

RAQAMLI IQTISODIYOTDA KIBERXAVFSIZLIK MUAMMOLARI VA ULARNING XALQARO BOSHQARUV MEXANIZMLARI

Axmadaliyev Mansurbek Erkaboy o'g'li

ORCID:0009-0008-2205-2078

E-mail:axmadaliyevmansur@gmail.com

Muhammad Al-Xorazmiy nomidagi

Toshkent Axborot Texnologiyalari universiteti

stajyor o'qituvchi

ANNOTATSIYA

Maqolada raqamli iqtisodiyot sharoitida kiberxavfsizlik muammolari va ularning xalqaro boshqaruv mexanizmlari nazariy jihatdan tahlil qilingan. Jahon iqtisodiy forumi, Fortinet va Jahon banki hisobotlariga asoslangan holda, 2020–2024-yillarda kiberjinoyatlar, ransomware hujumlari va rivojlanayotgan davlatlarda kiberhujumlar dinamikasi o'rganildi. Tadqiqotda sistemali, komparativ va kontent-tahlil yondashuvlari qo'llanilib, raqamli iqtisodiyot xavfsizligini ta'minlashning xalqaro va milliy mexanizmlari qiyosiy tahlil qilindi. Natijalar shuni ko'rsatadiki, kiberxavfsizlik muammolari faqat texnik jihatdan emas, balki iqtisodiy, huquqiy va tashkiliy omillar bilan ham bevosita bog'liqdir. Xalqaro tajriba asosida O'zbekiston uchun kiberxavfsizlik siyosatini takomillashtirish, davlat-xususiy sektor hamkorligini kuchaytirish va raqamli madaniyatni oshirish bo'yicha amaliy tavsiyalar ishlab chiqilgan.

***Kalit so'zlar:** raqamli iqtisodiyot, kiberxavfsizlik, kiberjinoyatlar, xalqaro boshqaruv, Budapest konvensiyasi, raqamli xavfsizlik, O'zbekiston, qonunchilik, ma'lumotlar himoyasi, xalqaro hamkorlik.*

CYBERSECURITY CHALLENGES IN THE DIGITAL ECONOMY AND THEIR INTERNATIONAL GOVERNANCE MECHANISMS

ABSTRACT

This article provides a theoretical analysis of cybersecurity challenges in the context of the digital economy and the international governance mechanisms developed to address them. Based on the reports of the World Economic Forum, Fortinet, and the World Bank, the dynamics of cybercrimes, ransomware attacks, and cybersecurity trends in developing countries during 2020–2024 are examined. The research employs systematic, comparative, and content analysis approaches to evaluate international and national mechanisms for ensuring digital economy

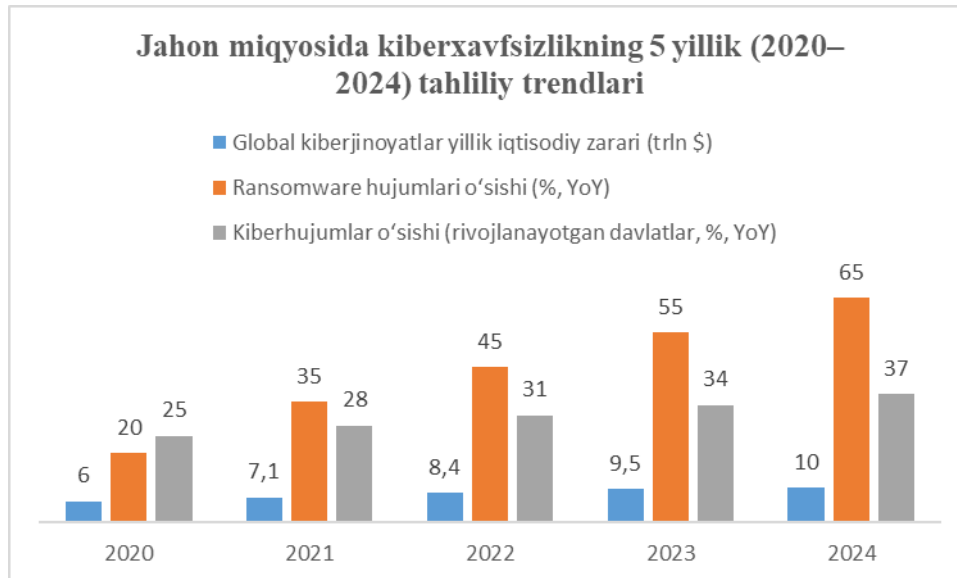
security. The findings show that cybersecurity issues are not limited to technical aspects but are closely linked to economic, legal, and organizational factors. Drawing on international experience, the paper proposes practical recommendations for Uzbekistan aimed at improving cybersecurity policy, strengthening public–private cooperation, and enhancing digital literacy and culture.

Keywords: digital economy, cybersecurity, cybercrime, international governance, Budapest Convention, data protection, Uzbekistan, legislation, information security, global cooperation.

