

RAQAMLI IQTISODIYOTDA KIBERXAVFSIZLIK: DOLZARB MUOMMOLAR VA ISTIQBOLI YECHIMLAR

Muallif: Xamdamov Suxrobbek Ravshanbek o'g'li

Toshkent davlat iqtisodiyot universiteti Menejment

fakulteti MNP-76 guruh talabasi

suhrobhamdamov005@gmail.com

Ilmiy rahbar: Ibragimov G'anijon G'ayratovich

Toshkent davlat iqtisodiyot universiteti Qoshma

ta'lim dasturlarini muvofiqlashtirish markazi boshlig'i

- Innovatsion menejment kafedrası dotsenti

Phd, g.ibragimov@tsue.uz

ANNOTATSIYA: Ushbu ilmiy maqolada zamonaviy raqamli iqtisodiyotni barqaror rivojlanishi uchun hal qiluvchi ahamiyatga ega bo'lgan kiberxavfsizlik muammolari tahlil qilinadi. Raqamli transformatsiya jarayonida iqtisodiy sub'yektlar, davlat tizimlari va yuridik shaxslarning muhim moliyaviy, tijorat va shaxsiy ma'lumotlari ko'plab kiberxavflarga duchor bo'lmoqda. Tadqiqotning asosiy maqsadi – raqamli iqtisodiyotning o'ziga xos xususiyatlarini hisobga olgan holda, kiberxavfsizlikning dolzarb muammolarini aniqlash, ularning iqtisodiy oqibatlarini baholash va istiqbolli yechimlarni taklif etishdir. Maqolada kiberhujumlarning iqtisodiy jihatdan jismoniy va yuridik shaxslarga, shuningdek, makroiqtisodiy barqarorlikka ta'siri tizimli o'rganiladi. Shuningdek, O'zbekiston iqtisodiyotini raqamlashtirish sharoitida kiberxavfsizlikni ta'minlash yo'nalishidagi chora-tadbirlar, xalqaro tajribalar va milliy risklarni boshqarishning zamonaviy usullari tahlil qilinadi. Tadqiqotda ilmiy tahlil, statistik ma'lumotlar qiyosiy tahlil, tizimli yondashuv kabi usullar qo'llanilgan.

Kalit so'zlar: raqamli iqtisodiyot, kiberxavfsizlik, kiberhujum, ma'lumotlar himoyasi, iqtisodiy xavf, raqamli transformatsiya, kibertahdid, blockchain, sun'iy intellekt, O'zbekiston.

KIRISH

XXI asr – axborot va raqamli texnologiyalar asri sifatida qaraladi. “Raqamli iqtisodiyot” tushunchasi nafaqat yangi texnologiyalarning qo'llanilishi, balki ishlab chiqarish, taqsimot, ayirboshlash va iste'mol qilishning butun tizimini tubdan o'zgartiruvchi ijtimoiy-iqtisodiy hodisadir. Raqamlashtirish iqtisodiy o'sishning yangi manbalarini ochib berayotgan bo'lsa-da, u bilan birga butunlay yangi turdagi xavflar – kiberxavflar ham paydo bo'lmoqda. Kibermakon iqtisodiy faoliyatning asosiy maydoniga aylangan sari, moliyaviy tizimlar, korporativ tarmoqlar, davlat xizmatlari

va hatto infratuzilma ob'yektlari raqamli hujumlarga nisbatan juda himoyasiz holga kelmoqda.

Dunyo bo'yicha kiberhujumlar soni va ularning iqtisodiy zarari har yili katlab o'sib bormoqda. Jahon Iqtisodiy Forumi ma'lumotlariga ko'ra, kibertahdidlar global miqyosda beshta eng katta xavf qatoriga kiradi. Kiberhujumlar natijasida yuzaga keladigan bevosita moliyaviy yo'qotishlar, intellektual mulkning o'g'irlanishi, ishonchning yo'qolishi va ish faoliyatining uzilishi nafaqat yakka tartibdagi kompaniyalar, balki butun mamlakatlar iqtisodiyotiga jiddiy zarar yetkazishi mumkin.

