

## MOLIYAVIY OPERATSIYALARDA KIBERXAVFSIZLIK RISKLARINING IQTISODIYOT RIVOJLANISHIGA TA'SIRI

**G'iyosov Otabek Alisher o'g'li**

*Bank-Moliya Akademiyasi "Biznessni boshqarish" sirtqi ta'lim shakli magistratura  
II-bosqich talabasi*

**Annotatsiya:** Ushbu maqolada hozirgi kunda dolzarb mavzuga aylangan kiberxavfsizlik riski tushunchasi, uning iqtisodiyot rivojidagi dolzarb ahamiyati haqida ma'lumotlar keltirilgan. Shuningdek, moliyaviy operatsiyalardagi kiberxavfsizlik risklarining iqtisodiyotga ta'siri tahlil qilinadi. Kiberxavfsizlikning ishlab chiqarish jarayonlari, xizmat ko'rsatish tarmoqlari va iqtisodiy resurslar boshqaruvi sohalaridagi mavjud muammo va savollari, shuningdek, jamiyat va iqtisodiy tizim o'rtasidagi bog'liqlik darajasi o'rganiladi.

**Kalit so'zlar:** kiberxavfsizlik, moliyaviy risk, risklarni boshqarish, iqtisodiy rivojlanish, globallashtiruv, axborot xavfsizligi, moliyaviy operatsiyalar.

## ВЛИЯНИЕ РИСКОВ КИБЕРБЕЗОПАСНОСТИ В ФИНАНСОВЫХ ОПЕРАЦИЯХ НА ЭКОНОМИЧЕСКОЕ РАЗВИТИЕ

**Гийосов Отабек Алишерович**

*Банковско-финансовая академия «Бизнес-менеджмент», студент заочного  
отделения магистратуры II степени*

**Аннотация:** В данной статье представлена информация о понятии риска кибербезопасности, которое стало актуальным вопросом сегодня, и его актуальном значении в развитии экономики. Также анализируется влияние рисков кибербезопасности при финансовых операциях на экономику. Изучены существующие проблемы и вопросы кибербезопасности в сфере производственных процессов, сетей обслуживания и управления экономическими ресурсами, а также степень связи общества и экономической системы.

**Ключевые слова:** кибербезопасность, финансовый риск, управление рисками, экономическое развитие, глобализация, информационная безопасность, финансовые операции.

## IMPACT OF CYBERSECURITY RISKS IN FINANCIAL OPERATIONS ON ECONOMIC DEVELOPMENT

**G'iyosov Otabek Alisherovich**

*Banking and Finance Academy, 2nd year student of the correspondence course*

*"Business Management"*

+998977531445

**Abstract:** This article presents information about the concept of cybersecurity risk, which has become a topical issue today, and its current importance in economic development. It also analyzes the impact of cybersecurity risks in financial transactions on the economy. The current problems and issues of cybersecurity in the areas of production processes, service industries and economic resource management, as well as the level of connection between society and the economic system, are studied.

**Keywords:** *cybersecurity, financial risk, risk management, economic development, globalization, information security, financial transactions.*

### KIRISH

Pul muomalasi va uning amalga oshirilish jarayonlari iqtisodiyotning rivojlanishini tobora kuchaytiradi. Raqamli pul muomalasi iqtisodiy moliya tizimlari faoliyatining samaradorligini oshiribgina qolmay qator muammolarni ham keltirib chiqaradi. Kiberxavfsizlik borasidagi muammolar hozirda iqtisodiyotda juda jiddiy dolzarb masala sifatida turibti.

Kiberxavfsizlik muammolari ko'proq moliyaviy institutlar jumladan pul munosabatlarini yuritish bilan shug'ullanuvchi kompaniya, bank va tashkilotlarga ko'proq o'z ta'sirini o'tkazadi. Jahon savdo tizmining yomonlashuvi, investorlarning ishonchini buzilishi va katta moliyaviy yo'qotishlarga olib keladi. To'lovlarni amalga oshirish jarayonlarida yoki banklararo moliyaviy operatsiyalarni amalga oshirish jarayonlarida ko'plab kiberhujumlar amalga oshiriladi. Bu o'z navbatida iqtisodiy rivojlanishga ta'sir ko'rsatadi. Ko'pgina mamlakatlar jahon miqyosda raqamli moliyaviy tizimlarni qabul qilish bilan birga, kiberxavfsizlik borasidagi chora tadbirlarni ham ishlab chiqishmoqda.

