

**O‘ZBEKISTON RESPUBLIKASIDA RAQAMLI IQTISODIYOTNI
RIVOJLANTIRISH JARAYONIDA KIBER JINOYATLARNI OLDINI
OLISH**

Umurzoqov Mexroj Umar o‘g‘li

E-mail: umirzakovm7@gmail.com

Jahon iqtisodiyoti va diplomatiya universiteti “Xalqaro huquq” fakulteti magistranti

Ilmiy rahbar: Ph.D., Yusupdjanov Odil Abdugafurovich

Yoshlar masalalari va ma’naviy-ma’rifiy ishlar bo‘yicha birinchi prorektor,

Jahon iqtisodiyoti va diplomatiya universiteti

ANNOTATSIYA

Mazkur maqola bugungi kunda iqtisodiyotni raqamashtirish va kripto-aktivlar aylanmasi sohasini rivojlantirish jarayonidagi xavflarni statistik ma’lumotlarga asoslangan holda yoritib beradi. Kiberhujum (raqamli hujumlar) tushunchasi, ularni keltirib chiqarayotgan sabablar va ushbu jinoyatni kvalifikatsiya masalalari yoritiladi.

Kalit so‘zalar: Raqamli iqtisodiyot, Kiberhujum, Raqamli hujum, Raqamli texnologiya, Kripto-aktivlar, Bitcoin, Kriptovalyutalar, kompyuter texnologiyalar, Sun’iy intellekt, jinoyat tarkibi (elementi).

**PREVENTION OF CYBERCRIME IN THE PROCESS OF DEVELOPING
THE DIGITAL ECONOMY IN THE REPUBLIC OF UZBEKISTAN
ABSTRACT**

This article today will highlight the risks in the process of digitizing the economy and developing the sphere of crypto-asset turnover based on statistics. The concept of cyberattacks (digital attacks), the reasons that cause them and the issues of qualification of this crime are covered.

Keywords: Competitive Economy, Cyber-attack, Digital Attack, Digital Technology, Crypto-assets, Bit coin, Crypto currencies, Computer Technology, Artificial Intelligence (IT), Crime composition (element).

**ПРОФИЛАКТИКА КИБЕРПРЕСТУПНОСТИ В ПРОЦЕССЕ РАЗВИТИЯ
ЦИФРОВОЙ ЭКОНОМИКИ В РЕСПУБЛИКЕ УЗБЕКИСТАН
АННОТАЦИЯ**

В данной статье на основе статистических данных будут освещены риски в процессе оцифровки экономики и развития сферы обращения криптоактивов на сегодняшний день. Будет освещена концепция кибератак (цифровых атак), причины, которые их вызывают, и освещаются вопросы квалификации данного преступления.

Ключевые слова: Цифровая экономика, Кибератака, Цифровая атака, Цифровые технологии, Биткойн, Криптовалюты, Компьютерные Технологии, Искусственный Интеллект, Состав преступления (элемент).

KIRISH:

2020 yilning “Ilm, ma’rifat va raqamli iqtisodiyotni rivojlantirish yili” deb e’lon qilinishi yangilanayotgan O‘zbekistondagi islohotlarni sifat jihatdan yangi bosqichga ko’tarishga yo’naltirilgan. Prezidentimizning Murojaatnomasida ta’kidlaganidek, “biz O‘zbekistonni rivojlangan mamlakatga aylantirishni maqsad qilib qo‘ygan ekanmiz, bunga faqat jadal islohotlar, ilm-ma’rifat va innovatsiya bilan erisha olamiz¹. Shundan keyin fuqarolarda “raqamli iqtisodiyot” atamasi haqida ko‘plab savollar tug‘ila boshladi.

O‘zbekiston Respublikasi Prezidentining 2020 – yil 5 – oktyabrdagi PF-6079-sonli “Raqamli O‘zbekiston — 2030” strategiyasini tasdiqlash va uni samarali amalga oshirish chora-tadbirlari to‘g‘risida” Farmoni 17 – bandi 2 – qismiga ko‘ra, iqtisodiyot tarmoqlarida virtual va to‘ldirilgan reallik, sun’iy intellekt, kriptografiya, mashina o‘rganishi, katta ma’lumotlarni tahlil qilish va “bulutli” hisoblash texnologiyalaridan foydalanish imkoniyatlarini o‘rganish va ularni amaliyotga tatbiq etish².