O'zbekiston Respublikasida "Raqamli O'zbekiston – 2030" strategiyasi qabul qilinganligi, davlat va bank xizmatlarining faol raqamlashtirilayotganligi, raqamli to'lov tizimlarining jadal rivojlanishi mamlakatimiz iqtisodiyotini ham kibertahdidlar oldida ochiq holga keltirmoqda. Shu sababli, raqamli iqtisodiyot sharoitida kiberxavfsizlik masalalarini o'rganish, milliy va korporativ darajada samarali himoya mexanizmlarini ishlab chiqish dolzarb ilmiy-amaliy vazifaga aylanmoqda.^[1] Ushbu maqolaning maghsadi raqamli iqtisodiyot kontekstida kiberxavfsizlikning dolzarb muammolarini ilmiy jihatdan o'rganish va ularni bartaraf etishning istiqbolli yo'nalishlarini taklif etishdir. Vazifalari esa: birinchidan, raqamli iqtisodiyot va kiberxavfsizlik o'rtasidagi bog'liqlikni tahli qilish; ikkinchidan, zamonaviy kibertahdidlarning turlari va ularning iqtisodiy oqibatlarini o'rganish; uchinchidan, kiberxavfsizlikni ta'minlashning xalqaro va milliy amaliyotlarini tahli qilish; to'rtinchi, raqamli iqtisodiyotning barqarorligini ta'minlash uchun kiberxavfsizlik sohasidagi istiqbolli texnologik va institutsional yechimlarni ishlab chiqish.^[2]

1. RAQAMLI IQTISODIYOTNING XUSUSIYATLARI VA KIBERXAVFSIZLIKKA BO'LGAN EHTIYOJ

Raqamli iqtisodiyot an'anaviy iqtisodiyotdan quyidagi asosiy jihatlari bilan farq qiladi: birinchidan, uning asosiy ishlab chiqarish omili ma'lumot (data) hisoblanadi; ikkinchidan, faoliyat asosan virtual makonda (Internet, bulutli texnologiyalar) olib boriladi; uchinchidan, ishtirokchilar o'rtasidagi o'zaro ta'sir va tranzaktsiyalar deyarli darhol amalga oshiriladi; to'rtinchi, tizimlarning o'zaro bog'liqligi (Internet of Things, IoT) juda yuqori darajada.

Aynan ushbu xususiyatlar raqamli iqtisodiyotni kiberxavflarga nihoyatda himoyasiz qiladi:

1. Ma'lumotlarning markazlashuvi va qimmatliligi: Kompaniyalarning barcha moliyaviy hisob-kitoblari, mijozlar bazasi, sanoaviy sirlari va biznes-rejalari raqamli shaklda saqlanadi. Ushbu ma'lumotlar o'g'irlanishi yoki shifrlanishi (ransomware hujumlari) to'g'ridan-to'g'ri kompaniyaning mablag' yo'qotishiga va bankrotligiga olib kelishi mumkin.

2. Tarmoqli infratuzilmaning murakkabligi: Hamma narsaning Internetga ulangani sanoat va energetika ob'jektlarini ham kiberhujumlar uchun ochiq nishonga

aylantiradi. Kiberhujum natijasida yirik ishlab chiqarish yoki energiya tizimi ishdan chiqsa, butun mintaqqa iqtisodiyotiga milliardlab zarar yetishi mumkin.

3. Trasaksiyalarning tezligi va virtual tabiati: Onlayn bankomatlar (ATM), to'lov tizimlari va kriptovalyuta birjalariga qilingan hujumlar bir necha daqiqada millionlab mablag'larni yo'q qilishi mumkin. Bunday hollarda hujumni qaytarish yoki yo'qotilgan mablag'ni qaytarib olish deyarli imkonsiz.

4. Xalqaro tabiat: Kiberhujumchi bir qit'ada joylashgan bo'lib, boshqa qit'adagi kompaniyani nishon olishi mumkin. Bu huquqni muhofaza qilish organlari uchun jinoyatchilarni aniqlash va javobgarlikka tortishda qiyinchiliklar tug'diradi.

Shunday qilib, kiberxavfsizlik raqamli iqtisodiyotning integratsiyalashgan, uzluksiz va strategik muhim elementi sifatida qaralishi kerak. Bu nafaqat IT-xavfsizlik masalasi, balki kompaniyaning moliyaviy barqarorligi, obro'si va raqobatbardoshligini saqlab qolishning asosiy omilidir.

