JOURNAL OF INTERNATIONAL SCIENTIFIC RESEARCH
Volume 5, Issue 1, November 2026 Online ISSN: 3030-3508
https://spaceknowladge.com

RAQAMLI IQTISODIYOT VA SUN'IY INTELLEKT DAVRIDA KIBERJINOYATLARNI KVALIFIKATSIYA QILISHNING DOLZARB MUAMMOLARI

Saliyeva Muxlisa Mansur qizi
Toshkent davlat yuridik universiteti magistranti
Moliyaviy-huquqiy monitoring yo'nalishi
Ilmiy darajasi: magistrant
Elektron pochta: mukhlisasaliyeva.gmail.com

.

ИНФОРМАЦИЯ О СТАТЬЕ

ИСТОРИЯ СТАТЬИ:
Received:16.11.2026
Revised: 17.11.2026
Accepted:18.11.2026

КЛЮЧЕВЫЕ СЛОВА:
kiberjinoyat, jinoyatlarni tasniflash, Jinoyat kodeksi, Budapesht konvensiyasi, virtual aktivlar, deepfake, muhim axborot infratuzilmasi, kiberxavfsizlik.

АННОТАЦИЯ:

Maqolada kiberjinoyatlarning huquqiy tabiati, tasnifi va ularga qarshi kurashni takomillashtirish masalalari O'zbekiston Respublikasi Jinoyat kodeksi, «Kiberxavfsizlik to'g'risida»gi Qonun, Budapesht konvensiyasi hamda Yevropa Ittifoqi, AQSH va Singapur qonunchiligi asosida tahlil qilinadi. Kiberjinoyatlarning to'rt guruhli tasnifi milliy normalar va Budapesht konvensiyasi tuzilmasi bilan solishtiriladi, kiberjinoyatchi shaxsining tiplari va kriminogen motivatsiya darajalari ajratiladi. Qonunchilikdagi bo'shliqlar (atamalar, virtual aktivlar, deepfake, elektron dalillar, javobgarlik yoshi) aniqlanib, Jinoyat kodeksiga o'zgartirishlar kiritish va muhim axborot infratuzilmasini himoya qilish bo'yicha takliflar asoslanadi. Takliflar 2025–2026-yillardagi milliy islohotlar hamda O'zbekistonning Budapesht konvensiyasiga qo'shilish va Birlashgan Millatlar Tashkilotining Kiberjinoyatchilikka qarshi konvensiyasi bo'yicha qadamlari kontekstida ko'rib chiqiladi. Axborot texnologiyalari orqali sodir etilgan jinoyatlar soni 2019-yildagi 863 tadan 2024-yilda 58 800 taga yetgani qayd etiladi. Muallif Jinoyat kodeksiga «Kiber-firibgarlik» va raqamli qiyofaga tajovuz bo'yicha yangi normalarni kiritish, virtual aktivlarni «o'zganing mulki» tushunchasiga qo'shish hamda javobgarlik yoshini pasaytirishni (gipoteza sifatida) taklif

etadi. Olingan natijalar konseptual xarakterga ega bo‘lib, kelgusida sud amaliyoti tahlili bilan to‘ldirilishi lozim.

KIRISH (INTRODUCTION)

Davlat boshqaruvi, bank-moliya tizimi va kundalik muloqotning raqamlashuvi jinoyatchilik uchun yangi muhit yaratdi. Ichki ishlar vazirligi ma’lumotlariga ko‘ra, axborot texnologiyalari orqali sodir etilgan jinoyatlar 2019-yildagi 18 turdagi 863 tadan 2024-yilda 62 turdagi 58 800 taga yetgan[26]. Bu taxminan 68 baravar o‘sish. Davlat siyosati ham bu tahdidga javob berib bormoqda: 2025-yil 30-apreldagi PQ-153-son Prezident qarori axborot texnologiyalari yordamida sodir etiladigan jinoyatlarga qarshi kurashni kuchaytirishga qaratilgan[27], 2026-yil 10-martdagi PF-38-son Farmon bilan 2026–2030-yillarga mo‘ljallangan Kiberxavfsizlik strategiyasi tasdiqlandi va kiberjinoyatchilikning oldini olish tizimini takomillashtirish vazifasi belgilandi[28]. Xalqaro Elektr Aloqa Ittifoqining Global kiberxavfsizlik indeksi (2024, beshinchi nashr) davlatlarni besh darajali model bo‘yicha baholaydi[29]; O‘zbekiston 89,2 ball bilan «T2 Advancing» toifasiga kiritilgan[30], avvalgi nashrdagi ko‘rsatkichi esa 71,11 ball bo‘lgan[31].

