



## RAQAMLI IQTISODIYOTDA KIBERXAVFSIZLIKNING AHAMIYATI

**Uzaqov Ortiq Shaymardanovich**

Muhammad al-Xorazmiy nomidagi Toshkent  
axborot texnologiyalari universiteti Qarshi filiali

**Annotatsiya.** Raqamli iqtisodiyot insonlarning turmush darajasini sezilarli darajada oshiradi, bu uning asosiy foydasidir. Raqamli iqtisodiyot korrupsiya va qora iqtisodiyotning asosiy kushandasidir. Chunki, raqamlar hamma narsani muhrlaydi, xotirada saqlaydi, kerak paytda ma'lumotlarni tez taqdim etadi. Bunday sharoitda biron ma'lumotni yashirish, yashirin bitimlar tuzish, u yoki bu faoliyat haqida to'liq axborot bermaslikning iloji yo'q, kompyuter hammasini namoyon qilib qo'yadi. Ma'lumotlar ko'pligi va tizimlilik yo'lga va qing'ir ishlarga yo'l bermaydi.

**Kalit so'zlar:** raqamli iqtisodiyot, kiberxavfsizlik, ruxsatsiz kirish, bulutli xavfsizlik, monitoring, autentifikatsiya, ma'lumotlarni shifrlash, tranzaksiya.

## ЗНАЧЕНИЕ КИБЕРБЕЗОПАСНОСТИ В ЦИФРОВОЙ ЭКОНОМИКЕ

**Узаков Ортик Шаймарданович**

Каршинский филиал Ташкентский университет информационных  
технологий имени Мухаммада аль-Хорезми

**Аннотация.** Цифровая экономика существенно повышает уровень жизни людей, что является ее основным преимуществом. Цифровая экономика является основным связующим звеном коррупции и теневой экономики. Потому что числа запечатлевают все, сохраняют в памяти и быстро предоставляют информацию, когда это необходимо. В таких условиях невозможно скрыть какую-либо информацию, совершить тайные сделки, не предоставить полную информацию о той или иной деятельности, компьютер все выявит. Обилие и систематичность информации не допускают лжи и мошеннических действий.

**Ключевые слова:** цифровая экономика, кибербезопасность, несанкционированный доступ, облачная безопасность, мониторинг, аутентификация, шифрование данных, транзакция.

## THE IMPORTANCE OF CYBER SECURITY IN THE DIGITAL ECONOMY

**Uzakov Ortiq Shaymardanovich**

Karshi branch of Tashkent University of Information  
Technologies named after Muhammad al-Khorezmi

**Abstract.** The digital economy significantly improves people's living standards, which is its main advantage. The digital economy is the main link between corruption and the shadow economy. Because numbers capture everything, store it in memory, and quickly provide information when needed. In such conditions, it is impossible to hide any information, make secret transactions, or not provide complete information about a particular activity; the computer will reveal everything. The abundance and systematicity of information does not allow lies and fraudulent actions.

**Keywords:** digital economy, cybersecurity, unauthorized access, cloud security, monitoring, authentication, data encryption, transaction.

## **Kirish.**

Biznes jarayoni va jismoniy shaxslarning raqamli texnologiyalar va o'zaro bog'langan tizimlarga tobora ko'proq tayanadigan raqamli iqtisodiyotda kiberxavfsizlik hal qiluvchi rol o'ynaydi. Texnologiya taraqqiyoti davom etar ekan, nozik ma'lumotlarni himoya qilish, ishonchni saqlash va raqamli ekotizimlarning uzluksiz ishlashini ta'minlash uchun mustahkam kiberxavfsizlik choralari bo'lgan ehtiyoj yanada muhimroq sanaladi. Raqamli iqtisodiyotda kiberxavfsizlikning asosiy jihatlari, jumladan: ma'lumotlarni himoya qilish va maxfiylik bunda ma'lumotlarni shifrlash tranzaksiya vaqtida ma'lumotlarni himoya qilish uchun shifrlash usullaridan foydalanish ruxsatsiz kirishning oldini olishga yordam berishning nazariy materiallarga asoslangan holda mantiqiy tahlil usullaridan foydalanildi. Raqamli iqtisodiyotda kiberxavfsizlikning asosiy jihatlari, jumladan: ma'lumotlarni himoya qilish va maxfiylik bunda ma'lumotlarni shifrlash tranzaksiya vaqtida ma'lumotlarni himoya qilish uchun shifrlash usullaridan foydalanish ruxsatsiz kirishning oldini olishga yordam beradi.