2. RAQAMLI IQTISODIYOT UCHUN ASOSIY KIBERTAHIDIDLAR VA ULARNING IQTISODIY OQIBATLARI

Zamonaviy kibertahdidlar juda xilma-xil va murakkabdir. Raqamli iqtisodiyot sub'yektlari uchun eng xavfli va keng tarqalgan hujum turlari quyidagilardir:

2.1. Ransomware (Fidye) hujumlari. Bu hujum turida zararli dastur (virus) tarmoqdagi barcha ma'lumotlarni shifrlab qo'yadi va shifrnı ochish uchun to'lov (odatda kriptovalyutada) talab qilinadi. Iqtisodiy ta'siri: bevosita to'lov, ish vaqtining yo'qolishi (downtime), mijozlarning ishonchsizligi, qayta tiklash uchun qo'shimcha xarajatlar. 2021-yilda Amerikadagi Colonial Pipeline neft quvuriga qilingan ransomware hujumi natijasida kompaniya 4,4 million dollar to'lashi va bir necha kun davomida quvur ishlaymay qolishi Shimoliy Amerikada benzin tanqisligi va narxlar o'sishiga olib keldi.

2.2. Phishing va ijro etilgan ijtimoiy muhandislik hujumlari. Xodimlar yoki mijozlarni aldab, ularning hisob ma'lumotlari, parollari yoki karta ma'lumotlarini olishga qaratilgan. Iqtisodiy ta'siri: bank hisobvarag'ining tozalanishi, firibgarlik tranzaksiyalari, kompaniyaning ichki ma'lumotlarining sizib chiqishi.

2.3. DDoS (Tarqatilgan Xizmatni Rad Qilish) hujumlari. Hujumchi bir nechta kompyuterlardan (botnet) maqsadli serverga shuncha so'rov yuboradiki, u haqiqiy foydalanuvchilarga xizmat ko'rsata olmay qoladi. Iqtisodiy ta'siri: elektron savdo (e-commerce) saytlarining ishlaymay qolishi, onlayn xizmatlarning to'xtab qolishi, daromadning bir vaqtning o'zida yo'qolishi. Masalan, yirik onlayn-do'kon bir soatlik ishlaymay qolishi yuz minglab dollar zarar keltirishi mumkin.

2.4. Zanjirli yetkazib berishdagi (Supply Chain) hujumlar. Hujumchi asosiy maqsadga bevosita emas, balki unga xizmat ko'rsatadigan kichikroq va himoyasi sustroq provayder (masalan, dasturiy ta'minot ishlab chiqaruvchi) orqali hujum qiladi. Iqtisodiy ta'siri: juda keng miqyosli bo'lishi mumkin, chunki bitta provayderga hujum

orqali yuzlab unga bog'liq bo'lgan kompaniyalarni zaiflashtirish mumkin. 2020-yilda SolarWinds kompaniyasining dasturiy ta'minotiga kirib olish orqali AQShning bir qancha davlat idoralari va yirik korporatsiyalari zarar ko'rgan edi.

2.5. Kriptovalyuta birjalari va defi (markazlashmagan moliya) platformalariga hujumlar. Blockchain texnologiyasi o'ziga xos xavfsizlik imkoniyatlariga ega bo'lsa-da, kriptovalyuta birjalari, hamyonlar (wallets) va aqlli shartnomalar (smart contracts) xatolari kiberhujumchilar uchun nishon bo'lib qolmoqda. Iqtisodiy ta'siri: birjalardan millionlab dollarlik kriptovalyutalarning o'g'irlanishi, investorlarning ishonchining uzilishi va butun bozorning o'zgaruvchanligining kuchayishi.

Kiberhujumlarning makroiqtisodiy oqibatlarini quyidagilarni o'z ichiga olishi mumkin:

- Investitsiya iqlimining yomonlashuvi: Mamlakatda kiberxavfsizlik darajasi past bo'lsa, xorijiy to'g'ridan-to'g'ri investitsiyalar jalb qilish qiyinlashadi.
- Davlat byudjetiga zarar: Davlatning soliq yig'ish tizimi, g'azna tizimi hujumga uchrasa, byudjet daromadlari sezilarli darajada kamayishi mumkin.
- Milliy valyuta barqarorligining buzilishi: Yirik banklar yoki milliy to'lov tizimiga hujum milliy valyutaga ishonchni susaytirishi va inflyatsiyani kuchaytirishi mumkin.