Ko‘rsatkichlarning yaxshilanishi jinoyat-huquqiy tasnifdagi noaniqliklarni yo‘qotmaydi. «Kiberjinoyat», «kompyuter jinoyati» va «axborot texnologiyalari sohasidagi jinoyat» tushunchalari ilmiy adabiyotda ko‘pincha sinonim sifatida ishlatiladi, Jinoyat kodeksida esa faqat XX¹ bob «Axborot texnologiyalari sohasidagi jinoyatlar» deb nomlangan[32]. Natijada bir xil qilmish amaliyotda turlicha kvalifikatsiya qilinishi mumkin. Kiberjinoyatlarning

[26] . Ichki ishlar vazirligi Tezkor-qidiruv departamenti Kiberxavfsizlik markazi faoliyatiga bag‘ishlangan press-tur. (2025, 29-may). O‘zbekiston Respublikasi hukumat portali (gov.uz). https://gov.uz/oz/iiv/news/view/57775

[27] O‘zbekiston Respublikasi Prezidenti. (2025, 30-aprel). Axborot texnologiyalari yordamida sodir etiladigan jinoyatlarga qarshi kurashish faoliyatini yanada kuchaytirishga qaratilgan chora-tadbirlar to‘g‘risida (PQ-153-son Qaror). https://lex.uz/en/docs/-7511145

[28] O‘zbekiston Respublikasi Prezidenti. (2026, 10-mart). O‘zbekiston Respublikasining Kiberxavfsizlik strategiyasini belgilash va kiberjinoyatchilikning oldini olish tizimini takomillashtirish to‘g‘risida (PF-38-son Farmon). https://lex.uz/uz/docs/-8079286

[29] International Telecommunication Union. (2024). Global Cybersecurity Index 2024 (5th ed.). ISBN 978-92-61-38751-8. https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv5/2401416_1b_Global-Cybersecurity-Index-E.pdf

[30]Uzbekistan improves its position in global cybersecurity index. (2024, 14-sentabr). Kun.uz. https://kun.uz/en/news/2024/09/14/uzbekistan-improves-its-position-in-global-cybersecurity-index

[31] Uzbekistan recognized as a country with developing cybersecurity. (2024, 16-sentabr). UzDaily. https://uzdaily.ru/en/uzbekistan-recognized-as-a-country-with-developing-cybersecurity

[32] . O‘zbekiston Respublikasi. (1994, 22-sentabr). O‘zbekiston Respublikasining Jinoyat kodeksi (2012-XII-son), XX¹ bob. https://lex.uz

huquqiy tabiatini va tasnifini tahlil qilish hamda kurash samaradorligini oshirish bo‘yicha asoslangan takliflar ishlab chiqish. Tushuncha va tarixiy rivojlanishni aniqlash; tasnifni milliy va xalqaro normalar bilan solishtirish; jinoyat tarkibi va shaxs tiplarini tavsiflash; qonunchilikdagi bo‘shliqlarni aniqlash; xorijiy tajribadan O‘zbekiston uchun xulosalar chiqarish

Maqolada (a) to‘rt guruhli tasnifning Jinoyat kodeksi va Budapesht konvensiyasi bilan o‘zaro muvofiqlik jadvali beriladi; (b) kiberjinoyatchi shaxsining besh tipi va kriminogen motivatsiyaning to‘rt darajasi ajratiladi; (c) Jinoyat kodeksiga kiritiladigan o‘zgartirishlarga asoslanadi. Bu natijalar konseptual xarakterga ega va sud amaliyoti tahlili bilan to‘ldirilishi kerak.

METODLAR (LITERATURE REVIEW AND METHODS)

Milliy adabiyotda kiberjinoyatchilikka qarshi kurashning jinoyat-huquqiy va kriminologik jihatlari tadqiq etilgan; kiberxavfsizlik, raqamli huquq va raqamli gigiyena o‘zaro bog‘liq holda ko‘rib chiqilgan. Xorijiy adabiyotda kiberjinoyatning kriminologik va raqamli sud-ekspertiza jihatlari tizimli yoritilgan. Ushbu maqola ularni takrorlamaydi: u tasnifni Jinoyat kodeksi va Budapesht konvensiyasi tuzilmasi bilan bog‘laydi va takliflarni 2025–2026-yillardagi islohotlar bilan solishtiradi.