Jumladan mamlakatimizda ham kiberxavfsizlik borasida "Kiberxavfsizlik to'g'risida"gi Qonun (O'RQ-764-son, 15.04.2022-y.) Prezident tomonidan qabul qilindi<sup>1</sup>. Moliyaviy operatsiyalarni amalga oshirish jarayonidagi kiberxavfsizlik muammolari nafaqat iqtisodiyotga balki jamiyat hayotiga ham o'z jiddiy ta'sirini ko'rsatadi.

<sup>1</sup> <https://onesecc.uz/uz/news/show/4>

Qonunga ko'ra, kibermakonda shaxs, jamiyat va davlat manfaatlarini tashqi va ichki tahdidlardan himoya qilish davlatning kibernetika xavfsizligini ta'minlashda ustuvor hisoblanadi. Kibernetika xavfsizlik sohasidagi yagona davlat siyosatini Prezident belgilaydi. Davlat xavfsizlik xizmati kibernetika xavfsizlik sohasidagi vakolatli davlat organidir. Qonunga ko'ra, davlat organlari va tashkilotlari kibernetika xavfsizlikni ta'minlash maqsadida vakolatli davlat organidan kibernetika tahdidlar, dasturiy ta'minotdagi, uskunalar va texnologiyalardagi zaifliklar to'g'risidagi axborotni olish huquqiga ega<sup>2</sup>.

Lekin mamlakatimizda murakkab kibernetika hujumlarga qarshi kurashish uchun kerakli texnologiyalar, kadrlar va bazalar yetishmaydi. Bu esa iqtisodiyot rivojlanishining oqsoqlanishiga taraqqiyot va ijtimoiy va siyosiy beqarorlikni yomonlashtirishga sabab bo'ladi.

Ushbu maqolada kibernetika xavfsizlik tahdidlari, moliyaviy operatsiyalar va ulardan kelib chiqadigan kibernetika xavf-xatarlarga, iqtisodiy muammolar keng tahlil qilingan.

Hozirgi globallashuv zamonida texnologiya, siyosat va iqtisodiyotni kibernetika xavfsizlik jihatdan muhofaza qilish bo'yicha tahlil olib bo'rish dolzarb masala bo'lib kelmoqda. Keyingi boblarda kibernetika xavflar, ularning manfaatdor tomonlarga ta'siri va yo'llari ko'rib chiqiladi.

Ushbu maqolada moliyaviy operatsiyalarda kibernetika xavfsizlik risklari va ularning iqtisodiyot rivojlanishiga ta'siri tahlil qilinadi.

Moliyaviy operatsiyalarda kibernetika xavfsizlik risklari quyidagi asosiy omillarni o'z ichiga oladi:

1. Ma'lumotlar o'g'irlanishi: Mijozlarning shaxsiy va moliyaviy ma'lumotlari kibernetika hujumchilar tomonidan o'g'irlanishi mumkin. Bu holat moliyaviy tashkilotlarga ishonchni pasaytiradi va mijozlarning xizmatlardan foydalanishidan voz kechishiga olib kelishi mumkin.

2. Tizimlarga kirish huquqi: Kibernetika hujumchilar moliyaviy tizimlarga kirish huquqini qo'lga kiritish orqali katta moliyaviy yo'qotishlarga sabab bo'lishi mumkin. Bu holat banklar va boshqa moliyaviy institutlar uchun jiddiy xavf tug'diradi.

3. Xavfsizlik tizimlarining zaifligi: Ko'plab moliyaviy tashkilotlar xavfsizlik tizimlarini yangilash va mustahkamlashda yetarli e'tibor bermaydilar. Bu esa kibernetika hujumchilarga osonlik bilan kirish imkonini beradi.