Ushbu normativ huquqiy hujjatda keltirilgan asosiy tushunchalardan biri sun’iy ong, sun’iy intellekt yoki sun’iy idrok (inglizcha: Artificial intelligence; odatda, AI sifatida ham qisqartiriladi) — insonlar yoki hayvonlar tomonidan ko‘rsatiladigan tabiiy ongdan farqli o‘laroq, mashinalar tomonidan ko‘rsatiladigan ongdir. Yetakchi sun’iy ong darslik kitoblari bu sohani „ongli agentlar“ni o‘rganish deya ta’riflaydi: o‘z muhitini fahmlaydigan va maqsadlariga muvaffaqiyatli erishish imkoniyatini maksimal darajada oshiradigan amallarni amalga oshiruvchi har qanday sistema. Xalq orasida „sun’iy ong“ atamasi ko‘pincha „o‘rganish“ va „muammolarni yechish“ kabi inson idroki bilan bog‘laydigan „kognitiv“ funksiyalarni taqlid qiladigan mashinalarni tasvirlashda ishlatiladi, biroq bu ta’rifni yirik sun’iy ong tadqiqotchilari rad etishadi³.

Shuningdek, O‘zbekiston Respublikasi Prezidentining 2020-yil 5-oktabrdagi PF-6079-son Farmoniga 1-ilova, 2 – bobi 2.5. Axborot texnologiyalari sohasida ta’lim berish va malaka oshirishning ustuvor yo‘nalishlari bo‘limining 2 – qismi 2 – baniga ko‘ra, iqtisodiyotning real sektorida raqamlashtirishning istiqbolli sohalarida yangi

¹ Yangilanayotgan O‘zbekistonning ustuvor yo‘nalish va vazifalari. <http://insonhuquqlari.uz/oz/news/yangilanayotgan-ozbekistonning-ustuvor-yonalish-va-vazifalari>;

² O‘zbekiston Respublikasi Prezidentining “Raqamli O‘zbekiston — 2030” strategiyasini tasdiqlash va uni samarali amalga oshirish chora-tadbirlari to‘g‘risida” 05.10.2020 yildagi PF-6079-son Farmoni 17 – bandi 2 – qism. <https://lex.uz/ru/docs/-5030957>;

³ Vikepediya Ochiq Ensklepediya. https://uz.wikipedia.org/wiki/Sun%CA%BCiy_intellekt.

yutuqlar muhokamasi bo'yicha tadbirlarni (forumlar, seminarlar, konferensiyalar va boshqalar) o'tkazish⁴;

Yuqorida keltirilgan normativ huquqiy hujjtning asosiy maqsadi butun duyo miqiyosidagi bugungi kunda iqtisodiyotni raqamlashtirish jarayonlari jadal suratda o'sib borayotgan bir vaqtda O'zbekiston Respublikasida ham turli xildagi sohalarni, xususan, iqtisodiyot sohasini raqamlashtirish hisoblanadi.

Yangiliklar bilan hamohang yashaydigan insonlar biladiki, rivojlanayotgan mamlakatlarning rivojlanish strategiyalarida ko'pincha bir so'zga duch kelish mumkin - raqamlashtirish. Hozirda dunyoda raqamlashtirish jarayoni ketmoqda, rivojlanayotgan va rivojlangan mamlakatlar bu jarayondan juda yaxshi foydalangan holda o'zlarini iqtisodlarini rivojlantirib, mamlakatlarida yangi ish o'rinlarini barpo etishmoqda. Savol tug'iladi: xo'sh raqamlashtirish o'zi nima va uning ahamiyati nimada?