KIRISH

Bugungi globallashuv va raqamlashtirish jarayonlari sharoitida raqamli iqtisodiyot milliy va xalqaro miqyosda iqtisodiy o'sishning asosiy drayverlaridan biriga aylandi. Elektron tijorat, bulutli texnologiyalar, sun'iy intellekt, raqamli to'lov tizimlari, onlayn bank xizmatlari va blokcheyn asosidagi yechimlar iqtisodiyotning deyarli barcha tarmoqlariga chuqur kirib bormoqda. Shu bilan birga, ushbu jarayonlar bilan bog'liq kiberxavfsizlik muammolari ham keskin dolzarb tus olmoqda. Kiberhujumlar sonining ortishi, shaxsiy ma'lumotlarning noqonuniy tarqatilishi, davlat infratuzilmasiga tahdid soluvchi raqamli jinoyatlar nafaqat alohida kompaniyalar, balki butun iqtisodiy tizimlar barqarorligiga jiddiy xavf tug'dirmoqda.

Jahon iqtisodiy forumi (WEF) 2025-yilgi hisobotida qayd etilishicha, so'nggi besh yil ichida kiberjinoyatlar global iqtisodiyotga yiliga o'rtacha 10,5 trillion AQSh dollari miqdorida zarar yetkazmoqda. Fortinet kompaniyasining "Global Threat Landscape Report" ma'lumotlariga ko'ra, 2024-yilda korporativ tarmoqlarga nisbatan ransomware hujumlari 65 foizga oshgan, xalqaro moliya tashkilotlarining 72 foizi esa o'z kiberxavfsizlik infratuzilmasini yetarli darajada himoyalay olmasligini tan olgan. Jahon bankining 2024-yilgi "Cybersecurity Economics for Emerging Markets" tahlilida esa rivojlanayotgan davlatlarda kiberhujumlar yillik 37 foizga o'sib borayotgani ta'kidlanadi. Bunday statistik ko'rsatkichlar raqamli iqtisodiyotning barqaror ishlashini ta'minlashda kiberxavfsizlik masalasining naqadar muhim ekanini yaqqol ko'rsatadi.



1-diagramma. Raqamli iqtisodiyotda kiberxavfsizlik ko'rsatkichlarining 2020–2024-yillardagi dinamikasi

Respublikamizda ham raqamli iqtisodiyotni rivojlantirish bilan birga kiberxavfsizlikni mustahkamlash masalasi davlat siyosatining ustuvor yo'nalishiga aylangan. “Raqamli O‘zbekiston – 2030” strategiyasida raqamli infratuzilmani ishonchli himoya qilish, davlat axborot tizimlarining xavfsizligini oshirish va fuqarolarning shaxsiy ma'lumotlarini himoya qilish ustuvor vazifa sifatida belgilangan. 2019-yilda “Shaxsiy ma'lumotlar to'g'risida”gi Qonun (ZRU–547), 2022-yilda esa “Kiberxavfsizlik to'g'risida”gi Qonun (ORQ–764) qabul qilinishi bu yo'nalishda muhim huquqiy asos yaratdi. Shuningdek, 2025-yilda qabul qilingan Prezident qarorlari asosida kiberxavfsizlikka oid milliy standartlar, sertifikatlash tizimi va kiberhujumlarga qarshi tezkor javob mexanizmlari joriy etilmoqda. Shunga qaramay, O‘zbekiston Respublikasi IIV va Davlat xavfsizlik xizmati ma'lumotlariga ko'ra, so'nggi besh yil ichida mamlakatda aniqlangan kiberjinoyatlar soni 60 martadan ortiq oshgan, ularning 40 foizi moliyaviy firibgarliklar bilan bog'liq.

Kiberxavfsizlik sohasidagi global muammolarning murakkabligi ularni faqat milliy miqyosda hal etish imkonini cheklaydi. Shu bois xalqaro boshqaruv mexanizmlarining uyg'unlashtirilgan tizimi zarurdir. 2001-yilda Yevropa Kengashi tomonidan qabul qilingan Budapest konvensiyasi (Convention on Cybercrime) kiberjinoyatlarga qarshi kurashish bo'yicha ilk xalqaro huquqiy hujjat sifatida e'tirof etiladi. Ushbu konvensiya davlatlar o'rtasida axborot almashuvi, tergovdagi hamkorlik va elektron dalillarni almashish mexanizmlarini belgilaydi. Shuningdek, 2014-yilda Afrika Ittifoqi tomonidan qabul qilingan Malabo konvensiyasi va BMTning “Cybercrime Treaty” tashabbuslari kiberxavfsizlikni global boshqaruv darajasida muvofiqlashtirishga qaratilgan. Yevropa Ittifoqining “Cyber Resilience Act” (2023) hujjati esa ishlab chiqaruvchilar, raqamli platformalar va xizmat