## **Mavzuga oid adabiyotlar tahlili**

Xorijlik olimlardan Singer va Allan Friedmanlarning (2014) "Cybersecurity and Cyberwar: What Everyone Needs to Know" nomli kitobida kiberxavfsizlik haqida umumiy tushunchalar va foydalanuvchilar uchun kerakli ma'lumotlarni taqdim etishgan. 2017 yilda Kevin Mitnick va Robert Vamosi (2017) "The Art of Invisibility: The World's Most Famous Hacker Teaches You How to Be Safe in the Age of Big Brother and Big Data" Mitnick dunyodagi eng mashhur hekerlardan biri sifatida, kiberxavfsizlik va shaxsiy himoya haqida o'z tajribasini bayon etgan. Bruce Schneierning "Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World" nomli kitobida ma'lumotlar almashish, shaxsiy himoya va kiberxavfsizlik sohasidagi muddatli jarayonlarni o'rganish uchun keng tahlil qilgan. Evan Gilman, Richard A. Clarke (2020) va Robert K. Knake dunyo olimlarining "Zero Trust Networks: Building Secure Systems in Untrusted Networks" - va Doug Barth "Zero Trust" nomli ilmiy kitoblarida tarmoq xavfsizligini o'rganishga yordam beradigan va tarmoqlarda kiberxavfsizlikni mustahkamlashda kerakli maslahatlarni yozishgan. 2019 yilda "The Fifth Domain: Defending Our Country, Our Companies, and Ourselves in the Age of Cyber Threats" nomli kitobda, davlatlar, korporatsiyalar va shaxslar uchun kiberxavfsizlikning ahamiyatini tahlil qiladi. Dr. Mary Aiken o'zining "Cyber Resilience: A Holographic Paradigm" nomli ilmiy ishida, kiber-hamjinslik va kiberxavfsizlikda ziddiyat va qabul qilinuvchi tahlillarni taqdim etadi Yuqoridagi xorij olimlari kiberxavfsizlik sohasida keng qamrovli tahlillar va tushunchalarni o'rgangan holda, foydalanuvchilarga va soha mutaxassislariga tegishli muhim ma'lumotlarni taqdim etishgan Raqamli iqtisodiyot davrida, kiberxavfsizlikning tizimli va amaliy integratsiyasi muhimdir, shuningdek o'zgaruvchilarni tahlil qilish, korporativ tarmoqlarni himoya qilish va kiberxavfsizlikni oshirish uchun hujjatlar tuzishni o'rgangan holda kiberxavfsizlik sohasida o'zlarini tayyorlash uchun foydalanuvchi yoki mutaxassislar uchun ham muhimdir.

## **Tadqiqot metodologiyasi.**

Tadqiqot davomida ilmiy adabiyotlarda keltirilgan nazariy materiallarga asoslangan holda mantiqiy tahlil usullaridan foydalanildi. Mavjud ma'lumotlarni tahlil qilishda tahlil va sintez, qiyosiy tahlil kabi uslublar va yondashuvlar qo'llanilgan.

## **Tahlil va natijalar muhokamasi.**

Maxfiylik qoidalari esa axborotni muhofaza qilish qoidalariga (masalan, GDPR, CCPA) rioya qilish shaxslarning shaxsiy ma'lumotlarini himoya qilish va huquqiy oqibatlariga olib kelmaslik uchun zarurdir. Tarmoq xavfsizligi bo'yicha xavfsizlik devorlari va tajovuzni aniqlash tizimlari (IDS)lardan foydalaniladi. Xavfsizlik devorlari va IDSni joriy qilish tarmoq trafigini kuzatish va nazorat qilish, ruxsatsiz kirishni oldini olish va potentsial tahdidlarni aniqlashga

yordam beradi. Virtual xususiy tarmoqlar (VPNlar) esa VPN-lardan foydalanish, ayniqsa, masofaviy ishchilar va biznes tranzaksiyalari uchun internet orqali xavfsiz aloqani ta'minlaydi. Xavfsizlik nuqtai nazardan oxirgi chora sifatida antivirus dasturlarini keltirishimiz mumkin. Antivirus yechimlaridan foydalanish zararli dasturlarni qurilmalardan aniqlash va olib tashlashga yordam beradi. Bu bo'yicha Endpoint Protection Platforms (EPP) tizimlari hujumlar va turli kiber tahdidlardan himoya qiluvchi keng qamrovli xavfsizlik yechimlari hisoblanadi.

Bulutli xavfsizlik bu- Identity and Access Management (IAM) Bulutli resurslarga kirishni nazorat qilish faqat vakolatli shaxslar yoki tizimlar maxfiy ma'lumotlar bilan o'zaro aloqada bo'lishini ta'minlaydi. Natijada bulutda ma'lumotlarni shifrlash juda samarali hisoblanib, bulutda saqlangan ma'lumotlarni shifrlash ruxsatsiz kirishdan qo'shimcha himoya qatlamini qo'shadi.

