni sug'urtalash bozori — allaqachon shakllangan. Rivojlanayotgan iqtisodiyotlarda esa, jumladan O'zbekistonda, ushbu institutsional infratuzilma hali shakllanish bosqichida bo'lib, ko'proq texnik-huquqiy tartibga solishga urg'u berilmoqda, iqtisodiy rag'batlantirish vositalari esa yetarlicha rivojlanmagan.

Bu borada N. Kshetri va C. Bienerlarning tadqiqotlarida [8; 9] ta'kidlanganidek, kiberrisklarni sug'urtalash instituti faqat rivojlangan sug'urta bozori mavjud bo'lgan mamlakatlarda samarali ishlaydi, chunki aktuar hisob-kitoblar uchun yetarli statistik ma'lumotlar bazasi talab qilinadi. Shu sababli O'zbekiston kabi rivojlanayotgan bozorlarda dastlabki bosqichda davlatning tartibga soluvchi roli, keyinchalik esa bozor mexanizmlarining bosqichma-bosqich rivojlantirilishi maqsadga muvofiqdir — bu xulosa ushbu tadqiqotning xalqaro adabiyotga qo'shgan o'ziga xos hissasi hisoblanadi.

Butunjahon iqtisodiy forumining ma'lumotlariga ko'ra [5], global miqyosda kiberxavfsizlik bo'yicha malakali kadrlar tanqisligi institutsional infratuzilmani rivojlantirishning asosiy to'siqlaridan biri hisoblanadi, bu muammo rivojlanayotgan bozorlarda yanada keskinroq namoyon bo'ladi. IMFning bahosiga ko'ra [3], kiberxavfsizlikka yetarli e'tibor bermagan moliyaviy tizimlar xalqaro kapital bozorlariga integratsiyalashuvda qo'shimcha risk mukofoti (risk premium) bilan yuzlashishi mumkin, bu esa kiberxavfsizlikni nafaqat ichki, balki tashqi moliyaviy barqarorlik nuqtai nazaridan ham strategik ahamiyat kasb ettiradi.

XULOSA

Raqamli moliyaviy xizmatlar tizimida kiberxavfsizlikni ta'minlash endi faqat texnik emas, balki chuqur iqtisodiy va institutsional mazmunga ega muammo hisoblanadi.

Kiberrisklarning tizimli xususiyati ularni davlat darajasidagi tartibga solish, moliyaviy nazorat organlarining faol ishtiroki hamda iqtisodiy rag‘batlantirish vositalari orqali boshqarishni taqozo etadi.

Tadqiqot natijalari asosida quyidagi amaliy takliflar ishlab chiqildi: birinchidan, Markaziy bank huzurida moliyaviy sektor uchun maxsus CERT/CSIRT markazini institutsionallashtirish; ikkinchidan, kiberinsidentlar to‘g‘risida majburiy va operativ hisobot berish tizimini joriy etish; uchinchidan, kiberxavfsizlik standartlariga rioya qiluvchi moliyaviy tashkilotlar uchun soliq va litsenziyalash imtiyozlarini nazarda tutish; to‘rtinchidan, milliy kiberrisklarni sug‘urtalash bozorini bosqichma-bosqich rivojlantirish uchun me‘yoriy-huquqiy baza yaratish; beshinchidan, moliya tashkilotlari xodimlarini kiberxavfsizlik bo‘yicha muntazam o‘qitish va malaka oshirish tizimini joriy etish.

Raqamli iqtisodiyotning barqaror rivojlanishi ko‘p jihatdan aynan shu sohadagi ishonch darajasiga bog‘liq bo‘lib, bu ishonchni faqat kompleks — institutsional, huquqiy va iqtisodiy — yondashuv orqali ta‘minlash mumkin.

FOYDALANILGAN ADABIYOTLAR RO‘YXATI

1. Financial Stability Board. Cyber Incident Reporting: Ensuring Effective Response to Cyber Incidents. — 2022.
2. Basel Committee on Banking Supervision. Principles for Operational Resilience. — Basel: Bank for International Settlements, 2021.
3. IMF. Cyber Risk and Financial Stability: It's a Small World After All // Global Financial Stability Report. — 2021.
4. World Bank. FinTech and the Future of Finance: Market and Policy Implications. — Washington, D.C., 2020.
5. World Economic Forum. Global Cybersecurity Outlook 2022. — Geneva, 2022.
6. OECD. Digital Disruption in Banking and its Impact on Competition. — Paris: OECD

Publishing, 2020.

7. European Central Bank. Cyber Resilience Oversight Expectations for Financial Market Infrastructures. — Frankfurt, 2021.
8. Biener, C., Eling, M., Wirfs, J.H. Insurability of Cyber Risk: An Empirical Analysis // The Geneva Papers on Risk and Insurance. — 2015. — Vol. 40, № 1. — P. 131–158.
9. Kshetri, N. The Economics of Cyber-Insurance // IT Professional. — 2021. — Vol. 23, № 2. — P. 34–39.
10. Ashraf, J. Digital financial services and cybersecurity risk management in emerging economies // Journal of Financial Regulation and Compliance. — 2022. — Vol. 30, № 4.
11. Sattarov, U.U. Raqamli iqtisodiyot sharoitida moliyaviy institutlarning kiberxavfsizligini ta'minlash muammolari // Iqtisodiyot va innovatsion texnologiyalar jurnali. — 2024. — № 3.
12. O'zbekiston Respublikasi Markaziy banki. To'lov tizimlarida axborot xavfsizligini ta'minlash bo'yicha me'yoriy hujjatlari. — Toshkent, 2023.