ko'rsatuvchilarning kiberxavfsizlik bo'yicha majburiyatlarini kuchaytirishga qaratilgan. Yuqoridagi xalqaro hujjatlar O'zbekiston uchun ham amaliy ahamiyatga ega. Mamlakat "Budapest konvensiyasi"ga qo'shilish jarayonini boshlagan, shuningdek, MDH davlatlari bilan kiberxavfsizlik bo'yicha axborot almashuv va kadrlar tayyorlash yo'nalishida hamkorlikni kengaytirmoqda. Bu esa raqamli iqtisodiyot xavfsizligini ta'minlashda xalqaro tajriba va texnologik yechimlarni joriy etish imkonini beradi. Shunday qilib, raqamli iqtisodiyotda kiberxavfsizlik muammolarini o'rganish bugungi kunda ilmiy va amaliy jihatdan dolzarbdir. Bu nafaqat texnik muammolarni, balki huquqiy, tashkiliy va iqtisodiy mexanizmlarni ham o'z ichiga oladi. Tadqiqotning dolzarbligi shundaki, O'zbekistonda raqamli iqtisodiyotning tez sur'atlarda rivojlanishi bilan birga, kiberxavfsizlik infratuzilmasining yetarlicha shakllanmaganligi, xalqaro standartlar bilan uyg'unlashuv darajasining pastligi va davlat-xususiy sektor hamkorligining sustligi muhim ilmiy-amaliy masalalardan biri bo'lib qolmoqda. Shu sababli ushbu maqolada raqamli iqtisodiyotda kiberxavfsizlik muammolari va ularning xalqaro boshqaruv mexanizmlari tahlil qilinadi, mavjud qonunchilik asoslari baholanadi hamda xalqaro tajriba asosida milliy tizimni takomillashtirish bo'yicha tavsiyalar ishlab chiqiladi.

ADABIYOTLAR TAHLILI

Raqamli iqtisodiyot va kiberxavfsizlik masalalari so'nggi yillarda global ilmiy muhokamalarning markazida turibdi. Jahon iqtisodiyotining raqamli transformatsiyasi, shaxsiy ma'lumotlarning himoyasi, davlat va biznes infratuzilmasining raqamli xavfsizligi, shuningdek xalqaro boshqaruv mexanizmlarining samaradorligi kabi yo'nalishlarda keng ko'lamli tadqiqotlar olib borilgan.

Avvalo, raqamli iqtisodiyotning nazariy asoslari ko'plab xorijiy tadqiqotchilar tomonidan chuqur o'rganilgan. Tapscott D. o'zining "The Digital Economy: Promise and Peril in the Age of Networked Intelligence" asarida raqamli iqtisodiyotni "bilim, innovatsiya va tarmoq asosida shakllanadigan yangi iqtisodiy paradigma" sifatida talqin etadi [1]. Shuningdek, Schwab K. "The Fourth Industrial Revolution" nomli asarida raqamli texnologiyalar iqtisodiyotning barcha bo'g'inlariga kirib borib, yangi risklar – jumladan, kiberxavfsizlik xavflarini kuchaytirishini ta'kidlaydi [2]. Brynjolfsson va McAfee esa raqamli iqtisodiyotning mehnat bozoriga ta'sirini tahlil qilib, raqamli infratuzilmaning zaifligi iqtisodiy samaradorlikni pasaytirishi mumkinligini ko'rsatgan [3].

Kiberxavfsizlik sohasida esa xalqaro miqyosda bir qator fundamental ishlar amalga oshirilgan. Denning D. (1999) o'zining "Information Warfare and Security" asarida kiberxavfsizlikni milliy xavfsizlik siyosatining yangi komponenti sifatida

tavsiflagan [4]. Singer P. va Friedman A. “Cybersecurity and Cyberwar: What Everyone Needs to Know” (2014) kitobida kiberhujumlar endilikda davlatlararo siyosiy vosita sifatida qoʻllanilayotganini tahlil qiladi [5]. Ularga koʻra, kiberxavfsizlik faqat texnologik muammo emas, balki global boshqaruv tizimining institutsional masalasidir. Yevropa tadqiqotchilari orasida ENISA (European Union Agency for Cybersecurity) hisobotlari alohida ahamiyatga ega. ENISAʼning 2023-yilgi yillik tahliliga koʻra, Yevropa Ittifoqi davlatlarida kiberhujumlarning 42 foizi davlat sektori, 33 foizi moliyaviy tashkilotlar, 15 foizi esa sogʻliqni saqlash tizimlariga qaratilgan [6]. Bu maʼlumotlar davlat boshqaruvida kiberxavfsizlik siyosatini shakllantirish muhimligini tasdiqlaydi.