Metodlar. **Formal-yuridik metod** orqali Jinoyat kodeksining XX[1] bobi, firibgarlik va o‘g‘rilik normalari hamda «Kiberxavfsizlik to‘g‘risida»gi Qonundagi tayanch tushunchalar (kiberfazo, kibertahdid, kiberhujum) matn darajasida tahlil qilindi. **Qiyosiy-huquqiy metod** Budapesht konvensiyasi, Yevropa Kengashi tayyorlagan O‘zbekiston huquqiy profili, Yevropa Ittifoqi, AQSH va Singapur normativ hujjatlarini bir xil mezonlar (jinoiy-huquqiy javobgarlik, muhim infratuzilmani himoya qilish, hamkorlik mexanizmi) bo‘yicha solishtirishda qo‘llandi. **Tizimli tahlil** kiberjinoyatni obyekt, obyektiv tomon, subyekt va subyektiv tomon elementlariga ajratish hamda jinoyatchi tiplarini guruhlash uchun ishlatildi. **Tarixiy-huquqiy metod** kiberjinoyatchilikning to‘rt bosqichini (1970–80-yillar; 1990-yillar; 2000–2015-yillar; 2016-yildan keyingi davr) huquqiy muhim sanalar (1986-yildagi AQSH Computer Fraud and Abuse Act, 2001-yildagi Budapesht konvensiyasi, 2022-yildagi O‘RQ-764-son Qonun, 2026-yildagi PF-38-son Farmon) bilan bog‘lash uchun xizmat qildi. **Statistik usul** IIV rasmiy ma’lumotlarini taqqoslash va o‘sish sur’atini hisoblashda qo‘llandi. Normativ hujjatlarning mavjudligi va nomi 2026-yil 4-noyabr holatida ochiq rasmiy manbalarda tekshirildi.

NATIJALAR (RESULTS)

Tasnif va jinoyat tarkibi

Tadqiqot kiberjinoyatlarni to‘rt guruhga ajratadi. 1-jadvalda ularning milliy va xalqaro normalarga mosligi ko‘rsatilgan.

1-jadval. Kiberjinoyatlar guruhlarining milliy va xalqaro normalarga muvofiqligi

Guruh	Mohiyati	Jinoyat kodeksi	Budapesht konvensiyasi

Guruh	Mohiyati	Jinoyat kodeksi	Budapesht konvensiyasi
Texnik (hacking)	tizim va ma’lumotlar daxlsizligiga tajovuz	XX¹ bob	2–6-moddalar (noqonuniy kirish, ushlab qolish, ma’lumotga va tizimga aralashuv, vositalarni noqonuniy qo‘llash)
Iqtisodiy (fraud)	mulkni aldov orqali qo‘lga kiritish	168-modda	7–8-moddalar (kompyuter soxtaligi, kompyuter firibgarligi)
Mazmunli (content)	taqiqlangan axborotni tarqatish	130-, 244¹-moddalar	9-modda (bolalar pornografiyasi)
Intellektual (piracy)	mualliflik huquqini buzish	149-modda	10-modda

Tasnif Budapesht konvensiyasining sarlavhalar tuzilmasini takrorlaydi; maqolaning hissasi uni Jinoyat kodeksi moddalari bilan aniq bog‘lashdadir. Mazmunli jinoyatlar bo‘yicha farq muhim: Konvensiyaning 9-moddasi faqat bolalar pornografiyasini qamrab oladi, irqchilik va ksenofobiya materiallari esa alohida Qo‘shimcha protokolda (ETS 189) tartibga solingan[33].

Kiberjinoyat tarkibining elementlari quyidagicha tavsiflandi. *Obyekt:* umumiy obyekt axborot xavfsizligi (maxfiylik, yaxlitlik, foydalanish imkoniyati) bilan bog‘liq munosabatlar; bevosita obyekt ikki xil: axborot tizimining o‘zi (masalan, DDoS-hujumda) yoki mulkiy va shaxsiy munosabatlar, bunda tizim vosita bo‘ladi (masalan, fishingda). Predmetga elektron ma’lumotlar, login-parollar, to‘lov rekvizitlari va kriptografik kalitlar kiradi. *Obyektiv tomon:* hacking, fishing, DDoS, zararli dasturlar va ijtimoiy muhandislik. *Subyekt:* umumiy qoidaga ko‘ra 16 yoshdan javobgarlik; maxsus subyekt sifatida tizimga kirish vakolatiga ega xodimlar (insayderlar). *Subyektiv tomon:* qasd, ko‘pincha to‘g‘ri qasd; motiv moddiy manfaat, siyosiy-mafkuraviy maqsad, raqobat yoki o‘zini isbotlash.

Shaxs tiplari. Kriminologik xususiyatlariga ko‘ra besh tip ajratildi: texnik (xaker), g‘arazli (kiber-firibgar), mazmunli (kontent tarqatuvchi), ehtiyotkor bo‘lmagan (loqayd xodim) va qaram (onlayn qimor yoki noqonuniy savdoga qaramlik tufayli jinoyat sodir etuvchi) tip. Kriminogen motivatsiya darajasi bo‘yicha to‘rt guruh: tasodifiy, vaziyatga bog‘liq, beqaror va professional kiberjinoyatchilar.

