

**RAQAMLI IQTISODIYOT SHAROITIDA KIBERXAVFSIZLIK:
IQTISODIY BARQARORLIK VA RAQAMLI ISHONCH MASALALARI****Jurayev Uktam Yusupovich**

“Sun’iy intellekt va raqamli iqtisodiyotni rivojlantirish markazi” davlat muassasasi
bosh buxgalteri

Annotatsiya: Mazkur tezisdagi raqamli iqtisodiyotning jadal rivojlanishi sharoitida kiberxavfsizlikning iqtisodiy barqarorlik va raqamli ishonchni ta’minlashdagi o’rni tahlil qilinadi. Raqamli xizmatlar, elektron tijorat, elektron hukumat, raqamli moliya va sun’iy intellektning keng qo’llanilishi bilan birga kiberxavflarning iqtisodiy oqibatlari ham ortib bormoqda. Tadqiqotda kiberhujumlarning biznes faoliyati, investitsiyalar, iste’molchilar ishonchi va davlat xizmatlariga ta’siri ko’rib chiqiladi. Shuningdek, kiberbarqarorlikni kuchaytirish, ma’lumotlarni himoyalash, inson kapitalini rivojlantirish va davlat-xususiy hamkorlikni takomillashtirish bo’yicha takliflar ishlab chiqiladi.

Kalit so’zlar: raqamli iqtisodiyot, kiberxavfsizlik, kiberbarqarorlik, raqamli ishonch, iqtisodiy barqarorlik, ma’lumotlar xavfsizligi, raqamli transformatsiya.

XXI asrda raqamli texnologiyalarning iqtisodiyotning deyarli barcha tarmoqlariga chuqur kirib borishi iqtisodiy munosabatlarning shakli va mazmunini tubdan o’zgartirmoqda. Bugungi kunda elektron tijorat, raqamli bank xizmatlari, masofaviy mehnat, elektron hukumat, bulutli texnologiyalar, sun’iy intellekt, katta ma’lumotlar, buyumlar interneti va boshqa raqamli yechimlar iqtisodiy faoliyatning ajralmas qismiga aylanmoqda. Raqamlashtirish korxonalar uchun xarajatlarni kamaytirish, bozorlarni kengaytirish, ishlab chiqarish samaradorligini oshirish va yangi biznes modellarini yaratish imkonini bermoqda. Shu bilan birga, iqtisodiy faoliyatning raqamli muhitga tobora ko’proq bog’lanishi kiberxavfsizlik masalasini nafaqat texnik, balki iqtisodiy va strategik masalaga aylantirmoqda.

OECD yondashuviga ko’ra, raqamli xavfsizlikni faqat texnik muammo sifatida ko’rish yetarli emas. Kiberhodisalarning iqtisodiy va ijtimoiy oqibatlari ko’pincha texnik zararning o’zidan ancha keng bo’lishi mumkin. Shu sababli raqamli xavflarni boshqarish iqtisodiy va ijtimoiy maqsadlar bilan uyg’unlashtirilishi lozim [1].

Kiberxavfsizlikning iqtisodiy ahamiyati, avvalo, raqamli infratuzilmaning uzluksiz ishlashini ta’minlash bilan bog’liq. Masalan, bank tizimlariga qilingan kiberhujumlar moliyaviy operatsiyalarning vaqtincha to’xtashiga, korxonalarning ishlab chiqarish yoki xizmat ko’rsatish jarayonlari buzilishiga, davlat axborot tizimlarining ishlamay qolishiga sabab bo’lishi mumkin. Bunday hodisalarning bevosita moliyaviy zarari bilan bir qatorda, mijozlar ishonchining pasayishi, biznes



reputatsiyasining yomonlashishi va kelgusidagi investitsiya qarorlariga salbiy ta'siri ham mavjud.

Jahon bankining kiberxavfsizlik iqtisodiyotiga bag'ishlangan tadqiqotida ham kiberxavfsizlik iqtisodiy o'sishning muhim omillaridan biri sifatida ko'rsatiladi. Tadqiqot natijalariga ko'ra, rivojlanayotgan mamlakatlarda kiberhodisalarni kamaytirish aholi jon boshiga YaIM o'sishiga ijobiy ta'sir ko'rsatishi mumkin; kiberxavfsizlikka investitsiyalar nafaqat zararlarni oldini oladi, balki ishonch, raqobatbardoshlik va raqamli innovatsiyalarni rivojlantirishga xizmat qiladi [2].