Moliyaviy operatsiyalarga nisbatan amalga oshirilgan kibernetika hujumlar iqtisodiyot rivojlanishiga bir necha jihatdan ta'sir ko'rsatadi:

1. Ishonchning pasayishi: Kibernetika hujumlar natijasida moliyaviy tashkilotlarga bo'lgan ishonch pasayadi. Bu esa mijozlarning xizmatlardan foydalanishidan voz kechishiga olib keladi va iqtisodiy o'sishga salbiy ta'sir ko'rsatadi.

<sup>2</sup> <https://yuz.uz/uz/news/kibernetika-xavfsizlik-qonun-bilan-tartibga-solindi>

2. Moliyaviy yo‘qotishlar: Kiberhujumlar natijasida moliyaviy tashkilotlar katta yo‘qotishlarga uchraydi. Bu moliyaviy resurslarning yo‘qolishiga va iqtisodiy o‘lishning sekinlashishiga olib kelishi mumkin.

3. Investitsiyalarning kamayishi: Kiberxavfsizlik masalalari moliyaviy tashkilotlarga investitsiyalarni jalb qilishda muammolar tug‘diradi. Investorlar xavf-xatarlarni hisobga olib, moliyaviy bozorlar va tashkilotlarga sarmoya kiritishdan ehtiyot bo‘lishadi.

Moliyaviy operatsiyalarda kiberxavfsizlik risklari iqtisodiyot rivojlanishiga salbiy ta‘sir ko‘rsatishi mumkin. Mijozlarning ishonchini saqlab qolish, moliyaviy yo‘qotishlarni kamaytirish va investitsiyalarni jalb qilish uchun moliyaviy tashkilotlar kiberxavfsizlikni mustahkamlashga e‘tibor qaratishlari zarur. Raqamli iqtisodiyot rivojlanishi davomida kiberxavfsizlik masalalariga jiddiy yondashish, barqaror va xavfsiz moliyaviy muhit yaratishda muhim ahamiyatga ega.

### ADABIYOTLAR TAHLILI

Bugungi kunda raqamli iqtisodiyotning rivojlanishi bilan birga moliyaviy operatsiyalar ham onlayn platformalarda kengaymoqda. Bu jarayon kiberxavfsizlik masalalarini yanada dolzarb qilmoqda. Kiberhujumlar va ma‘lumotlar o‘g‘irlash holatlari moliyaviy tashkilotlar va ularning mijozlari uchun jiddiy xavf tug‘dirmoqda. Bu masala ustida ko‘pgina iqtisodchi olimlar, ilmiy izlanuvchilar chuqur tadqiqotlar olib borishmoqda.

1. Kiberxavfsizlik moliyaviy tizimlar uchun muhim ahamiyatga ega, chunki moliyaviy ma‘lumotlar va operatsiyalar kiberhujumlar uchun asosiy maqsad bo‘lib xizmat qiladi. Kiberxavfsizlikning kuchayishi moliyaviy tashkilotlarning mijozlar ma‘lumotlarini himoya qilish va moliyaviy operatsiyalarni xavfsiz o‘tkazish imkoniyatlarini oshiradi. Anderson va Moore (2006) o‘z tadqiqotlarida kiberxavfsizlikning iqtisodiy ta‘sirini va moliyaviy tizimlar uchun xavflarni tahlil qiladilar<sup>3</sup>.

2. Kiberhujumlar moliyaviy tashkilotlarga katta moliyaviy yo‘qotishlarga olib kelishi mumkin. Kiberhujumlar natijasida yuzaga keladigan yo‘qotishlar, shuningdek, mijozlar ishonchini yo‘qotish va brendning obro‘sigacha zarar yetkazishi mumkin. Ponemon Institute (2020) tomonidan o‘tkazilgan tadqiqotda kiberhujumlarning moliyaviy ta‘siri va ularning biznesga zarar yetkazish darajasi ko‘rib chiqilgan<sup>4</sup>.