[33] Council of Europe. (2001, 23 November). Convention on Cybercrime (ETS No. 185). https://coe.int/en/web/cybercrime/the-budapest-convention

IIV ma’lumotlari[34] kiberjinoyatlar sonining va turlarining keskin o‘sganini ko‘rsatadi. Prezident 2026-yil 12-mart kuni o‘tkazilgan yig‘ilishda axborot texnologiyalari sohasidagi jinoyatlar uchun jazo choralarini kuchaytirish va kiberjinoyat oqibatida yetkazilgan zarar uchun banklar va to‘lov tashkilotlarining javobgarligi bo‘yicha takliflarni ma’qulladi[35]. Rasmiy xabarlarga ko‘ra, jinoyat sodir etishda axborot texnologiyalaridan foydalanish javobgarlik va jazoni og‘irlashtiruvchi holat sifatida belgilanishi rejalashtirilgan[36]. Demak, quyida ilgari surilgan takliflarning bir qismi qonun ijodkorligi jarayoni bilan kesishadi va ularning yakuniy ko‘rinishi qabul qilingan normalarga moslashtirilishi lozim.

Aniqlangan bo‘shliqlar

1. Terminologik noaniqlik. Tahlil qilingan tahrirdagi Jinoyat kodeksida «kiberjinoyat», «kiberfazo», «DDoS-hujum», «raqamli aktiv», «kripto-aktiv», «elektron identifikatsiya vositasi» kabi atamalar mustahkamlanmagan. Bu bir xil qilmishning turlicha kvalifikatsiya qilinishiga olib keladi.

2. Virtual aktivlar. Kripto-hamyonga kirish va private key o‘g‘irlash holatlari odatda o‘g‘rilik sifatida baholanadi, biroq virtual aktivning ashyoviy xususiyati yo‘qligi sababli kvalifikatsiyada kolleziya yuzaga keladi.

3. Sun’iy intellekt va deepfake. Tuhmat va haqorat normalari an’anaviy tarqatish usullariga mo‘ljallangan; raqamli qiyofa, ovoz va biometrik ma’lumotlarni soxtalashtirish alohida himoyalanmagan.

4. Elektron dalillar. Skreenshot, log-fayl, IP-manzil va blokcheyn tranzaksiyalari amaliyotda har doim ham yetarli dalil sifatida qabul qilinmaydi; isbotlash standartlari aniq emas.

5. Javobgarlik yoshi va institutsional tayyorgarlik. Murakkab hujumlarni 14–15 yoshli shaxslar sodir etishi mumkinligi masalasi hamda maxsus tayyorlangan tergovchi va ekspertlar yetishmasligi.

Qiyosiy natijalar

2-jadval. Yevropa Ittifoqi, AQSH va Singapur tajribasining qiyosiy tahlili

Tizim	Asosiy hujjat	Mexanizm	O‘zbekiston uchun xulosa
Yevropa Ittifoqi	Direktiva 2013/40/EU [16]; NIS2 [19]; GDPR	tizimlarga hujumlar uchun jinoiy javobgarlik; botnet, jiddiy zarar va muhim	og‘irlashtiruvchi holatlar tizimi; hodisa haqida

[34] Ichki ishlar vazirligi Tezkor-qidiruv departamenti Kiberxavfsizlik markazi faoliyatiga bag‘ishlangan press-tur. (2025, 29-may). O‘zbekiston Respublikasi hukumat portali (gov.uz). https://gov.uz/oz/iiv/news/view/57775

[35] «Moliyaviy piramida» uchun jazo choralari og‘irlashtiriladi (Prezident huzuridagi yig‘ilish, 2026-yil 12-mart). (2026, 12-mart). Kun.uz. https://kun.uz/news/2026/03/12/moliyaviy-piramida-uchun-jazo-choralari-ogirlashtiriladi

[36] Kiberjinoyat uchun jazo choralari kuchaytirilmoqda. (nashr sanasi manbada ko‘rsatilmagan). Anhor.uz. https://anhor.uz/uzl/news/kiberjinoyat-uchun-jazo-choralari-kuchaytirilmoqda/