Bugungi sharoitda "raqamli ishonch" tushunchasi ham alohida ahamiyat kasb etmoqda. Raqamli xizmatdan foydalanuvchi fuqaro yoki tadbirkor o'z ma'lumotlari xavfsizligiga, elektron to'lov tizimlarining ishonchliligiga, davlat axborot tizimlarining barqarorligiga va platformalarning qonuniy faoliyatiga ishonsa, raqamli iqtisodiyotning rivojlanish sur'ati ham yuqori bo'ladi. Aksincha, ma'lumotlarning o'g'irlanishi, firibgarlik, shaxsiy ma'lumotlarning noqonuniy tarqalishi yoki axborot tizimlarining tez-tez ishlamay qolishi raqamli xizmatlardan foydalanishga bo'lgan ishonchni susaytirishi mumkin.

Mazkur masala O'zbekiston uchun ham dolzarbdir. Mamlakatda davlat xizmatlari, bank-moliya tizimi, elektron savdo, ta'lim, sog'liqni saqlash va boshqa sohalarda raqamli texnologiyalardan foydalanish kengayib bormoqda. "O'zbekiston — 2030" strategiyasida kuchli iqtisodiyotni shakllantirish, zamonaviy texnologiyalarni rivojlantirish, xavfsizlik va barqarorlikni ta'minlash kabi ustuvor yo'nalishlar belgilangan.

Xalqaro elektraloqa ittifoqining Global Cybersecurity Index 2024 ma'lumotlariga ko'ra, O'zbekiston kiberxavfsizlik bo'yicha "Tier 2 — Advancing" guruhiga kiritilgan. Mamlakatning indeksdagi umumiy ko'rsatkichi 89,2 ballni tashkil etgan, 2020-yilgi ko'rsatkich bilan taqqoslaganda sezilarli o'sish qayd etilgan. Shu bilan birga, ITU mamlakatning texnik va tashkiliy yo'nalishlarida rivojlantirish imkoniyatlari mavjudligini ko'rsatadi [3].

Iqtisodiy barqarorlik deganda iqtisodiy tizimning ichki va tashqi ta'sirlarga moslashishi, faoliyatning uzluksizligini saqlab qolishi va salbiy shoklardan keyin tiklana olishi tushuniladi. Raqamli iqtisodiyot sharoitida kiberhujumlar ana shunday shoklarning yangi turini shakllantirmoqda.

Kiberhodisalarning iqtisodiy oqibatlarini bir necha guruhga ajratish mumkin:

- bevosita moliyaviy yo'qotishlar;
- ishlab chiqarish yoki xizmat ko'rsatishning to'xtashi;
- ma'lumotlarni tiklash xarajatlari;
- mijozlar va hamkorlar ishonchining pasayishi;
- huquqiy va kompensatsion xarajatlar;
- intellektual mulkning yo'qotilishi;





- investitsiya jozibadorligining pasayishi;
- davlat xizmatlari va muhim infratuzilma faoliyatining buzilishi.

Ayniqsa, moliya, energetika, transport, telekommunikatsiya va sog'liqni saqlash kabi strategik sohalarda raqamli tizimlarning ishdan chiqishi kengroq iqtisodiy oqibatlariga ega bo'lishi mumkin. Shu sababli zamonaviy kiberxavfsizlik strategiyasi faqat "hujumni oldini olish" tamoyiliga asoslanmasligi kerak. Hujumning mutlaqo oldini olish har doim ham mumkin emas. Muhim vazifa — hujumni imkon qadar erta aniqlash, zararni cheklash, asosiy xizmatlarni saqlab qolish va tizimni tez tiklashdan iborat. Bu esa "kiberbarqarorlik" tushunchasini yuzaga chiqaradi. Kiberbarqarorlik tashkilotning jiddiy kiberhodisadan keyin asosiy biznes funksiyalarini saqlab qolishi yoki tezda tiklashi qobiliyatini anglatadi. Jahon iqtisodiy forumi 2026-yilgi hisobotida kiberbarqarorlikni iqtisodiy qiymatni himoya qilishning muhim elementi sifatida ko'rsatadi [4].

Raqamli ishonch — raqamli iqtisodiyotning ko'zga ko'rinmaydigan, ammo fundamental aktivlaridan biridir. Fuqaro elektron davlat xizmatidan foydalanayotganda o'z ma'lumotlari himoyalaniishiga ishonsa, undan foydalanish ehtimoli ortadi. Tadbirkor elektron to'lov tizimining xavfsizligiga ishonsa, raqamli savdoga ko'proq murojaat qiladi. Investor mamlakatning raqamli infratuzilmasi va ma'lumotlarni boshqarish tizimlariga ishonsa, raqamli loyihalarga investitsiya kiritish imkoniyati oshadi. Demak, raqamli ishonchni faqat texnik himoya vositalari bilan yaratib bo'lmaydi. Bunda qonunchilik, institutlar, korporativ madaniyat, kadrlar malakasi, foydalanuvchi xabardorligi va davlat-xususiy hamkorlik bir butun tizim sifatida ishlashi lozim.