Raqamlashtirish – iste'molchilar, korxonalar va hukumatlar tomonidan qabul qilingan o'zaro bog'langan raqamli xizmatlarning ommaviy o'zlashtirilishi. Hozirda dunyoda, asosan rivojlangan va rivojlanayotgan mamlakatlarda, raqamlashtirish jarayoni juda ildamlik bilan davom etmoqda. Mamlakatlar kundan-kunga o'z iqtisodiyotlarni raqamlashtirib borishmoqda, raqamlashtirish hozirgi kunda dunyoda iqtisodiy rivojlanishning asosiy drayverlaridan biriga aylanib bormoqda. Misol uchun, tahlilchilar hisoblashicha, atigi 10 yildan biroz ko'proq vaqt oldin, ya'ni 2011-yilda (raqamlashtirishning ahamiyati endigina xalqaro hamjamiyat tomonidan e'tirof etila boshlangan davrda) uning xalqaro iqtisodiyotga 193 milliard dollar atrofida foyda keltirgan va 6 milliondan ortiq ish o'rinlari yaratilishiga sababchi bo'lgan. Bundan keyingi yillarda esa bu raqamlar asosan o'sib borgan. Shundan kelib chiqish mumkinki, hozirda dunyoda iqtisodiy rivojlanish va yangi ish o'rinlari yaratish bo'yicha eng asosiy omil aynan raqamlashtirish bo'lib kelmoqda.

Raqamlashtirish haqida qisqa qilib aytadigan bo'lsak, biz analogdan raqamli ma'lumotlarga, vositalarga, ommaviy axborot vositalariga va qurilmalarga o'tish jarayonini nazarda tutamiz. Ushbu jarayonga misol sifatida qog'oz hujjatlar o'rniga matnli fayllardan foydalanish, an'anaviy pochta o'rniga elektron pochtdan (@gmail.com) foydalanish, analoglar o'rniga raqamli mediadan foydalanish va boshqalar kiradi. Raqamli transformatsiya narsalar Interneti, sun'iy intellekt (AI), virtual va kengaytirilgan reallik kabi yangi va tobora ilg'or texnologiyalarni joriy etish orqali amalga oshirilmoqda.

O'zbekiston Respublikasi ham raqamli iqtisodiyotga o'tar ekan, o'z-o'zidan mamlakat iqtisodiyotida yangi toifadagi internetga asoslangan bizneslar ko'payib

⁴ O'zbekiston Respublikasi Prezidentining "Raqamli O'zbekiston — 2030" strategiyasini tasdiqlash va uni samarali amalga oshirish chora-tadbirlari to'g'risida" 05.10.2020 yildagi PF-6079-son Farmoni 2 – bobi 2.5. bo'lim. <https://lex.uz/ru/docs/-5030957>.

bormoqda. Bular jumlasiga turli xil internet do‘konlari orqali turli xildagi tovarlarning xaridlari, turli xildagi yetkazib berish (eltuv) xizmatlari, onlayn kurslar, masofaviy ta’lim va shunga o‘xshash yangidan-yangi bizneslar ko‘payib bormoqda. Shu bilan birga, an’anaviy shakldagi (offline) tadbirkorlik subyektlari ham tabiiyki, internetdan foydalanishga majbur bo‘layotganligining sababi soliq hisobotari va shunga o‘xshash hujjatlar O‘zbekiston Respublikasi Yagona interaktiv davlat xizmatlari portali (*my.gov.uz*) orqali topshirishga o‘tildi. Amalga oshirilayotgan ushbu o‘zgarishlar davlat, yuridik va jismoniy shaxslarga bir qancha qulayliklar yaratish bilan bir qatorda, quyida turli xildagi muammolar va xavflarni keltirib chiqarmoqda:

“Telegram” ijtimoiy tarmog‘ida e‘lon qilingan hamda buzilgan ma‘lumotlar bazasini o‘rganish jarayonida mutaxassislar tomonidan 2023-yil 18-oktabr sanasida 200 mingdan ortiq foyalanuvchi ma‘lumotlari sizdirilganligi aniqlandi. Ularning aksariyati dolzarb ahamiyatga ega bo‘lib, davlat organlari va boshqa tashkilotlarning axborot tizimlari xavfsizligiga kibertahdidlarini keltirib chiqarmoqda. So‘nggi paytlarda foydalanuvchining oshkor qilingan ma‘lumotlar bazasining bunday holatlari tez-tez uchrab turibdi. Ilgari bunday ma‘lumotlar sizib chiqishi faqat yopiq forumlarda yoki Darknet-da uchrab turar edi⁵.