Tizim	Asosiy hujjat	Mexanizm	O‘zbekiston uchun xulosa
	[20]	infratuzilmaga hujum og‘irlashtiruvchi holat sifatida; xavflarni boshqarish va hodisa haqida xabar berish majburiyati	muddatli xabar berish
AQSH	CFAA, 18 U.S.C. § 1030 [17]; CISA Act of 2018 [18]	alohida federal norma; muhim infratuzilma xavfsizligi uchun mustaqil agentlik	idoralararo va davlat–xususiy sektor axborot almashinuvi
Singapur	Cybersecurity Act 2018, 15-bo‘lim [21; 22]	muhim axborot infratuzilmasi egalari uchun kamida ikki yilda bir marta audit va har yili xavflarni baholash	muhim infratuzilma uchun majburiy audit

Eslatma: GDPR’ning 33-moddasi shaxsiy ma’lumotlar buzilishi haqida nazorat organiga 72 soat ichida xabar berishni talab qiladi[37], NIS2 esa xavflarni boshqarish choralari va hodisa haqida xabar berish tartibini belgilaydi[38].

MUHOKAMA (DISCUSSION)

Budapesht va BMT konvensiyalari kontekstida

2024-yil 24-dekabrda BMT Bosh Assambleyasi 79/243-son rezolyutsiyasi bilan Kiberjinoyatchilikka qarshi BMT Konvensiyasini qabul qildi[39]; u 2025-yil 25-oktabrda Hanoyda imzolash uchun ochildi[40]. Xalqaro hamkorlik loyihasi materiallariga ko‘ra, O‘zbekiston bu konvensiyani 2025-yil oktabr oxirida imzoladi va Budapesht konvensiyasiga qo‘shilish jarayonini boshlashini e’lon qildi. Yevropa Komissiyasining O‘zbekistonning qo‘shilish so‘rovi bo‘yicha baholashi Yevropa Ittifoqi Kengashining

[37] European Parliament & Council of the European Union. (2022). Directive (EU) 2022/2555 of 14 December 2022 (NIS2 Directive). https://eur-lex.europa.eu/eli/dir/2022/2555/oj

[38] European Parliament & Council of the European Union. (2016). Regulation (EU) 2016/679 of 27 April 2016 (General Data Protection Regulation), Art. 33. https://eur-lex.europa.eu/eli/reg/2016/679/oj

[39] . United Nations General Assembly. (2024, 24 December). United Nations Convention against Cybercrime (A/RES/79/243). UNODC. https://unodc.org/unodc/en/cybercrime/convention/home.html

[40] United Nations Convention against Cybercrime. (n.d.). United Nations Treaty Collection, Ch. XVIII-16. https://treaties.un.org/doc/Publication/MTDSG/Volume%20II/Chapter%20XVIII/XVIII-16.en.xml

COPEN ishchi guruhi 2026-yil 13-fevral yig‘ilishi uchun taqdim etilgan[41]. Yevropa Kengashining 2020-yil holatidagi huquqiy profilida O‘zbekiston konvensiyani imzolamagani qayd etilgan[42]. Bu holat tadqiqot uchun ikki xulosa beradi: birinchidan, 1-jadvalda keltirilgan muvofiqlik qo‘shilish jarayonida milliy normalarni konvensiyaga moslashtirish uchun amaliy asos bo‘la oladi; ikkinchidan, 2020-yilgi profil eskirgan va qayta baholanishi kerak.

Jinoyat kodeksiga takliflar bo‘yicha mualliflik pozitsiyasi. Muallif quyidagi takliflarni ilgari suradi. *Birinchi,* Jinoyat kodeksining atamalar bo‘limiga «kiberjinoyat» (axborot tizimlari, telekommunikatsiya tarmoqlari, kompyuter texnikasi, raqamli ma’lumotlar yoki kiberfazo vositasida yoxud ularga qarshi sodir etiladigan ijtimoiy xavfli qilmish) ta’rifini kiritish. *Ikkinchi,* ijtimoiy muhandislik va fishing orqali sodir etiladigan firibgarlik uchun alohida «Kiber-firibgarlik» normasi (shartli 168¹-modda). *Uchinchi,* shaxsning roziligisiz sun’iy intellekt yordamida yuz, ovoz yoki biometrik ma’lumotlarini soxtalashtirish va tarqatish uchun javobgarlik belgilovchi norma (shartli 141³-modda). *To‘rtinchi,* «o‘zganing mulki» tushunchasiga virtual aktivlar, kriptovalyutalar va raqamli hamyonlarni kiritish. *Beshinchi,* firibgarlik va o‘g‘rilikning kvalifikatsiya belgilariga fishing va ijtimoiy muhandislik orqali masofadan talon-toroj qilishni qo‘shish.