3. KIBERXAVFSIZLIKNI TA'MINLASHDA XALQARO VA MILLIY TAJRIBALAR

3.1. Xalqaro amaliyot va statistik tahlillar. Rivojlangan davlatlar kiberxavfsizlikni mamlakat mudofaasi va iqtisodiy xavfsizligining ajralmas qismi sifatida qaraydilar. Statistik ma'lumotlar bu sohadagi investitsiyalar zarurligini aniq ko'rsatmoqda.

Moliyaviy yo'qotishlar hajmi: "Cybersecurity Ventures" tashkilotining 2023-yilgi hisobotiga ko'ra, kiberjinoyatchilik tufayli butun dunyo bo'yicha yillik zarar 2025-yilga kelib 10,5 trillion AQSh dollariga yetishi kutilmoqda. Bu 2021-yildagi 6 trillion dollarlik ko'rsatkichdan deyarli ikki baravar o'sishni anglatadi. Bu miqdor butun dunyo YalChning taxminan 10% ga teng bo'lib, iqtisodiyotga ta'siri beqiyos ekanligini ko'rsatadi.

· Investitsiyalar va bozor hajmi: Xuddi shu manbaga ko'ra, global kiberxavfsizlik bozori 2023-yilda 173 milliard dollar miqdorida baholangan bo'lsa, 2030-yilga kelib u 500 milliard dollardan oshishi kutilmoqda. Bu esa kiberxavfsizlik sanoatining o'sish sur'atlarining o'ziga xosligini va unga bo'lgan talabning ortib borayotganini anglatadi.

· Hujumlar soni: "Check Point Research"ning 2023-yilgi ma'lumotlariga ko'ra, butun dunyo bo'yicha tashkilotlarga qilingan hujumlar soni oldingi yilga nisbatan 38% ga oshgan. Har o'rtacha tashkilot haftasiga 1200 dan ortiq hujumga uchraydi. Eng ko'p

hujumga uchragan sohalar qatorida ta'lim/sanoat (o'rtacha haftasiga 2300 hujum) va hukumat/harbiy tashkilotlar (o'rtacha haftasiga 1600 hujum) turadi.

- Davlatlar reytingi: "ITU Global Cybersecurity Index (GCI) 2020" ma'lumotlariga ko'ra, kiberxavfsizlik sohasida eng rivojlangan davlatlar AQSh, Birlashgan Qirollik va Saudiya Arabistoni hisoblanadi. Ushbu reyting qonunchilik, texnik, tashkiliy, hamkorlik va ta'lim sohalaridagi tayyorgarlik darajasini baholaydi.

3.2. Milliy darajadagi g'oyalar: O'zbekiston misolida. O'zbekiston Respublikasi raqamlashtirish va kiberxavfsizlik sohasida bir qator muhim qonun hujjatlarini qabul qildi. "Raqamli O'zbekiston – 2030" strategiyasi va "Kiberxavfsizlik to'g'risida"gi Qonun (2021-yil) asosiy me'yoriy-huquqiy bazani yaratdi.

Statistik jihatdan O'zbekistonda vaziyat:

O'zbekiston ITU Global Cybersecurity Indexda 2020-yilda 82-o'rinni egallagan bo'lsa, sa'y-harakatlar tufayli bu ko'rsatkichni yaxshilash ustida ish olib borilmoqda.

- O'zbekiston Markaziy Banki ma'lumotlariga ko'ra, 2022-yilda O'zbekistondagi bank tizimiga qilingan kiberhujumlar soni 2021-yilga nisbatan 25% ga oshgan. Eng keng tarqalgan hujum turlari qatorida phishing va bank kartalaridagi firibgarlik operatsiyalari bor.

- "Uzkomnazorat" ma'lumotlariga asosan, mamlakatdagi davlat axborot tizimlariga qilingan hujumlarning asosiy manbai (75% holatlarda) tashqi tomondan, turli mamlakatlardan amalga oshirilgan. Bu milliy tizimlarni himoya qilish murakkabligini ko'rsatadi.

Amaldagi chora-tadbirlar:

"2022-2023-yillarda O'zbekiston Respublikasi kiberxavfsizlik sohasini rivojlantirishning asosiy yo'nalishlari" davlat dasturi qabul qilindi.

- Milliy Kiberxavfsizlik Markazi tashkil etildi, uning vazifasi davlat axborot resurslarini himoya qilish va inqirozli vaziyatlarda operativ aralashuvdir.

- Kiberpolis tuzilmasi faoliyat yuritmoqda, kiberjinoyatchilarga qarshi kurash olib borilmoqda.