3. Moliyaviy tashkilotlar kiberxavfsizlikka investitsiyalarni oshirish orqali o‘z xavfsizlik darajalarini yaxshilashga harakat qilmoqdalar. Kiberxavfsizlikka investitsiyalar, o‘z navbatida, moliyaviy barqarorlikni ta‘minlash va mijozlar

<sup>3</sup> Anderson, R., & Moore, T. (2006). The Economics of Information Security.

<sup>4</sup> Ponemon Institute. (2020). Cost of a Data Breach Report.

ishonchini oshirishga yordam beradi. KPMG (2019) o'z hisobotida kiberxavfsizlikka investitsiyalarning moliyaviy tashkilotlar uchun ahamiyatini tahlil qiladi<sup>5</sup>.

4. Kiberxavfsizlik sohasidagi regulatsiyalar va standartlar moliyaviy muomalalarni boshqarishda muhim rol o'ynaydi. Moliyaviy tashkilotlar kiberxavfsizlik standartlariga rioya qilish orqali o'z mijozlarini himoya qilish va qonuniy talablarni bajarishlari zarur. NIST (National Institute of Standards and Technology) va ISO (International Organization for Standardization) kabi tashkilotlar kiberxavfsizlik standartlarini ishlab chiqishda muhim ahamiyatga ega<sup>6</sup>.

5. Kelajak istiqbollari yuzasida kiberxavfsizlikning pul muomalasiga ta'siri kelajakda yanada muhim bo'lishi kutilmoqda. Yangi texnologiyalar, masalan, blockchain va sun'iy intellekt, kiberxavfsizlikni yanada kuchaytirishga yordam berishi mumkin. Shuningdek, kiberxavfsizlikka oid yangi tahdidlar va muammolar paydo bo'lishi mumkin, bu esa moliyaviy tashkilotlarni doimo yangilanib turishga majbur qiladi<sup>7</sup>. Xalqaro ISO tashkilotining kiberxavfsizlik standartlari haqidagi bobida bu borada keng ko'lamli mulohazalar keltirib o'tilgan.

“Kiberxavfsizlikning pul muomalasiga ta'siri” mavzusi moliyaviy tizimlar, kiberhujumlar va xavfsizlik investitsiyalari kabi keng ko'lamli tadqiqotlarni o'z ichiga oladi. Kiberxavfsizlikning kuchayishi moliyaviy tashkilotlar uchun xavfsizlik darajasini oshirish va mijozlar ishonchini saqlab qolish uchun zarurdir.

## **METODOLOGIYA**

Ushbu tadqiqotning maqsadi kiberxavfsizlik borasidagi chora-tadbirlarning joriy etishning iqtisodiy samarasi, moliyaviy operatsiyalardagi zamonaviy iqtisodiy tizimidagi ahamiyatini tahlil qilish, uni yanada rivojlantirish va shakllantirish yo'nalishlarini aniqlashdir. Mavzuni ilmiy o'rganish, statik tahlillar, mantiqiylik, tahlil va tadqiq etish jarayonida turli xil adabiyotlar va maqolalar tahlilidan foydalanilgan.

## **MUHOKAMA VA NATIJALAR**

Moliyaviy operatsiyalar amalga oshish jarayonida kiberxujumlar soni har yili ortib bormoqda. Bu holat moliyaviy tashkilotlar uchun jiddiy xavf tug'dirib, ularning operatsion samaradorligini pasaytiradi. Mijozlar o'z ma'lumotlarining xavfsizligiga ishonch hosil qilmasalar, bu moliyaviy xizmatlardan foydalanishdan voz kechishlariga olib keladi.

Kiberxavfsizlik risklari moliyaviy tashkilotlarga bo'lgan ishonchni pasaytiradi. Mijozlar o'zlarining moliyaviy ma'lumotlarini himoya qilish uchun xavfsiz va ishonchli xizmatlarni tanlashga intilishadi. Natijada, kiberhujumlar natijasida

<sup>5</sup> KPMG. (2019). The Future of Cybersecurity in Financial Services.

<sup>6</sup> NIST. (National Institute of Standards and Technology). Kiberxavfsizlik standartlari.