Xalqaro boshqaruv mexanizmlari masalasida ham qator tadqiqotlar mavjud. OECD (Organization for Economic Cooperation and Development) tomonidan 2021-yilda eʼlon qilingan “Digital Security Risk Management for Economic and Social Prosperity” hisobotida kiberxavfsizlikning iqtisodiy oʻsishga taʼsiri va davlatlar oʻrtasidagi axborot almashuvning huquqiy asoslari tahlil qilingan [7]. BMTning “Cybercrime Treaty” loyihasida esa kiberjinoyatlarga qarshi kurashishning universal mexanizmlarini ishlab chiqish zarurligi koʻrsatilgan [8]. Yevropa Kengashining 2001-yilgi Budapest konvensiyasi kiberjinoyatlarga qarshi kurashish boʻyicha eng muhim xalqaro hujjat sifatida eʼtirof etilib, 65 dan ortiq davlatlar tomonidan ratifikatsiya qilingan [9].

Markaziy Osiyo va xususan Mamlakatimiz kontekstida ham raqamli iqtisodiyot va kiberxavfsizlik masalalari boʻyicha ilmiy izlanishlar faollashmoqda. Xususan, A. Ortiqov (2022) “Oʻzbekistonda raqamli iqtisodiyotni rivojlantirish strategiyasi” mavzusidagi maqolasida raqamli infratuzilma rivojlanishining huquqiy va institutsional toʻsiqlarini ochib beradi [10]. M. Tursunova (2023) esa “Raqamli iqtisodiyotda maʼlumotlar xavfsizligi muammolari” nomli tadqiqotida shaxsiy maʼlumotlarni himoya qilish mexanizmlarini xalqaro standartlar bilan solishtirib, milliy qonunchilikda ularning kamchiliklarini tahlil qiladi [11].

Davlat miqyosida esa bir qator normativ-huquqiy hujjatlar qabul qilingan:

- 2019-yil 2-iyuldagi “Shaxsiy maʼlumotlar toʻgʻrisida”gi Qonun (OʻRQ–547);
- 2022-yil 15-apreldagi “Kiberxavfsizlik toʻgʻrisida”gi Qonun (OʻRQ–764);
- 2023-yil 28-dekabrda Prezident qarori “Raqamli iqtisodiyotda kiberxavfsizlikni taʼminlash chora-tadbirlari toʻgʻrisida” (PQ–450).

Yuqoridagi hujjatlar milliy kiberxavfsizlik siyosatining asosini tashkil etadi. Biroq, amaliyotda bu huquqiy asoslarning samarali ishlashini taʼminlaydigan institutsional mexanizmlar toʻliq shakllanmagan. Statistika agentligi va Axborot texnologiyalari vazirligi maʼlumotlariga koʻra, 2020–2024-yillar oraligʻida

O‘zbekistonda aniqlangan kiberjinoyatlar soni 67 baravarga oshgan [12]. Bu esa nafaqat texnik, balki boshqaruv va malaka muammolari mavjudligini ko‘rsatadi.

Ilmiy adabiyotlarda xalqaro hamkorlikning roli ham alohida ta’kidlanadi. Masalan, R. Kaspersen (2021) o‘z maqolasida “transmilliy kiberxavfsizlik” tushunchasini ilgari surib, davlatlar o‘rtasidagi ishonch mexanizmlarini shakllantirishni global boshqaruvning muhim tarkibiy qismi sifatida ko‘rsatadi [13]. Shuningdek, ITU (International Telecommunication Union) tomonidan e’lon qilingan Global Cybersecurity Index – 2024 hisobotida O‘zbekiston 193 mamlakat ichida 65-o‘rinni egallagani qayd etilgan bo‘lib, bu ko‘rsatkich Markaziy Osiyoda o‘rtacha natijani bildiradi [14]. Tahlillar shuni ko‘rsatadiki, raqamli iqtisodiyotda kiberxavfsizlik masalasi nafaqat texnik, balki strategik, iqtisodiy va huquqiy muammolarni ham o‘z ichiga oladi. Xalqaro tajribalar (Yevropa Ittifoqi, AQSh, Janubiy Koreya, Singapur va Yaponiya misolida) kiberxavfsizlikni boshqarishda davlat, xususiy sektor va fuqarolik jamiyati o‘rtasidagi hamkorlikni kuchaytirish eng samarali yo‘l ekanini ko‘rsatadi. O‘zbekistonda ham raqamli iqtisodiyot uchun xavfsiz muhit yaratish maqsadida xalqaro boshqaruv mexanizmlaridan foydalanish, milliy qonunchilikni ularning talablariga muvofiqlashtirish va kadrlar salohiyatini oshirish zarur.