Bu takliflarni tanqidiy baholashda muhim jihat: alohida modda (shartli 168¹) va og‘irlashtiruvchi holat yondashuvlari raqobatlashadi. Yevropa Ittifoqi direktivasi[43] og‘irlashtiruvchi holatlar yo‘lini tanlagan, O‘zbekistonda ham aynan shu yo‘l rejalashtirilmoqda. Shuning uchun muallif alohida norma zaruriyatini faqat 168-modda orqali raqamli usulni qamrab olish imkoni bo‘lmagan taqdirda saqlab qoladi va ikkala variantni qonun loyihasi muhokamasida solishtirishni tavsiya qiladi. Yangi normalarning raqamlari joriy tahrirga qarab aniqlanishi kerak.

Javobgarlik Yoshi. Muallif XX¹ bob moddalari bo‘yicha javobgarlik yoshini 14 yoshga tushirishni taklif etadi, chunki murakkab texnik hujumlarni o‘smirlar sodir etishi mumkin. Bu taklif eng munozarali. Tadqiqotda 14–15 yoshli shaxslar tomonidan sodir etilgan kiberjinoyatlar ulushi bo‘yicha statistik ma’lumot keltirilmagan, shuning uchun taklif gipoteza sifatida qaralishi kerak. Muqobil yo‘l sifatida iqtidorli yoshlarni qonuniy IT-

[41] European Commission’s assessment on the request for accession of Uzbekistan to the Council of Europe Convention on Cybercrime (58649/EU XXVIII.GP). (2026, 13 February). COPEN. https://www.parlament.gv.at/gegenstand/XXVIII/EU/58649

[42] Council of Europe, C-PROC. (2020, 1 May). Uzbekistan: Cybercrime legislation. Domestic equivalent to the provisions of the Budapest Convention (Legal profile, version 01 May 2020). https://rm.coe.int/octocom-legal-profile-uzbekistan/16809ed70e

[43] European Parliament & Council of the European Union. (2013). Directive 2013/40/EU of 12 August 2013 on attacks against information systems. Official Journal of the European Union, L 218, 8–14. https://eur-lex.europa.eu/eli/dir/2013/40/oj

faoliyatga («oq xakerlik») yo‘naltirish va profilaktik ta’lim tavsiya etiladi; raqamli gigiyena yondashuvi[44] shu yo‘nalishni qo‘llab-quvvatlaydi.

Muhim infratuzilma va profilaktika. Singapur tajribasi muhim axborot infratuzilmasi egalari uchun audit va xavflarni baholashni qonun darajasida majburiy qilishning aniq namunasini beradi[45]. Muallif O‘zbekistonda ham banklar, energetika, transport va sog‘liqni saqlash tizimlari uchun muntazam audit tizimini qonuniy mustahkamlashni tavsiya etadi. AQSH tajribasi[46] banklar, to‘lov tizimlari va ichki ishlar organlari o‘rtasida tahdidlar haqida tezkor axborot almashinuvi platformasini yaratish g‘oyasini asoslaydi; bunday platforma PF-38 doirasidagi institutsional choralar bilan uyg‘unlashtirilishi kerak[47]. Ta’lim muassasalarida kiber-gigiyena darslarini joriy etish profilaktik yo‘nalishning tarkibiy qismi sifatida taklif etiladi[48].

XULOSA (CONCLUSION)

Xulosa qilib aytganda, raqamli iqtisodiyot va sun’iy intellekt jadal rivojlanayotgan bir sharoitda kiberjinoyatga qarshi kurashish jinoiy-huquqiy normalarni zamonaviy tahdidlarga hamda Budapesht va BMT konvensiyalari talablariga mos holda izchil takomillashtirishni talab etadi. Bu borada Jinoyat kodeksida atamalar va javobgarlik asoslarini aniqlashtirish, virtual aktivlar daxlsizligi hamda deepfake kabi texnologik tajovuzlardan himoyalanish mexanizmlarini belgilash bilan birga, elektron dalillar bilan ishlash tartibini puxta yo‘lga qo‘yish, muhim axborot infratuzilmasi uchun kiberxavfsizlik auditini majburiy etish va aholining raqamli gigiyena madaniyatini yuksaltirish maqsadga muvofiqdir.

O‘tkazilgan tadqiqot natijalari umumlashtirilib, O‘zbekiston Respublikasining Jinoyat kodeksini takomillashtirish bo‘yicha quyidagi aniq qonunchilik takliflari ilgari suriladi:

1. Jinoyat kodeksiga 168¹-moddani («Kiber-firibgarlik») kiritish:

«168¹-modda. Kiber-firibgarlik

Kiber-firibgarlik, ya’ni kiberfazoda axborot tizimlari, telekommunikatsiya tarmoqlari yoki hisoblash texnikasi vositalaridan foydalangan holda, fishing, ijtimoiy