<sup>7</sup> ISO. (International Organization for Standardization). Kiberxavfsizlik standartlari.

yo'qotilgan ishonch, moliyaviy tashkilotlarning mijozlar sonining kamayishiga olib kelishi mumkin.

Kiberhujumlar moliyaviy tashkilotlarga katta moliyaviy yo'qotishlarga sabab bo'ladi. Tahlil shuni ko'rsatdiki, har bir kiberhujumning o'rtacha moliyaviy zarari millionlab dollarni tashkil etishi mumkin. Bu yo'qotishlar nafaqat tashkilotning o'ziga, balki uning mijozlariga ham ta'sir ko'rsatadi.

Kiberxavfsizlik masalalari investorlar uchun muhim xavf-xatarlarni keltirib chiqaradi. Tahlil natijalari shuni ko'rsatdiki, kiberhujumlar ko'pincha investorlarning moliyaviy bozorlar va tashkilotlarga bo'lgan qiziqishini kamaytiradi. Natijada, investitsiyalarning kamayishi iqtisodiy o'sishni sekinlashtiradi.

Kiberxavfsizlikni mustahkamlash uchun moliyaviy tashkilotlar xavfsizlik tizimlarini yangilash va qo'shimcha resurslar ajratishlari zarur. Tahlil natijalari shuni ko'rsatdiki, kuchli xavfsizlik tizimlari kiberhujumlarning oldini olishda muhim rol o'ynaydi va moliyaviy tashkilotlarning barqarorligini ta'minlaydi.

Moliyaviy operatsiyalarda kiberxavfsizlik risklari iqtisodiyot rivojlanishiga salbiy ta'sir ko'rsatmoqda. Mijozlarning ishonchini saqlab qolish, moliyaviy yo'qotishlarni kamaytirish va investitsiyalarni jalb qilish uchun moliyaviy tashkilotlar kiberxavfsizlikni mustahkamlashga e'tibor qaratishlari zarur. Kiberxavfsizlik masalalariga jiddiy yondashish, barqaror va xavfsiz moliyaviy muhit yaratishda muhim ahamiyatga ega bo'lib, bu iqtisodiy o'sishni ta'minlashga yordam beradi.

Kelajakda moliyaviy tashkilotlar kiberxavfsizlikni yanada kuchaytirish, zamonaviy texnologiyalarni joriy etish va mijozlarga xavfsiz xizmatlar taklif qilish orqali iqtisodiy rivojlanishni qo'llab-quvvatlashlari zarur.

Quyida platformalarga amalga oshirilgan kiberhujumlar statistikasi uchun jadval keltirilgan. Ushbu jadvalda turli platformalarga qilingan kiberhujumlar soni va ularning ta'siri ko'rsatilgan.

### 1-jadval

#### Platformalarga amalga oshirilgan kiberhujumlar statistikasi tahlili<sup>8</sup>

| Platforma nomi                 | Kiberhujumlar soni | Ta'sir darajasi<br>million dollar<br>qiymatida | Mijozlar sonining<br>kamayishi (%)<br>ko'rinishida |
|--------------------------------|--------------------|------------------------------------------------|----------------------------------------------------|
| Banklar                        | 150                | 500                                            | 20                                                 |
| Elektron tijorat<br>saytlar    | 120                | 300                                            | 15                                                 |
| Ijtimoiy tarmoqlar             | 200                | 400                                            | 25                                                 |
| Sog'liqni saqlash<br>tizimlari | 80                 | 250                                            | 10                                                 |
| O'yin platformalari            | 100                | 200                                            | 18                                                 |

<sup>8</sup> <http://cybersecurity.k.li.com>

|                          |     |     |    |
|--------------------------|-----|-----|----|
| Moliyaviy texnologiyalar | 90  | 350 | 15 |
| Kichik bizneslar         | 130 | 100 | 22 |

- Kiberhujumlar soni - har bir platformaga qilingan kiberhujumlar sonini ko'rsatadi jadvalda.