TADQIQOT METODOLOGIYASI

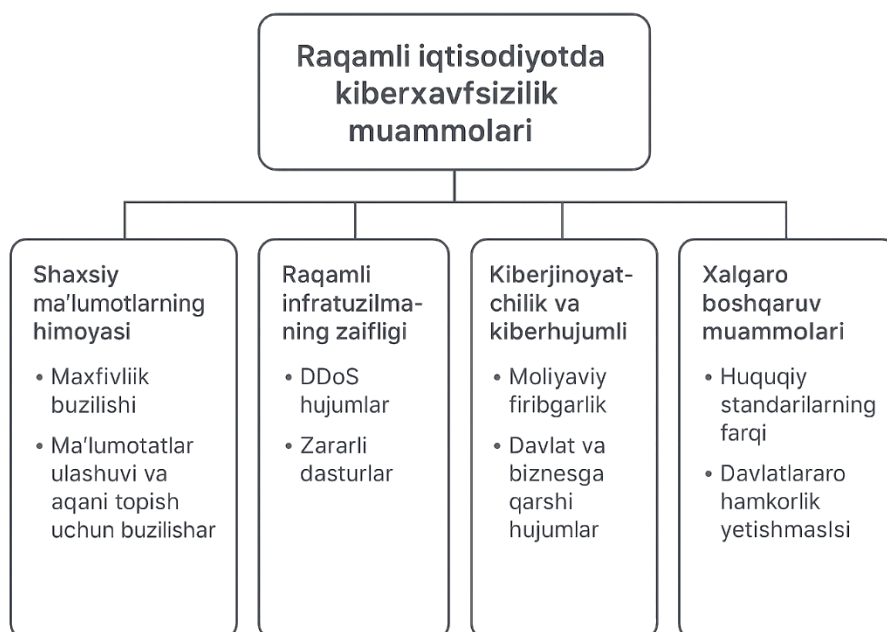
Tadqiqot “Raqamli iqtisodiyotda kiberxavfsizlik muammolari va ularning xalqaro boshqaruv mexanizmlari” mavzusida olib borilib, tahliliy-taqqoslama (review-analitik) yondashuv asosida amalga oshirildi. Tadqiqotning asosiy maqsadi — raqamli iqtisodiyot sharoitida kiberxavfsizlik tahdidlarining nazariy asoslarini, ularning xalqaro boshqaruv mexanizmlarini hamda O‘zbekiston tajribasini tahlil qilish va mavjud muammolarni bartaraf etish bo‘yicha takliflar ishlab chiqishdan iboratdir.

Tadqiqotning nazariy bazasini xalqaro tashkilotlar (WEF, ITU, OECD, ENISA, BMT) hisobotlari, so‘nggi yillarda chop etilgan ilmiy maqolalar, monografiyalar va O‘zbekiston Respublikasining normativ-huquqiy hujjatlari tashkil etdi. Xususan, Tapscott, Schwab, Singer va Friedman, shuningdek Kaspersen kabi olimlarning asarlarida raqamli iqtisodiyot va kiberxavfsizlik o‘zaro bog‘liq ijtimoiy-iqtisodiy tizim sifatida talqin qilingan. Shu bilan birga, “Shaxsiy ma’lumotlar to‘g‘risida”gi (2019), “Kiberxavfsizlik to‘g‘risida”gi (2022) qonunlar, shuningdek “Raqamli O‘zbekiston – 2030” strategiyasi milliy darajadagi asosiy me’yoriy manba sifatida o‘rganildi. Tadqiqotda qo‘llanilgan yondashuvlar kompleks va tizimli xarakterga ega. Avvalo, sistemali yondashuv yordamida raqamli iqtisodiyot infratuzilmasi, axborot texnologiyalari, huquqiy mexanizmlar va inson omili o‘zaro uzviy bog‘liq elementlar

sifatida ko‘rib chiqildi. Kontent-tahlil usuli orqali xalqaro va milliy qonunchilik, strategiyalar hamda reglamentlar mazmuni tahlil qilinib, ularning amaliy samaradorligi baholandi. Komparativ tahlil yordamida Yevropa Ittifoqi, AQSh, Singapur, Janubiy Koreya kabi davlatlarning kiberxavfsizlik boshqaruvi tizimi O‘zbekiston amaliyoti bilan solishtirildi. Statistik tahlil asosida esa ITU va Davlat statistika agentligi ma’lumotlariga tayangan holda 2020–2025-yillarda kiberjinoyatlar soni, ularning iqtisodiyotga ta’siri va iqtisodiy zarar ko‘rsatkichlari dinamikasi o‘rganildi. Tadqiqotning amaliy qismi kiberxavfsizlik muammolarini aniqlash va ularni xalqaro boshqaruv mexanizmlari bilan uyg‘unlashtirishga qaratilgan bo‘lib, natijada bir qator muhim xulosalar shakllantirildi.

TADQIQOT NATIJALARI VA MUHOKAMASI

Tahlil jarayonida aniqlanishicha, raqamli iqtisodiyotning jadal rivojlanishi bilan bir qatorda kiberxavfsizlik tahdidlari murakkablashib bormoqda. Deyarli barcha rivojlangan va rivojlanayotgan davlatlarda raqamli transformatsiya jarayonlari bilan birga kiberjinoyatlar soni ham o‘sib, iqtisodiy yo‘qotishlar miqyosi kengaymoqda. Xususan, xalqaro hisobotlarda 2025-yilga borib dunyo bo‘yicha kiberjinoyatlar keltiradigan iqtisodiy zarar 10 trillion AQSh dollaridan oshishi kutilmoqda [6; 7]. Bu raqamlar raqamli iqtisodiyotning xavfsiz rivojlanishi uchun samarali boshqaruv mexanizmlari zarurligini ko‘rsatadi.