Kiberxavfsizlikni ta'minlashda barcha xavflarga bir xil miqdorda resurs sarflash iqtisodiy jihatdan samarali emas. Shu sababli riskka asoslangan yondashuv muhim ahamiyat kasb etadi. Riskka asoslangan yondashuvda avvalo tashkilot uchun eng muhim aktivlar aniqlanadi. Keyin ushbu aktivlarga tahdidlar, zaifliklar va potensial zararlar baholanadi. Shundan so'ng mavjud resurslar eng muhim xavflarni kamaytirishga yo'naltiriladi.

Texnologik vositalar qanchalik rivojlangan bo'lsin, kiberxavfsizlikning eng muhim omillaridan biri inson kapitali hisoblanadi. Parolni boshqa shaxsga berish, shubhali havolani ochish, soxta elektron xatga javob berish yoki ma'lumotlarni noto'g'ri saqlash kabi xatti-harakatlar texnik himoya vositalarining samaradorligini kamaytirishi mumkin. Shu sababli kiberxavfsizlik bo'yicha ta'limni faqat IT mutaxassislarini tayyorlash bilan cheklamaslik kerak. Oddiy foydalanuvchilar, davlat xizmatchilari, bank xodimlari, tadbirkorlar va talabalar ham asosiy kiberxavfsizlik ko'nikmalariga ega bo'lishlari zarur.

O'zbekistonning raqamli transformatsiyasi chuqurlashgani sari kiberxavfsizlikning iqtisodiy ahamiyati ham ortib bormoqda. Elektron davlat





xizmatlari, raqamli to'lovlar, bank ilovalari, elektron savdo va boshqa raqamli xizmatlarning kengayishi foydalanuvchilar uchun qulaylik yaratadi, biroq ushbu tizimlarda yuzaga kelishi mumkin bo'lgan zaifliklarning iqtisodiy ta'sirini ham oshiradi.

ITU ma'lumotlari O'zbekistonning kiberxavfsizlik bo'yicha xalqaro ko'rsatkichlarida sezilarli rivojlanish qayd etilganini ko'rsatadi [3]. 2024-yilgi Global Cybersecurity Indexda mamlakat huquqiy, texnik, tashkiliy, salohiyatni rivojlantirish va hamkorlik kabi besh yo'nalish bo'yicha baholangan. O'zbekistonning nisbatan kuchli yo'nalishlari sifatida hamkorlik, huquqiy choralalar va salohiyatni rivojlantirish ko'rsatilgan, texnik va tashkiliy yo'nalishlar esa rivojlantirish imkoniyati mavjud sohalar sifatida qayd etilgan.

Bu natijalar kiberxavfsizlik siyosatining faqat qonunchilikni takomillashtirish bilan chegaralanmasligi kerakligini ko'rsatadi. Qonunchilikni amaliy texnik mexanizmlar, monitoring, audit, hodisalarga javob berish, kadrlar tayyorlash va biznesning xavfsizlik madaniyati bilan mustahkamlash zarur. Kelajakda kiberxavfsizlik siyosati "hujumni oldini olish" tamoyilidan "oldini olish — aniqlash — javob berish — tiklanish" tamoyiliga bosqichma-bosqich o'tishi kerak. Bunda kiberbarqarorlik tushunchasi asosiy o'rinlardan birini egallaydi. Tashkilotlar nafaqat himoyalani, balki kiberhodisa yuz berganda iqtisodiy faoliyatni imkon qadar qisqa vaqt ichida tiklay olishi lozim.

Umuman olganda, raqamli iqtisodiyotning uzoq muddatli barqarorligi uchta o'zaro bog'liq omilga tayanadi: xavfsiz raqamli infratuzilma, samarali risk boshqaruvi va yuqori darajadagi raqamli ishonch. Ushbu uch yo'nalish birgalikda rivojlantirilgan taqdirdagina raqamlashtirishning iqtisodiy samarasi to'liq namoyon bo'ladi.

Foydalanilgan adabiyotlar

1. OECD. OECD Policy Framework on Digital Security: Cybersecurity for Prosperity. Paris: OECD Publishing, 2022.
2. World Bank. Cybersecurity Economics for Emerging Markets. Washington, D.C.: World Bank, 2026.
3. International Telecommunication Union. Global Cybersecurity Index 2024. Geneva: ITU, 2024.
4. World Economic Forum. Global Cybersecurity Outlook 2026. Geneva: World Economic Forum, 2026.