[44] Zoilboev, J. (2022). Kiberxavfsizlik, raqamli huquq va raqamli gigiyena – kiberjinoyatchilikka qarshi muqobil yechim. Jamiyat va innovatsiyalar – Society and innovations. https://inscience.uz/index.php/socinov/article/download/2139/2367/8015

[45]Cyber Security Agency of Singapore. (n.d.). Cybersecurity audit requirements for Critical Information Infrastructure: FAQs. https://csa.gov.sg/faqs/cybersecurity-audit-cii

[46]Cybersecurity and Infrastructure Security Agency Act of 2018, Pub. L. No. 115-278 (2018). https://www.congress.gov/bill/115th-congress/house-bill/3359

[47] O‘zbekiston Respublikasi Prezidenti. (2026, 10-mart). O‘zbekiston Respublikasining Kiberxavfsizlik strategiyasini belgilash va kiberjinoyatchilikning oldini olish tizimini takomillashtirish to‘g‘risida (PF-38-son Farmon). https://lex.uz/uz/docs/-8079286

[48] Zoilboev, J. (2022). Kiberxavfsizlik, raqamli huquq va raqamli gigiyena – kiberjinoyatchilikka qarshi muqobil yechim [Cybersecurity, digital law and digital hygiene: An alternative solution against cybercrime]. Jamiyat va innovatsiyalar – Society and innovations. https://inscience.uz/index.php/socinov/article/download/2139/2367/8015

muhandislik yoxud boshqa raqamli usullar orqali foydalanuvchilarni aldash yoki ishonchini suiiste'mol qilish yo‘li bilan o‘zganing mulkini yoki mulkiy huquqini qo‘lga kiritish — *BCMning 100 baravaridan 300 baravarigacha jarima yoki 320 soatdan 480 soatgacha majburiy jamoat ishlari yoki 2 yilgacha axloq tuzatish ishlari yoxud 1 yildan 3 yilgacha ozodlikni cheklash yoki 3 yilgacha ozodlikdan mahrum qilish bilan jazolanadi.*

O‘sha qilmish: a) ko‘p miqdorda; b) bir guruh shaxslar tomonidan oldindan til biriktirib; c) kompyuter tizimlariga masofadan ruxsatsiz daxl qilish yoki ularni bloklash orqali sodir etilgan bo‘lsa — *BHMning 300 baravaridan 600 baravarigacha jarima yoki 2 yildan 3 yilgacha axloq tuzatish ishlari yoxud 3 yildan 5 yilgacha ozodlikni cheklash yoki 5 yildan 8 yilgacha ozodlikdan mahrum qilish bilan jazolanadi.»*

2. Jinoyat kodeksiga 141³-moddani («Raqamli qiyofaga va virtual daxlsizlikka tajovuz qilish») kiritish:

«141³-modda. Raqamli qiyofaga va virtual daxlsizlikka tajovuz qilish

Shaxsning roziligisiz sun'iy intellekt, neyrotarmoqlar yoki boshqa raqamli dasturiy texnologiyalar yordamida uning yuz tasviri, ovozi yoxud boshqa biometrik ma'lumotlarini qasddan soxtalashtirish (deepfake) va kiberfazoda, internet tarmoqlarida tarqatish orqali shaxsning sha'ni, qadr-qimmati yoki ishchanlik obro‘siga jiddiy zarar yetkazish — *BHMning 50 baravaridan 100 baravarigacha jarima yoki 300 soatgacha majburiy jamoat ishlari yoki 2 yilgacha axloq tuzatish ishlari bilan jazolanadi.*

O‘sha qilmish: a) g‘arazli yoki boshqa past niyatlarda; b) jabrlanuvchining yaqin qarindoshlariga nisbatan; c) pornografik yoki ekstremistik xarakterdagi materiallarga montaj qilish orqali sodir etilgan bo‘lsa — *BHMning 100 baravaridan 300 baravarigacha jarima yoki 360 soatdan 480 soatgacha majburiy jamoat ishlari yoxud 1 yildan 3 yilgacha ozodlikni cheklash yoki 3 yilgacha ozodlikdan mahrum qilish bilan jazolanadi.»*

3. JK 8-bo‘limidagi «O‘zganing mulki» tushunchasini kengaytirish:

JK 8-bo‘limiga *«Virtual (raqamli) aktivlar, kriptovalyutalar va blokcheyn tizimidagi raqamli hamyonlar»* iborasini jinoiy tajovuz predmeti sifatida kiritish.

4. Javobgarlik yoshini pasaytirish:

JK 17-moddasida og‘ir kiber-tajovuzlar (XX¹-bob moddalari) uchun jinoiy javobgarlikka tortishning eng kichik yoshini 14 yosh qilib belgilash.