Kiberxujumlarga javob berish va boshqarish. Kiberxavfsizlik bo'yicha treninglar xodimlarni kiberxavfsizlik bo'yicha ilg'or tajribalar bo'yicha o'rgatish, malaka oshirish va muntazam mashg'ulotlar o'tkazish tashkilotlarni xavfsizlik hodisalariga samarali javob berishga tayyorlaydi. Kiberxavfsizlik hodisalarining ta'sirini bartaraf etish va yumshatish uchun rejalarni ishlab chiqish va muntazam yangilash hamda uchinchi tomon ishlab chiqaruvchilari va hamkorlari bilan bog'liq kiberxavfsizlik risklarini baholash va boshqarish imkonini beradi.

Dasturiy ta'minot va tizimlarning zaifliklarning oldini olish uchun xavfsizlikni hisobga olgan holda ishlab chiqilishini ta'minlash. Kiberxavfsizlikda sun'iy intellekt (AI) va mashinani o'rganish (ML):

Tahdidlarni aniqlash: Shakllarni tahlil qilish va potentsial kiber tahdidlarni ko'rsatadigan anomaliyalarni aniqlash uchun AI va ML algoritmlaridan foydalanish. Avtomatlashtirilgan javob esa tez va samarali javob qaytarish uchun ayrim turdagi tahdidlarga avtomatlashtirilgan javoblarni amalga oshirish.

Doimiy monitoring yordamida tegishli qoidalarga doimiy rioya etilishini ta'minlash uchun kiberxavfsizlik choralari muntazam ravishda monitoring qilish va tekshirish shart hisoblanadi. Ma'lumotlarning buzilishi to'g'risida bildirishnoma ma'lumotlar buzilgan taqdirda o'z vaqtida va shaffof aloqa uchun protokollarni o'rnatishdan iborat. Axborot almashish platformalari yordamida sanoatdagi xamkorlar bilan xamkorlik aloqalarini o'rnatish va paydo bo'layotgan tahdidlar haqida ma'lumot almashish kiberxavfsizlik bo'yicha jamoaviy sa'y-harakatlarni kuchaytirish kerak.

Davlat-xususiy sheriklik orqali hukumatlar va xususiy sektor sub'ektlari kiberxavfsizlik choralari yanada kengroq miqyosda kuchaytirish uchun birgalikda ishlashini ta'minlashi lozim. Foydalanuvchi autentifikatsiyasi va avtorizatsiyasi bu ko'p faktorli autentifikatsiya (MFA) foydalanuvchilardan identifikatsiyaning bir nechta shakllarini taqdim etishni talab qilish orqali qo'shimcha xavfsizlik qatlamini qo'shishdan iborat. Kirish nazorati orqali kirish huquqlarini faqat shaxslar o'z rollarini bajarishi uchun zarur bo'lganlar bilan cheklashi mumkin. Raqamli iqtisodiyotning dinamik manzarasida kiberxavfsizlik bir martalik yechim sifatida emas, balki doimiy jarayon sifatida ko'rish kerak. Tashkilotlar resurslari va manfaatdor tomonlarini himoya qilish uchun rivojlanayotgan tahdidlarga, rivojlanayotgan texnologiyalarga moslashishi va kiberxavfsizlik madaniyatini rivojlantirishi kerak.

Raqamli iqtisodiyotda kiberxavfsizlikni ta'minlash nozik ma'lumotlarni himoya qilish, ishonchni saqlash va onlayn tizimlarning umumiy yaxlitligini ta'minlash uchun juda muhimdir. Kiberxavfsizlik bo'yicha mutaxassislar bilan hamkorlik qilish: Kiberxavfsizlik bo'yicha mutaxassislar bilan bog'lanish va so'nggi tahdidlar va xavfsizlik choralari haqida xabardor bo'lish. Xavfsizlikni baholash va maslahat uchun tashqi ekspertlarni yollash. Uchinchi tomon va hamkorlarning kiberxavfsizlik holatini baholash, chunki ular kiber tahdidlar uchun potentsial kirish nuqtasi bo'lishi mumkin. Ular xavfsizlik standartlariga va kiberxavfsizlik talablariga mos kelishiga ishonch hosil qilish. Tarmoqlar va tizimlarning noodatiy harakatlar uchun doimiy monitoringini amalga oshirish. Rivojlanayotgan tahdidlar va zaifliklar haqida xabardor bo'lish

uchun tahdidlar haqida ma'lumotdan foydalanish. Tashkilot dasturiy ta'minotini ishlab chiqsa, xavfsiz kodlash amaliyotiga rioya qilish, dasturiy ta'minot xatoliklarini bartaraf etish va ishlab chiqish muddati davomida muntazam ravishda xavfsizlik tekshiruvlarini o'tkazish. Tegishli kiberxavfsizlik qoidalari va standartlariga rioya qilish. Tashkilotda xavfsizlik bo'yicha o'rnatilgan eng yaxshi amaliyotlarga amal qilishini ta'minlashga yordam beradi. Tashkilot bulutli xizmatlardan foydalanish, bulutli xavfsizlik choralarini qo'llash. Bunga xavfsiz konfiguratsiya, ma'lumotlarni shifrlash va bulutli muhitni kuzatish amaliyotlari kiradi.