Ijtimoiy tarmoqlarda 200 mingdan ortiq O‘zbekistonlik foydalanuvchilarning sizdirilgan parollari – *OneID, DTM, ko‘plab davlat va ta’lim tashkilotlari, qidiruv va to‘lov tizimlariga aloqador*. Kiberxavfsizlik markazi bu axborot tizimlari xavfsizligiga kibertahdidlarni keltirib chiqarayotganini ta’kidladi va parollarni asrash bo‘yicha foydalanuvchilarga maslahatlar berdi. Bu xavf - kiberhujumlar (raqamli hujumlar) bo‘lib, buning natijasida, internet orqali pul o‘tazmalari, davlat va tijorat sirlari, fugarolarning daxlsizligi xavf ostida qolishi mumkin⁶.

Yuqoridagilardan kelib chiqqan holda shuni aytishimiz muminki, iqtisodiyotning ragamlashuvi davlat, yuridik shaxslar va jismoniy shaxslarga keng imkoniyatlar yaratib berishi bilan birgalikda ularga yuqoridagi bir qancha kiber – hujumlar (raqamli hujumlarni) keltirib chiqarmoqda. Buning natijasida esa, internet orqali online pul o‘tkazmalari, davlat va tijorat sirlari, fugarolarning shaxsiy daxlsizligi xavf ostida qolmoqda.

Mustaqil izlanuvchi Michael Aaron Dennis ning “cybercrime” nomli maqolasida keltirilishacha Kiberjinoyatni kompyuter yordamidagi jinoyati qamrab oluvchi keng qamrovli atama sifatida ko‘rish mumin. Kiberjinoyatchilik, kompyuterdan jinoyat

⁵ “Kiberxavfsizlik markazi” davlat unitar korxonasi. Turli axborot resurslariga tegishli bo‘lgan foydalanuvchilar ma‘lumotlari e‘lon qilinganligi aniqlandi. <https://csec.uz/uz/news/maqolalar/turli-axborot-resurslariga-tegishli-bo-lgan-foydalanuvchilar-ma-lumotlari-e-lon-qilinganligi-aniqlan/>;

⁶ Kun.uz rasmiy manbasi. Misli ko‘rilmagan kiberhujum: hakerlar 200 mingdan ortiq o‘zbekistonlik foydalanuvchilarning login-parollarini sizdirdi. <https://kun.uz/uz/news/2023/10/20/misli-korilmagan-kiberhujum-hakerlar-200-mingdan-ortiq-ozbekistonlik-foydalanuvchilarning-login-parollarini-sizdirdi>.

vositasi sifatida foydalangan holda firibgarlik, bolalar pornografiyasi va intellektual mulk savdosi, shaxsni o'g'irlash yoki shaxsiy hayotni buzish kabi noqonuniy xatti harakatlarni sodir etish tushuniladi. Kiberjinoyatchilik, ayniqsa Internet orqali, kompyuter online tijoratda markaziy o'rinni egalladi va ahamiyati oshdi⁷.

Ko'plab xorijiy adabiyotlarda kiberjinoyatning obyektini asosan ikki guruhga bo'lishadi. Barcha kiberjinoyatlar kompyuterni ham, uning orqasidagi odamni ham jinoyat obyekti (qurbon) sifatida jalb qilishi mumkin. Ushbu jinoyatning asosiy obyektini aniqlashda kiberhujumni sodir etayotgan subyektning asosiy maqsadi nimaga qaratilganligiga bog'liq, ya'ni jinoyat obyekti kompyuterni ham, uning orqasidagi odamni ham bo'lishi mumkin. Misol uchun, bir necha xorijiy adabiyotlarda ushbu jinoyat obyekti ikki turga bo'linadi:

1. Kiberhujumni sodir etayotgan shaxs e'tibori nimaga qaratilganligi, bular kompyuter ma'lumotlari va boshqa ma'lumotlarga hujum qilishni maqsad qilib olganligi.

2. Kiberhujumni sodir etayotgan shaxsning maqsadi, ta'qib qilinayotgan shaxsning shaxsiy ma'lumotlariga (shaxsiy dahlsizligiga) hujum qilishni o'z ichiga olishi mumkin.