- Kiberxavfsizlik mutaxassislarini tayyorlash yo'lga qo'yildi. Oliy ta'lim muassasalarida (Toshkent Axborot Texnologiyalari Universiteti, TDIU va boshqalar) tegishli mutaxassisliklar ochildi.

Shunga qaramay, O'zbekiston raqamli iqtisodiyotda kiberxavfsizlikni ta'minlashda bir qator muammolarga duch kelmoqda:

1. Malakali kadrlar tanqisligi. Kiberxavfsizlik bo'yicha chuqur bilimga ega mutaxassislar soni talabdan ancha past.

2. Kichik va o'rta biznesning himoyasizligi. KOB lar ko'pincha kiberxavfsizlikga investitsiya qilish uchun moliyaviy imkoniyatga ega emas, natijada ular hujumchilar uchun oson nishonga aylanadi.

3. Aholining kibermadaniyat darajasining pastligi. Foydalanuvchilarning ko'pchiligi oddiy parol xavfsizligi qoidalariga ham rioya qilmaydi, bu esa phishing hujumlarining muvaffaqiyatli bo'lish imkoniyatini oshiradi.

4. Qonunchilikning rivojlanayotgan xususiyati. Tezkor rivojlanayotgan texnologik tahdidlarga tezda javob bera oladigan huquqiy mexanizmlar hali to'liq shakllanmagan.

4. RAQAMLI IQTISODIYOT UCHUN ISTIQBOLLI YECHIMLAR VA TAKLIFLAR

Kibertahdidlar murakkablashib borar ekan, himoya usullari ham yangi texnologiyalar va yondashuvlar asosida takomillashtirilishi zarur.

4.1. Texnologik yechimlar:

Sun'iy intellekt (SI) va Mashina o'rganishi (MO): SI tizimlari tarmoqdagi normal faoliyatdan og'ishlarni (anomalyarni) aniqlash, potensial hujumlarni real vaqt rejimida kutish va oldini olish, zararli dasturlarni tahlil qilishda insondan ancha tezroq ishlashi mumkin. Statistika ko'ra, SI asosidagi xavfsizlik yechimlari an'anaviy usullarga nisbatan tahdidlarni aniqlash tezligini 95% ga oshirishi mumkin.

- Blockchain texnologiyasi: Ma'lumotlarning o'zgarmasligi va shaffofligi tamoyiliga asoslangan. Trasaksiyalar zanjirini himoya qilish, hujumni aniqlash va uning manbasini kuzatish uchun ishlatilishi mumkin. Bu ayniqsa moliyaviy operatsiyalar, zanjirli yetkazib berish (supply chain) va shaxsni tasdiqlash tizimlarida samarali.

- Nol ishonch (Zero Trust) arxitekturasini: "Ichkaridagi hamma narsaga ishon" tamoyilidan voz kechish va tashqi va ichki har qanday so'rovni doimiy ravishda tekshirish va tasdiqlashga asoslangan yondashuv. Bu ichki tahdidlarni (masalan, noroz xodim) kamaytirishga yordam beradi.

- Bulutli xavfsizlik (Cloud Security): Bulutli xizmatlar provayderlari (AWS, Google Cloud, Microsoft Azure) o'z mijozlari uchun keng ko'lamli va yangilanib turadigan xavfsizlik vositalarini taklif etadi, bu esa, ayniqsa, KOB lar uchun o'z infratuzilmasini yaratishdan ko'ra arzonroq va samaraliroq variant bo'lishi mumkin.

4.2. Tashkiliy va qonunchilik yechimlari (O'zbekiston kontekstida):

1. Kibermadaniyatni rivojlantirishning milliy dasturini ishlab chiqish va joriy etish. Maktablardan boshlab, oliy ta'lim muassasalarida va korxonalarda majburiy o'quv kurslari orqali aholi va xodimlarning savodxonligini oshirish.

2. Davlat va xususiy sektor o'rtasidagi ma'lumot almashinuvini kuchaytirish. Xavf haqida ogohlantirish (Threat Intelligence) platformasini yaratish, barcha iqtisodiy sub'yektlar, ayniqsa banklar va yirik korxonalar uchun hujumlar to'g'risidagi ma'lumotlarni almashishni majburiy qilish.