- Ta'sir darajasi - kiberhujumlar natijasida yuzaga kelgan moliyaviy yo'qotishlar.

- Mijozlar sonining kamayishi - kiberhujumlar natijasida platformaning mijozlar sonidagi o'zgarish foizi.

Ushbu jadval kiberhujumlarning turli platformalarga ta'sirini ko'rsatadi va kiberxavfsizlik masalalariga e'tibor qaratish zarurligini ta'kidlaydi. Har bir kiberhujumlar nafaqat dasturiy ta'minotga, balkim moliyaviy zarar ham keltiradi moliyaviy institutlar uchun.

*Kelajakdagi tendensiyalar va rivojlanishlar.* Rivojlanayotgan tahdidlar va ojiz taraflari: Texnologiya rivojlanishi davom etar ekan, yangi tahdidlar paydo bo'lishi mumkin buni fanda Advanced Persistent Threats (APT) deb ataladi, raqamli hisoblash va murakkab ijtimoiy muhandislik texnikasi moliyaviy institutlar ogoh bo'lishi hamda shay turishi kerak bo'lgan potensial xavflardan biridir. APTlar uzoq vaqt davomida maxfiy ma'lumotlarni o'g'irlashni maqsad qilgan kuchli manbalarga ega bo'lgan kiber jinoyatchilarning hujumlariga qaratilgan bo'lib, Kvant hisoblash joriy shifrlash algoritmlarini buzib kiradi va ularni yangi usullarda ishlab chiqishni talab qiladi. Ijtimoiy kiberhujumlari tobora murakkablashib bormoqda, kiberjinoyatchilar maxfiy ma'lumotlarni oshkor qilish uchun shaxslarni aldash uchun psixologik manipulyatsiyadan foydalanadilar.

Moliyaviy institutlar o'zlarining xavfsizlik strategiyalarini doimiy ravishda yangilab, ilg'or tahdidlarni aniqlash va javob berish imkoniyatlariga sarmoya kiritib, ushbu paydo bo'layotgan tahdidlardan ogoh bo'lishlari kerak. Bu moliyaviy institutlar uchun nafaqat zarurat, balkim iqtisodiy barqarorlikni ta'minlashlari uchun ham asos bo'lib xizmat qiladi.

Sun'iy intellekt (AI) va Machine Learning (ML) sohasidagi yutuqlar moliyaviy operatsiyalar uchun kiberxavfsizlikni samarali qilishga tayyor<sup>9</sup>. SI va ML algoritmi real vaqtda katta hajmdagi ma'lumotlarni tahlil qilishi, shifrlarni aniqlashi, potensial tahdidlarni aniqlashi va xavflarni kamaytirish uchun javoblarni avtomatlashtirishi mumkin<sup>10</sup>. SI tomonidan boshqariladigan tizimlar tranzaksiya shakllaridagi xavflarni aniqlay oladi, bu firibgarlik faoliyatini aniqlashi va topishi mumkun, bu esa tezkor integratsiyalashuvga imkon beradi. Raqamli hisoblashlar keltirib chiqaradigan

<sup>9</sup> Mandru S. Journal of Scientific and Engineering Research, 2018, 5

<sup>10</sup>[https://www.researchgate.net/publication/388649175\\_The\\_Role\\_of\\_Cybersecurity\\_in\\_Protecting\\_Financial\\_Transactions](https://www.researchgate.net/publication/388649175_The_Role_of_Cybersecurity_in_Protecting_Financial_Transactions)

potentsial tahdidlarni bartaraf etish uchun mo'ljallangan kvantga chidamli shifrlash algoritmlari ham mavjud. Ushbu algoritmlar kvant quvvatli hujumlar oldida ham samarali bo'lib qoladigan xavfsiz shifrlashni ta'minlashga qaratilgan. Growth-Quantum Research kriptografiyasi shifrlangan moliyaning uzoq muddatli xavfsizligini ta'minlash uchun zarurdir.