Kiberjinoyatlar boshqa turdagi jinoyatlardan ancha farq qiladi, chunki ularni aniqlash, tergov qilish va jinoiy javobgarlikka tortish ko'pincha qiyin va shu sababli kiber jinoyatlar boshqa turdagi jinoyatlarga qaraganda jamiyatga katta zarar yetkazadi. Kiber jinoyatchilikka internet yoki boshqa har qanday kompyuter texnologiyalari orqali amalga oshiriladigan alohida jinoyat tarkibiga ega bo'lgan ijtimoiy xavfli qilmishlar ham kiradi. Masalan: firibgarlik (qalbakilashtirish), o'g'irlik va shunga o'xshash jinoyatlar kompyuter texnikasi va internetdan foydalanish orqali sodir etilgan bo'lsa, kiber jinoyatlar hisoblanadi⁸.

Kiberjinoyatlar obyekti – asosan, jismoniy shaxslar (shaxsiy dahlsizlik), davlat xavfsizligi va mollyaviy bargarorligi, shu bilan birga biznes tashkilotlarining normal faoliyati hamda tijorat sirlari bo'ladi.

Mazkur jinoyat subyektlari hakerlar deb atalgan va odatda yugori malakaga ega bolgan komputer mutaxassislari sanaladi. Shuning uchun ko'plab davlatlar o'zining kiberxavfsizlik tizimiga yuqori darajadagi kompyuter mutaxassislarini jalb qilishni istashadi.

Kiberjinoyatlar subyektiv tomoni – kiberhujumni sodir etgan ijtimoiy xavfli qilmish va uning uning oqibatlariga bo'lgan ruhiy munosabatlarini ko'rsatadi. Ya'ni ushbu jinoyat turi yuqori malakali IT bilimlarga ega bo'lgan shaxslar tomonidan sodir

⁷ History & Society. Cybercrime. Law. Michael Aaron Dennis. <https://www.britannica.com/topic/cybercrime/ATM-fraud>.

⁸ Cyber-crimes. 5.1 objectives. <https://egyankosh.ac.in/bitstream/123456789/73775/1/Unit-5.pdf>

etilganligi sababli, ushbu turdagi jinoyatning har doim maqsadi aniq bo‘ladi va u qasddan sodir etiladi.

Kiberjinoyatlar obyektiv tomoni – kiberhujum amalga oshirilishi natijasida kelib chiqadigan oqibatlar o‘rtasidagi sababli bog‘lanish, shuningdek, uning fakultativ belgilar: kiberhujum sodir etilgan joy, vaqt, usul, sharoiti, jinoyatni amalga oshirish quroli va vosita singari belgilardan iborat.

Jinoyat quroli – internet va eng so‘nggi raqamli texnologiyalar. Mamlakatning harbiy, strategik tarmoqlarini ishdan chiqarish salohiyatiga ega⁹.

Ushbu turdagi jinoyat odatda, kompyuter texnika sohasida yuqori malakaga ega bo‘lgan kiberjinoyatning o‘ziga xosligi shundaki, mazkur jinoyatda ustunlik buzg‘unchi jinoyatchilar qo‘lida bo‘ladi. Negaki, bunday jinoyatni fosh qilish juda qiyin va murakkab sanaladi. Shu bois bunday jinoyatlar odatda laten jinoyatlar qatoriga kiritiladi.

Expert intelning 2023 yil 23 avgustdagi maqolasida keltirilishicha, Jahon Iqtisodiy Forumi (WEF) ma‘lumotlariga ko‘ra, kiberjinoyatchilik asosan AQSh va Xitoyning ortda qoldirib, dunyodagi uchinchi yirik iqtisodiyotga aylandi.

Cybersecurity Ventures, uning ta‘siri 2025 yilga borib 10,5 trillion dollarga yetishi haqidagi loyihalar Tarmoqlar va to‘lov dasturlariga onlayn kirishning mavjudligi ushbu eksponensial o‘shishni boshqarishda hal qiluvchi rol o‘ynadi va bu qulaylik turli darajadagi texnik tajribaga ega bo‘lgan shaxslar uchun murakkab kiber va to‘lov dasturlari hujumlarini boshlash uchun eshiklarni ochdi.

Global iqtisodiyotga zararli ta‘sir: Har qanday o‘g‘irlikda bo‘lgani kabi, yo‘qotishlar ham bo‘ladi... Ajablanarlisi shundaki, kiberjinoyat global iqtisodiyotga salbiy ta‘sir ko‘rsatmoqda. Biznes yo‘qotishlar o‘shishda davom etmoqda va iqtisodiy yutuqlar o‘shishda davom etmoqda - hatto Tesla, Facebook, Microsoft, Apple, Amazon va Walmart kabi texnologiya gigantlarining yillik daromadlari 1,28 trillion dollarni tashkil etadi.