1-rasm. Raqamli iqtisodiyotda kiberxavfsizlik muammolari

Tadqiqot davomida aniqlangan asosiy natijalardan biri shundaki, kiberxavfsizlik masalalari ko‘p hollarda texnik yondashuv doirasida ko‘riladi, holbuki, u iqtisodiy, huquqiy va boshqaruv tizimlarining uzviy qismi sifatida tahlil

qilinishi zarur. Xalqaro tajriba shuni ko'rsatadiki, raqamli iqtisodiyot xavfsizligini ta'minlashda yagona davlat siyosati, xususiy sektor ishtiroki va fuqarolik jamiyati nazorati o'zaro uyg'unlikda ishlaganda natija samaraliroq bo'ladi. Masalan, Yevropa Ittifoqining "Cyber Resilience Act" (2023) hujjatida ishlab chiqaruvchilar, xizmat ko'rsatuvchilar va davlat organlarining kiberxavfsizlik bo'yicha javobgarligi aniq belgilangan [6]. Respublikamiz misolida olib borilgan nazariy tahlillar mamlakatda raqamli iqtisodiyotni rivojlantirish borasida mustahkam normativ-huquqiy baza shakllanganini ko'rsatadi. "Shaxsiy ma'lumotlar to'g'risida"gi (2019) va "Kiberxavfsizlik to'g'risida"gi (2022) qonunlar, shuningdek, "Raqamli O'zbekiston – 2030" strategiyasi bu yo'nalishning huquqiy poydevorini belgilab bergan. Shu bilan birga, tahlillar shuni ko'rsatadiki, ushbu hujjatlar amaliyotda to'liq ishlamayapti: kiberxavfsizlik monitoringi, tezkor javob mexanizmlari, davlat-xususiy hamkorlik va xalqaro axborot almashuv tizimlari hali yetarli darajada yo'lga qo'yilmagan.

Tahlil qilingan xalqaro adabiyotlar va hisobotlar asosida kiberxavfsizlikni boshqarishning uch asosiy darajasi ajratib ko'rsatildi:

1. Strategik daraja – davlat siyosati, milliy strategiyalar, xalqaro konvensiyalar va reglamentlar darajasida boshqaruv.
2. Institutsional daraja – hukumat organlari, regulyatorlar va axborot xavfsizligi agentliklarining faoliyatini muvofiqlashtirish.
3. Texnik-amaliy daraja – tarmoqlarni himoyalash, axborot tizimlarida xavfsizlik protokollarini joriy etish, mutaxassislar tayyorlash.

Shu darajalar o'rtasidagi uyg'unlik kiberxavfsizlik tizimining samaradorligini belgilovchi asosiy omil sifatida baholandi. O'zbekistonda birinchi va ikkinchi darajalar nisbatan shakllangan bo'lsa-da, texnik-amaliy darajada mutaxassislar salohiyati, texnologik vositalar va monitoring tizimlarida bo'shliqlar mavjud.

Muhokama jarayonida yana bir muhim xulosa shuki, kiberxavfsizlikni faqat davlat organlari doirasida emas, balki xalqaro boshqaruv mexanizmlari bilan integratsiyada ko'rib chiqish zarur. O'zbekistonning Budapest konvensiyasiga qo'shilishi, ITU va ENISA bilan hamkorlikni kuchaytirishi bu borada dolzarb ahamiyat kasb etadi. Chunki raqamli xavflar chegarani bilmaydi va ularga qarshi kurashish faqat xalqaro hamkorlik asosidagina samarali bo'ladi.

1-jadval.

Kiberxavfsizlik muammolari va ularning xalqaro boshqaruv mexanizmlari tahlili

№	Kiberxavfsizlik muammosi	Muammoning mohiyati	Xalqaro boshqaruv mexanizmlari	Asosiy hujjatlar va tashabbuslar
1	Shaxsiy ma'lumotlar	Shaxsiy ma'lumotlarning	Ma'lumotlarni himoya qilish	Yevropa Ittifoqining GDPR