Moliyaviy operatsiyalarda kiberxavfsizlikning istiqboli sifatida moliyaviy institutlar, tartibga soluvchilar va kiberxavfsizlik bo'yicha mutaxassislar o'rtasidagi hamkorlikni kuchaytirishni o'z ichiga oladi. Axborot almashishni yaxshilash va birgalikda rivojlantirish sa'y-harakatlari va ilg'or xavfsizlik choralari amalga oshirish o'zgaruvchan tahdidlardan himoyalaniş uchun juda muhim bo'ladi. Moliyaviy institutlar potentsial hujumlarni oldindan ko'rish va pragnoz qilish, oldini olish uchun tahdidlar bo'yicha razvedka va tahlillarga e'tibor qaratib, kiberxavfsizlikka nisbatan jiddiy ko'lamda yondashishi, blokcheyn texnologiyasi va sun'iy intellektga asoslangan yechimlarni integratsiya qilish orqali moliyaviy kiberxavfsizlikning kelajakda tug'dirishi mumkun bo'lgan xavflaridan himoyalanişda muhim rol o'ynaydi. Blockchain - bu moliyaviy operatsiyalarda xavfsizlik va shaffoflikni yaxshilash uchun ma'lumot va imkoniyatlarni taklif qiluvchi munosib hisoblangan ilg'or tahliliy qobiliyatlari. Ushbu texnologiyalardan samarali foydalanadigan yoki paydo bo'ladigan tahdidlarga javob berish va o'z tizimlarini himoya qilish uchun yaxshiroq pozitsiyaga ega bo'lgan moliyaviy institutlar uchun juda samarali bo'lishi mumkun.

## **XULOSA**

Kiberxavfsizlik moliyaviy ma'lumotlarning xavfsiz va shaffofligini ta'minlash orqali moliyaviy operatsiyalarni himoya qilishda muhim rol o'ynaydi. Ushbu maqolada moliyaviy operatsiyalar uchun turli tahdidlarni o'rganib chiqib, joriy xavfsizlik choralari va texnologiyalarini ko'rib chiqish zaruratini va ushbu sohadagi moliyaviy operatsiyalarning muammolari va kelajagini muhokama qilindi. Moliyaviy institutlar kuchli kiberxavfsizlik strategiyasiga sarmoya kiritishda davom etishlari va rivojlanayotgan tahdidlardan himoyalanişlari kerak.

Moliyaviy pul munosabatlari raqamli platformalarda tobora ortib borar ekan, institutlar yangi tahdidlar va texnologik yutuqlarga doimiy ravishda moslashib, kiberxavfsizlikka hushyor va sha'y bo'lishlari kerak. Kelajakdagi tadqiqotlar aniqlangan kamchiliklarni bartaraf etishga va moliyaviy operatsiyalar xavfsizligini oshirish, moliyaviy tizimlarning o'zgarishlarga chidamliligi va xavfsizligini ta'minlash uchun innovatsion yechimlarni o'rganishga qaratilishi kerak. Iqtisodiy barqarorlikni ta'minlashlikni maqsad qilgan har bir moliya institutlari uchun bu juda muhim hisoblanadi.

## FOYDALANILGAN ADABIYOTLAR RO‘YXATI

1. <https://onesecc.uz/uz/news/show/4>
2. <https://yuz.uz/uz/news/kiberxavfsizlik-qonun-bilan-tartibga-solindi>
3. <https://cybersecurity.k.li.com>
4. Anderson, R., & Moore, T. (2006). The Economics of Information Security.
5. Ponemon Institute. (2020). Cost of a Data Breach Report.
6. KPMG. (2019). The Future of Cybersecurity in Financial Services.
7. NIST. (National Institute of Standards and Technology). Kiberxavfsizlik standartlari.
8. ISO. (International Organization for Standardization). Kiberxavfsizlik standartlari.
9. Mandru S. Journal of Scientific and Engineering Research, 2018, 5.
10. [https://www.researchgate.net/publication/388649175\\_The\\_Role\\_of\\_Cybersecurity\\_in\\_Protecting\\_Financial\\_Transactions](https://www.researchgate.net/publication/388649175_The_Role_of_Cybersecurity_in_Protecting_Financial_Transactions).