### Xulosa va takliflar.

Xulosa qilib shuni aytishimiz mumkin, kiberxavfsizlik uzluksiz jarayon bo'lib, raqamli iqtisodiyotda rivojlanayotgan tahdidlardan oldinda borish uchun faol va moslashuvchan yondashuvni talab qiladi. Yangi tahdid va xavf-xatarlarni aniqlash va bartaraf etish uchun kiberxavfsizlik strategiyasini muntazam ravishda qayta ko'rib chiqish va yangilab borish lozim. Raqamli iqtisodiyotda kiberxavfsizlikning ahamiyati juda yuqori darajada. Bu tizimlar va platformalar orqali ma'lumot almashish, xizmat ko'rsatish, tijorat, va o'zaro hamkorlik qilishning ko'plab sohalarida ishlashda ahamiyatli bo'lib keladi. Kiberxavfsizlikning hozirgi kundagi ahamiyati va dolzarbligini quyidagicha ifodalashimiz mumkin. Raqamli iqtisodiyotda ma'lumotlar o'zaro almashish va ishlab chiqishning boshqa sohalarida yaxshi foydalanilishi kafolatlangan bo'lishi kerak. Kiberxavfsizlik, shu ma'lumotlarni viruslar, hekeralar va boshqa xavf-xatarlardan himoya qilishda muhim rol o'ynaydi. Tijorat va biznes sohalarida, ma'lumot almashish va xavfsizlikni ta'minlash kabi ko'nikmalarga ega bo'lish, kompaniyalarni raqobatga bardoshlilikini kafolatlaydi. Korxonalar iqtisodiyoti va korporativ tizimlar, korxonalar ma'lumotlari, mijozlarning ma'lumotlari, va hokazo kabi ko'plab ma'lumotlarni saqlashadi. Shuning uchun kiberxavfsizlik, korxonalar iqtisodiyotini yaxshi himoya qilishda katta ahamiyatga ega.

### Adabiyotlar / Лумепамыра / Reference:

Ergash o'g'li, Qodirov Farrux. "Creation of electronic medical base with the help of software packages for medical services in the regions." *Conferencea (2022): 128-130.*

Ergash o'g'li, Qodirov Farrux. "Importance of kash-health web portal in the development of medical services in the regions." *Conferencea (2022): 80-83.*

Evan Gilman, Richard A. (2020) Clarke Zero Trust Networks: Building Secure Systems in Untrusted Networks" -Doug Barth "Zero Trust.

F Qodirov. Aholiga tibbiy xizmatlar ko'rsatishning rivojlanishini iqtisodiy-matematik modellashtirish. *Scienceweb academic papers collection . 2023/1/1.*

F Qodirov. Zamonaviy to'lov tizimlari tahlili va elektron pul birliklari. *Scienceweb academic papers collection. 2023/1/1.*

Farrux Qodirov. Development of scientific and technological system of management of industrial enterprises. *Scienceweb academic papers collection. 2023/1/1*

Farrux Qodirov. The place of econometrical modeling of healthcare quality improvement in the digital economy. *Scienceweb academic papers collection. 2023/1/1*

Farrux Qodirov. Zamonaviy trenajyor va simulyatsiya qiluvchi dasturlarning hozirgi kundagi ahamiyati. *Scienceweb academic papers collection. 2023/1/1*

Farrux, Qodirov. "Foreign experience in the development of medical services to the population." *Хоразм Маъмун академияси (2022).*

Kevin Mitnick & Robert Vamosi (2017). *The Art of Invisibility: The World's Most Famous Hacker Teaches You How to Be Safe in the Age of Big Brother and Big Data.*

Singer P.W. va Allan Friedman (2014). *Cybersecurity and Cyberwar: What Everyone Needs to Know.*

Қодиров, Фаррух. "Аҳолига соғлиқни сақлаш хизматлари кўрсатишининг ижтимоий-иқтисодий ривожланиши таҳлили." *Агро илт (2022).*

Фаррух Қодиров. Аҳолига хизмат кўрсатиш соҳасининг моделлаштиришни тизимли имитация қилиш. *Визнес-Эксперт. Том 173. Номер №5. Страницы 102-106. Дата публикации 2022.*