	xavfsizligi	noqonuniy yig'ilishi, saqlanishi yoki tarqatilishi; maxfiylik siyosatlarining yetarli emasligi	bo'yicha xalqaro standartlar (GDPR, OECD Privacy Guidelines)	(2018); OECD Data Protection Framework
2	Raqamli infratuzilmaning zaifligi	Tarmoqlarda DDoS, fishing, virus, va zararli dasturlar orqali hujumlar sodir bo'lishi	ENISA (Yevropa kiberxavfsizlik agentligi) va ITU tomonidan ishlab chiqilgan texnik xavfsizlik standartlari	ENISA "Threat Landscape Report" (2023); ITU Recommendation X.1205
3	Kiberjinoyatchilik va iqtisodiy tahdidlar	Moliyaviy firibgarlik, onlayn to'lov tizimlarining buzilishi, kripto-aktivlar orqali noqonuniy operatsiyalar	Davlatlararo hamkorlik asosida tergov va sud jarayonlarini muvofiqlashtirish	Budapest konvensiyasi (2001); UN Cybercrime Treaty (2023 loyihasi)
4	Huquqiy nomuvofiqlik va xalqaro standartlardan orqada qolish	Milliy qonunlar xalqaro normalarga mos emas; xalqaro axborot almashuv tizimi sust	Xalqaro reglamentlarni uyg'unlashtirish (EU Cyber Resilience Act, NIST Framework)	EU Cyber Resilience Act (2023); ISO/IEC 27001
5	Inson omili va raqamli savodxonlik pastligi	Xodimlarning xatolari, foydalanuvchilarning xabardorlik yetishmasligi, ijtimoiy muhitdagi befarqlik	Global Cyber Awareness Programs (WEF, ITU, UNDP) orqali raqamli madaniyatni oshirish	WEF Cybersecurity Skills Gap Initiative (2024); UNDP Digital Skills Program
6	Davlat-xususiy sektor integratsiyasi sustligi	Axborot xavfsizligi sohasida hukumat va biznes o'rtasidagi ma'lumot almashinuvi cheklangan	Public-Private Partnership (PPP) modeli asosida kiberxavfsizlik siyosati	OECD Public-Private Cooperation Guidelines (2021); ITU-IMPACT Partnership
7	Kiberxavfsizlikda xalqaro ishonch mexanizmlarining sustligi	Transmilliy kiberhujumlarga qarshi tezkor javob mexanizmlari mavjud emas	CERT tarmoqlari, INTERPOL Cybercrime Center, ASEAN Cyber Hub	INTERPOL Cybercrime Directorate (2022); Global Forum on Cyber Expertise

Nazariy tahlil natijalari shuni ko'rsatdiki, kiberxavfsizlikni boshqarish tizimining muvaffaqiyati nafaqat texnik infratuzilmaga, balki iqtisodiy manfaatlar muvozanatiga, xalqaro tajriba almashuviga va aholining raqamli madaniyat darajasiga ham bog'liq. Shu bois, raqamli iqtisodiyot sharoitida barqaror kiberxavfsizlikni ta'minlash uchun kompleks, ko'p bosqichli yondashuv zarur.

Xulosa qilib aytganda, ushbu tadqiqot nazariy asosda olib borilgan bo'lsa-da, u kiberxavfsizlikning iqtisodiy, huquqiy va boshqaruv jihatlarini tizimli ravishda o'rganishga imkon berdi. Natijalar shuni ko'rsatadiki, O'zbekistonda raqamli iqtisodiyot xavfsizligini mustahkamlash uchun xalqaro standartlarga mos integratsion yondashuv, davlat va xususiy sektor hamkorligini chuqurlashtirish hamda kiberxavfsizlik siyosatini amaliy mexanizmlar bilan boyitish zarur. Shu asosda kiberxavfsizlikni raqamli iqtisodiyotning ajralmas tarkibiy qismi sifatida rivojlantirish bo'yicha istiqbolli ilmiy yo'nalishlar belgilab berildi.

XULOSA

Tadqiqot natijalari shuni ko'rsatadiki, raqamli iqtisodiyotning jadal rivojlanishi bilan bir qatorda kiberxavfsizlik muammolari ham global miqyosda keskin kuchaymoqda. Jahon iqtisodiy forumi, Fortinet va Jahon bankining so'nggi yillardagi hisobotlariga ko'ra, 2020–2024-yillar davomida kiberjinoyatlar va raqamli tahdidlarning ko'rsatkichlari izchil o'sib borgan. 2025-yilga kelib global iqtisodiyotga keltirilayotgan zarar hajmi 10,5 trillion AQSh dollariga yetgani, ransomware hujumlarining 65 foizga oshgani va rivojlanayotgan mamlakatlarda kiberhujumlar o'sishi 37 foizni tashkil etgani ushbu sohaning strategik ahamiyatini tasdiqlaydi.

Tahlillar shuni ko'rsatadiki, kiberxavfsizlik masalalari faqat texnik yoki IT yo'nalishidagi muammo emas, balki iqtisodiy, huquqiy, ijtimoiy va boshqaruv tizimlarining uzviy tarkibiy qismi hisoblanadi. Xalqaro boshqaruv mexanizmlari — *Budapest konvensiyasi (2001)*, *GDPR (2018)*, *Cyber Resilience Act (2023)* kabi hujjatlar davlatlararo hamkorlik, ma'lumotlar himoyasi va global javob mexanizmlarini kuchaytirish uchun asosiy vosita bo'lib xizmat qilmoqda.