2023-yil asosiy yo‘llari – hozirgacha, yuqori hujumlar yili bo‘lib qolmoqda. 2020-yilda kiberhujumlar davlat va xususiy sektorda keng tarqalgan xavf-xatar bo‘yicha beshinchi o‘rinni egalladi. Bu yuqori xavfli landshaft saqlanib qolmoqda va 2023 yilga kelib IoT kiberhujumlari 2025 yilga kelib ikki baravar ko‘payishi prognoz qilinmoqda. Jahon iqtisodiy forumining 2020 yilgi Global xavf hisoboti ushbu tahdidlarni aniqlash yoki ta‘qib qilishning atigi 0,05 foizini ko‘rsatib, muammoni ta‘kidlaydi.

Dunyo Twitter kabi tashkilotlarga qarshi to‘g‘ridan-to‘g‘ri hujumlarni ko‘rdi, bu bugungi kunga qadar eng muhim ma‘lumotlarning sizib chiqishiga olib keldi va JD

⁹ Kiberjinoyatlar - yangi zamon, yangi muammo. <https://www.amerikaovozi.com/a/a-36-2010-03-26-voa1-93371769/807021.html>.

Sports buzilgan serverlari 10 million mijozning onlayn buyurtma ma'lumotlarini oshkor qilgan¹⁰.

Internet Security Alliance kiberxavfsizlik yuzasidan quyidagilarni ma'lumotlarni keltiradi:

1. Yomon xabar: siz kiberxavfsizlik muammosini “hal qila olmaysiz”;
2. Yaxshi xabar: siz kiberxavfingizni boshqarishingiz mumkin;
3. Kiberxavfsizlik haqida shaxsiy sog'lig'ingiz haqida o'ylaganingizdek o'ylang, hech kim mikrobsiz yashamaydi¹¹.

“Masalani qay jihatidan olib qaramang, ustunlik buzg'unchi-jinoyatchilar tomonida”, - deydi ekspert Larri Klinton. “Qonunlar sust. Sohoni yashi biladigan mutaxassislar kam. Xurujlarni uyushtirish oson va arzon. Qo'lidan kelgan odam katta mukofot oladi”.

Birlashkan millatlar tashkiloti ham ushbu turdagi jinoyatni transmilliy jinoyatlar qatorida hisoblaydi. Shuningdek, kiberhujumning chegarasiz hududida sodir bo'ladigan jinoyatning murakkab tabiati uyushgan jinoyatchilik guruhlarining tobora ko'proq jalb etilishi bilan kuchaymoqda. Kiberjinoyatchilar va ularning qurbonlari turli mintaqalarda joylashgan bo'lishi mumkin va uning ta'siri butun dunyo bo'ylab jamiyatlar orqali tarqalib, shoshilinch, dinamik va xalqaro javob choralari ko'rish zarurligini ta'kidlaydi. Ya'ni ushbu jinoyat muayyan mintaqada doirasida qamrab olgani emas, balki universal landshaft doirasida sodir bo'lmoqda.

UNODC milliy tuzilmalar va harakatlarni qo'llab-quvvatlash orqali kiberjinoyatchilikka qarshi kurashda uzoq muddatli va barqaror salohiyatni oshirishga yordam beradi. Xususan, UNODC salohiyatni oshirish, profilaktika va xabardorlikni oshirish, xalqaro hamkorlik va kiberjinoyatchilik bo'yicha ma'lumotlar yig'ish, tadqiqotlar va tahlil qilishda texnik yordam ko'rsatish uchun jinoiy Adliya tizimlariga javob berish bo'yicha ixtisoslashgan tajribasidan foydalanadi¹².