3. Kichik va o'rta biznes uchun subsidiyalar va imtiyozlar. Kiberxavfsizlik echimlarini (antivirus, firewall, SI asosidagi monitoring tizimlari) sotib olish yoki

bulutli xizmatlar sifatida olishda davlat tomonidan qisman kompensatsiya yoki soliq imtiyozlari joriy etish.

4. Milliy kiberxavfsizlik kadrlar tayyorlash ekotizimini yanada rivojlantirish. Xalqaro sertifikatlash (CEH, CISSP, CompTIA Security+) dasturlarini joriy qilish, talabalarni rag'batlantirish, ilmiy-tadqiqot ishlarini moliyalashtirish.

5. "Kibersug'urta" bozorini rivojlantirish. Raqamli aktivlarni sug'urtalash xizmatlarini taklif qiluvchi mahalliy sug'urta kompaniyalarini rag'batlantirish, bu kompaniyalarga kiberhodisalardan keyin tez tiklanishing moliyaviy yukini kamaytiradi.

6. Xalqaro hamkorlikni kengaytirish. INTERPOL, ASEAN, MDH doirasidagi kiberxavfsizlik agentliklari bilan operativ ma'lumot almashish, qo'shma mashqlar o'tkazish va mutaxassislar almashinuvini yo'lga qo'yish.

XULOSA

Raqamli iqtisodiyot nafaqat yangi imkoniyatlar, balki global miqyosli yangi xavflar makonini ochdi. Kiberxavfsizlik endi ixtiyoriy "texnik masala" emas, balki har qanday davlat, korporatsiya va hatto jismoniy shaxsning raqamli dunyodagi mavjudligi va barqarorligi uchun strategik shartdir.

Tadqiqot shuni ko'rsatdiki, kiberhujumlar yil sayin murakkablashib, tashkil etilganroq bo'lib borayotgani holda, ularning iqtisodiy zarari trillionlab dollarlarni tashkil etmoqda. O'zbekiston kabi raqamli transformatsiya bosqichida bo'lgan mamlakatlar uchun tahdidlar alohida jiddiydir, chunki infratuzilma va madaniy tayyorgarlik hali yetarli emas.

Kiberxavflarga qarshi kurashda muvaffaqiyat kompleks yondashuvni talab qiladi. Bunga texnologik innovatsiyalar (SI, blockchain, Zero Trust), qat'iy va moslashuvchan qonunchilik bazasi, malakali kadrlar tayyorlash tizimi va, eng muhimi, keng jamoatchilikning kibermadaniyat darajasini oshirish kiradi. Faqatgina ushbu yo'nalishlarni uyg'un amalga oshirish orqali raqamli iqtisodiyotning ijobiy imkoniyatlari to'liq ochilishi va uning rivojlanishi xavfsiz va barqaror bo'lishi mumkin.

Kelajakda tadqiqotni O'zbekistonning aniq iqtisodiy sektorlari (bank-moliya, energetika, transport) uchun kiberxavflarni baholash modellarini ishlab chiqish va milliy lashtirilgan kiberxavfsizlik mahsulotlari bozorini rivojlantirish yo'nalishlarida chuqurlashtirish maqsadga muvofiqdir.

FOYDALANILGAN ADABIYOTLAR RO'YXATI

1. Cybersecurity Ventures. (2023). 2023 Cybersecurity Almanac: 100 Facts, Figures, Predictions and Statistics.
2. Check Point Research. (2023). Cyber Security Report 2023: The Year of Mega Ransomware.

3. International Telecommunication Union (ITU). (2021). Global Cybersecurity Index (GCI) 2020.
4. IBM Security. (2023). Cost of a Data Breach Report 2023.
5. O'zbekiston Respublikasi Prezidentining "Raqamli O'zbekiston-2030" strategiyasini tasdiqlash to'g'risidagi PF-6079-son Farmoni. 05.10.2020.
6. O'zbekiston Respublikasining "Kiberxavfsizlik to'g'risida"gi Qonuni. 03.04.2021.
7. O'zbekiston Respublikasi Markaziy Banki ma'lumotlari. (2022). Bank tizimining xavfsizligi bo'yicha hisobot.
8. McAfee. (2023). The Hidden Costs of Cybercrime.
9. World Economic Forum. (2023). The Global Risks Report 2023.
10. Toshkent Davlat Iqtisodiyot Universiteti. (2022). Raqamli iqtisodiyotning zamonaviy tendensiyalari. Ilmiy ma'ruzalar to'plami.