O'zbekiston misolida olib borilgan nazariy tahlil mamlakatda "Raqamli O'zbekiston – 2030" strategiyasi doirasida kiberxavfsizlikni ta'minlash borasida muhim yutuqlar qayd etilganini ko'rsatdi. "Shaxsiy ma'lumotlar to'g'risida" (2019) va "Kiberxavfsizlik to'g'risida" (2022) qonunlar milliy huquqiy bazani shakllantirdi. Shu bilan birga, amaliyotda xalqaro standartlarga to'liq integratsiyalashuv, tezkor javob mexanizmlarini kuchaytirish va davlat-xususiy sektor o'rtasidagi hamkorlikni kengaytirish zarurati saqlanib qolmoqda.

Xulosa sifatida ta'kidlash joizki, raqamli iqtisodiyotda kiberxavfsizlikni ta'minlash milliy xavfsizlik, iqtisodiy barqarorlik va xalqaro raqobatbardoshlikning muhim omiliga aylanmoqda. Shu sababli, O'zbekistonda quyidagi yo'nalishlarni kuchaytirish maqsadga muvofiqdir:

1. Kiberxavfsizlik siyosatini xalqaro standartlarga mos ravishda yangilash;

2. Davlat va xususiy sektor o'rtasida axborot almashuv mexanizmlarini takomillashtirish;

3. Aholi va mutaxassislar o'rtasida raqamli madaniyat va kiberhushyorlikni oshirish;

4. Kiberxavfsizlik infratuzilmasini texnologik va institutsional jihatdan mustahkamlash;

5. Xalqaro tashkilotlar bilan doimiy hamkorlikni rivojlantirish.

Shunday qilib, raqamli iqtisodiyot barqaror rivojlanishi uchun kiberxavfsizlikni kompleks boshqaruv tizimi sifatida shakllantirish nafaqat zarurat, balki milliy iqtisodiy strategiyaning ajralmas tarkibiy qismidir.

FOYDALANILGAN ADABIYOTLAR RO'YXATI

1. Tapscott, D. (2015). *The Digital Economy: Promise and Peril in the Age of Networked Intelligence*. McGraw–Hill Education, New York.
2. Schwab, K. (2016). *The Fourth Industrial Revolution*. World Economic Forum, Geneva.
3. Brynjolfsson, E., & McAfee, A. (2014). *The Second Machine Age: Work, Progress, and Prosperity in a Time of Brilliant Technologies*. W. W. Norton & Company.
4. Denning, D. E. (1999). *Information Warfare and Security*. Addison–Wesley, Boston.
5. Singer, P. W., & Friedman, A. (2014). *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford University Press, Oxford.
6. ENISA (European Union Agency for Cybersecurity). (2024). *ENISA Threat Landscape Report 2023*. Luxembourg: Publications Office of the European Union.
7. OECD. (2021). *Digital Security Risk Management for Economic and Social Prosperity*. OECD Publishing, Paris.
8. World Economic Forum (2025). *Global Cybersecurity Outlook 2025*. Geneva: WEF Centre for Cybersecurity.
9. Fortinet. (2024). *Global Threat Landscape Report*. Fortinet Inc., California.
10. World Bank. (2024). *Cybersecurity Economics for Emerging Markets*. Washington D.C.: World Bank Group.
11. Council of Europe. (2001). *Budapest Convention on Cybercrime*. Strasbourg: Council of Europe Treaty Series.
12. European Commission. (2023). *Cyber Resilience Act*. Brussels: Official Journal of the European Union.
13. ITU. (2024). *Global Cybersecurity Index (GCI) 2024*. International Telecommunication Union, Geneva.

14. O‘zbekiston Respublikasi Oliy Majlisi. (2019). *“Shaxsiy ma’lumotlar to‘g‘risida”gi Qonun* (O‘RQ–547). Toshkent.
15. O‘zbekiston Respublikasi Oliy Majlisi. (2022). *“Kiberxavfsizlik to‘g‘risida”gi Qonun* (O‘RQ–764). Toshkent.
16. O‘zbekiston Respublikasi Prezidentining qarori. (2023). *“Raqamli iqtisodiyotda kiberxavfsizlikni ta’minlash chora-tadbirlari to‘g‘risida”* (PQ–450). Toshkent.
17. Kaspersen, R. (2021). “Transnational Cybersecurity Governance.” *Journal of Cyber Policy*, Vol. 6, No. 3, pp. 145–160.
18. Ortiqov, A. (2022). “O‘zbekistonda raqamli iqtisodiyotni rivojlantirish strategiyasi.” *Iqtisodiyot va Innovatsiya Jurnali*, № 2.
19. Tursunova, M. (2023). “Raqamli iqtisodiyotda ma’lumotlar xavfsizligi muammolari.” *Axborot Texnologiyalari Jurnali*, № 3.
20. UNODC. (2023). *Draft Cybercrime Treaty Report*. United Nations Office on Drugs and Crime, Vienna.