Hozirgi kunda Bitcoin, Cirus Foundation, Terra classic va boshqalar kabi kriptovalyuta bilan bog'liq bo'lmagan yoki uning yordam amalga oshirilmagan biror – bir jinoyat turini tasavvur qilishimiz qiyin bo'lib bormoqda. 2023 yil yanvar holatiga ko'ra, 22.000 dan ortiq kriptovalyutalar mavjud, Bitcoin hali ham umumiy kriptovalyuta bozor qiymatining 41% atrofida saqlanadi. Bitkoin kriptovalyutasi

¹⁰ Expert Intel. Cybercrime is world's third-largest economy. Published: August 23, 2023. [https://stripeolt.com/knowledge-hub/expert-intel/cybercrime-is-worlds-third-largest-economy/#:~:text=our%20interconnected%20world.According%20to%20the%20World%20Economic%20Forum%20\(WEF\)%2C%20cybercrime%20has,reach%20%2410.5%20trillion%20by%202025%E2%80%A6](https://stripeolt.com/knowledge-hub/expert-intel/cybercrime-is-worlds-third-largest-economy/#:~:text=our%20interconnected%20world.According%20to%20the%20World%20Economic%20Forum%20(WEF)%2C%20cybercrime%20has,reach%20%2410.5%20trillion%20by%202025%E2%80%A6).

¹¹ Internet Security Alliance. https://chapters.acp-international.com/images/newyorkcitymetro/ACO_NY_Metro-7-19-17.pdf;

¹² United Nations Office on Drugs and Crime. Cybercrime. <https://www.unodc.org/romena/en/cybercrime.html>.

kiberjinoyatchilarning eng sevimli va ishonchli valyutasi hisoblanadi. Avstraliya universitetlari tadqiqotiga ko'ra, yillik nolegal daromadlarning 76 milliard AQSh dollari miqdori bitkoinlar orqali olinadi (jami bitcoin otkazmalarining 46 foizi). Bu esa AQSh va Yevropa bozorlaridagi narkotik savdosining yillik qiymatiga teng¹³.

Yuqoridagi tashqari raqamli iqtisodiyot keltirib chiqarishi mumkin bo'lgan xavflar quyidagilar hisoblanadi:

1. Yuqorida ta'kidlanganidek, kiberhujum xavfi, shaxsiy ma'lumotlar himoyasi bilan bog'liq muommolar;
2. "Raqamli qullik" (millionlab insonlar ma'lumotlaridan keyinchalik ularni o'zlarini tutishini boshqarish uchun foydalanish);
3. Ishsizlikni oshishi, axborot texnologiyalarini rivojlanishi va uni tadbiiq qilinishi ortidan bir qancha sohalar va kasblar yo'q bo'lib ketishi mumkin.

Yuqoridagilardan kelib chiqqan holda shuni xulosa qilish mumkinki, mamlakat raqamli iqtisodiyotga o'tishdan avval raqamli xavfsizlik tizimini ishlab chiqishi va jinoyat qonunchiligini ham ushbu tizimga moslab olishi lozim. Yuqorida ushbu soha yuzasidan xalqao mutaxassis Larri Klinton ta'kidlaganidek, "Masalani qay jihatidan olib qaramang, ustunlik buzg'unchi-jinoyatchilar tomonida", "Qonunlar sust. Sohani yashi biladigan mutaxassislar kam. Xurujlarni uyushtirish oson va arzon. Qo'lidan kelgan odam katta mukofot oladi". Shunday ekan, doimo orqada yurgan qonunchilik va kiberxavfsizlikdan doim bir qadam oldinda yurgan kiberjinoyatchilarga yeta olmaydi. Kiberxavfsizlik bo'yicha mustahkam tizimini yaratish va kiberjinoyatlar yuzasidan jinoiy javobgarliklarni mukammal ishlab chiqish kerak. Ushbu jinoyatlarni oldini olish va qarshi kurashish yuzasidan aholini huquqiy ongini oshirish, maktab, kollej, texnikumlar va oliy o'quv yurtlariga yuqori IT bilimlarga ega bo'lgan mutaxassislarni jalb qilgan holda yuqori malakali o'quv kurslarini doimiy ravishda olib borishdan iborat. Yuqorida ta'kidlab o'tilganidek, ushbu jinoyatlarni oldini olish va unga qarshi kurashish yuzasidan normativ huquqiy hujjatlarni ishlab chiqaruvchi yuridik sohadagi kadrlarni ham yuqori darajadagi kompyuter savoxonligi sohasidagi bilimlarini oshirib borish lozim. Shundagina, ragamli iqtisodiyot sharoitida kiberjinoyatlardan oson himoyalanish mumkin bo'ladi.

References:

1. O'zbekiston Respublikasi Prezidentining "Raqamli O'zbekiston — 2030" strategiyasini tasdiqlash va uni samarali amalga oshirish chora-tadbirlari

¹³ CRIME AND CRYPTOCURRENCY IN AUSTRALIAN COURTS. AARON M LANE* AND LISANNE ADAM**. [file:///C:/Users/User/Downloads/5.%20Lane%20and%20Adam%20\(2022\)%2048\(3\)%20MonULR%20146.pdf](file:///C:/Users/User/Downloads/5.%20Lane%20and%20Adam%20(2022)%2048(3)%20MonULR%20146.pdf).

- to'g'risida" 05.10.2020 yildagi PF-6079-son Farmoni 17 – bandi 2 – qism.
<https://lex.uz/ru/docs/-5030957>;
2. O'zbekiston Respublikasi Prezidentining "Raqamli O'zbekiston — 2030" strategiyasini tasdiqlash va uni samarali amalga oshirish chora-tadbirlari to'g'risida" 05.10.2020 yildagi PF-6079-son Farmoni 2 – bobi 2.5. bo'lim.
<https://lex.uz/ru/docs/-5030957>;
 3. Turli axborot resurslariga tegishli bo'lgan foydalanuvchilar ma'lumotlari e'lon qilinganligi aniqlandi. <https://csec.uz/uz/news/maqolalar/turli-axborot-resurslariga-tegishli-bo-lgan-foydalanuvchilar-ma-lumotlari-e-lon-qilinganligi-aniqlan>;
 4. Misli ko'rilmagan kiberhujum: hakerlar 200 mingdan ortiq o'zbekistonlik foydalanuvchilarning login-parollarini sizdirdi.
<https://kun.uz/uz/news/2023/10/20/misli-korilmagan-kiberhujum-hakerlar-200-mingdan-ortiq-ozbekistonlik-foydalanuvchilarning-login-parollarini-sizdirdi>;
 5. History & Society. Cybercrime. Law. Michael Aaron Dennis.
<https://www.britannica.com/topic/cybercrime/ATM-fraud>;
 6. Cyber-crimes. 5.1 objectives.
<https://egyankosh.ac.in/bitstream/123456789/73775/1/Unit-5.pdf>;
 7. Kiberjinoyatlar - yangi zamon, yangi muammo.
<https://www.amerikaovozi.com/a/a-36-2010-03-26-voa1-93371769/807021.html>;
 8. Expert Intel. Cybercrime is world's third-largest economy. Published: August 23, 2023. [https://stripeolt.com/knowledge-hub/expert-intel/cybercrime-is-worlds-third-largesteconomy/#:~:text=our%20interconnected%20worldAccording%20to%20the%20World%20Economic%20Forum%20\(WEF\)%2C%20cybercrime%20has,reach%20%2410.5%20trillion%20by%202025%E2%80%A6](https://stripeolt.com/knowledge-hub/expert-intel/cybercrime-is-worlds-third-largesteconomy/#:~:text=our%20interconnected%20worldAccording%20to%20the%20World%20Economic%20Forum%20(WEF)%2C%20cybercrime%20has,reach%20%2410.5%20trillion%20by%202025%E2%80%A6);
 9. Internet Security Alliance. https://chapters.acp-international.com/images/newyorkcitymetro/ACO_NY_Metro-7-19-17.pdf;
 10. United Nations Office on Drugs and Crime. Cybercrime.
<https://www.unodc.org/romena/en/cybercrime.html>;
 11. CRIME AND CRYPTOCURRENCY IN AUSTRALIAN COURTS. AARON M LANE* AND LISANNE ADAM**.
[file:///C:/Users/User/Downloads/5.%20Lane%20and%20Adam%20\(2022\)%2048\(3\)%20MonULR%20146.pdf](file:///C:/Users/User/Downloads/5.%20Lane%20and%20Adam%20(2022)%2048(3)%20MonULR%20146.pdf);
 12. Cybercrime magazine. Cybercrime To Cost The World \$10.5 Trillion Annually By 2025. <https://cybersecurityventures.com/hackerpocalypse-cybercrimereport2016/#:~:text=Cybersecurity%20Ventures%20expects%20global%20cybercrime,%243%20trillion%20USD%20in%202015>.