FOYDALANILGAN ADABIYOTLAR RO‘YXATI

1. O‘zbekiston Respublikasi Prezidenti. (2026, 10-mart). *O‘zbekiston Respublikasining Kiberxavfsizlik strategiyasini belgilash va kiberjinoyatchilikning oldini olish tizimini takomillashtirish to‘g‘risida* (PF-38-son Farmon). https://lex.uz/uz/docs/-8079286

2. O‘zbekiston Respublikasi Prezidenti. (2025, 30-aprel). *Axborot texnologiyalari yordamida sodir etiladigan jinoyatlarga qarshi kurashish faoliyatini yanada kuchaytirishga qaratilgan chora-tadbirlar to‘g‘risida* (PQ-153-son Qaror). https://lex.uz/en/docs/-7511145

3. Ichki ishlar vazirligi Tezkor-qidiruv departamenti Kiberxavfsizlik markazi faoliyatiga bag‘ishlangan press-tur. (2025, 29-may). *O‘zbekiston Respublikasi hukumat portali (gov.uz)*. https://gov.uz/oz/iiv/news/view/57775

4. International Telecommunication Union. (2024). *Global Cybersecurity Index 2024* (5th ed.). ISBN 978-92-61-38751-8. https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv5/2401416_1b_Global-Cybersecurity-Index-E.pdf

5. Uzbekistan improves its position in global cybersecurity index. (2024, 14-sentabr). *Kun.uz*. https://kun.uz/en/news/2024/09/14/uzbekistan-improves-its-position-in-global-cybersecurity-index

6. Uzbekistan recognized as a country with developing cybersecurity. (2024, 16-sentabr). *UzDaily*. https://uzdaily.ru/en/uzbekistan-recognized-as-a-country-with-developing-cybersecurity

7. Do‘smatov, D. R. (2026). *Kiberjinoyatchilikka qarshi kurashning jinoyat-huquqiy va kriminologik jihatlari* [Yuridik fanlar bo‘yicha falsafa doktori (PhD) dissertatsiyasi avtoreferati]. Toshkent davlat yuridik universiteti. https://api.ziyonet.uz/uploads/books/10000014/8gvnDivBURroIBt.pdf

8. Zoilboev, J. (2022). Kiberxavfsizlik, raqamli huquq va raqamli gigiyena – kiberjinoyatchilikka qarshi muqobil yechim. *Jamiyat va innovatsiyalar – Society and innovations*. https://inscience.uz/index.php/socinov/article/download/2139/2367/8015

9. Holt, T. J., Bossler, A. M., & Seigfried-Spellar, K. C. (2017). *Cybercrime and digital forensics: An introduction*. Routledge.

10. O‘zbekiston Respublikasi. (2022, 15-aprel). *Kiberxavfsizlik to‘g‘risida* (O‘RQ-764-son Qonun). https://lex.uz/docs/5960593

11. O‘zbekiston Respublikasi. (1994, 22-sentabr). *O‘zbekiston Respublikasining Jinoyat kodeksi* (2012-XII-son), XX¹ bob. https://lex.uz

12. Council of Europe. (2001, 23 November). *Convention on Cybercrime* (ETS No. 185). https://coe.int/en/web/cybercrime/the-budapest-convention

13. Council of Europe, C-PROC. (2020, 1 May). *Uzbekistan: Cybercrime legislation. Domestic equivalent to the provisions of the Budapest Convention* (Legal profile, version 01 May 2020). https://rm.coe.int/octocom-legal-profile-uzbekistan/16809ed70e

14. «Moliyaviy piramida» uchun jazo choralari og‘irlashtiriladi (Prezident huzuridagi yig‘ilish, 2026-yil 12-mart). (2026, 12-mart). *Kun.uz*. https://kun.uz/news/2026/03/12/moliyaviy-piramida-uchun-jazo-choralari-ogirlashtiriladi

15. Kiberjinoyat uchun jazo choralari kuchaytirilmoqda. (nashr sanasi manbada ko‘rsatilmagan). *Anhor.uz*. https://anhor.uz/uzl/news/kiberjinoyat-uchun-jazo-choralari-kuchaytirilmoqda/

16. European Parliament & Council of the European Union. (2013). Directive 2013/40/EU of 12 August 2013 on attacks against information systems. *Official Journal of the European Union, L 218*, 8–14. https://eur-lex.europa.eu/eli/dir/2013/40/oj

17. Computer Fraud and Abuse Act, 18 U.S.C. § 1030. https://www.law.cornell.edu/uscode/text/18/1030

18. Cybersecurity and Infrastructure Security Agency Act of 2018, Pub. L. No. 115-278 (2018). https://www.congress.gov/bill/115th-congress/house-bill/3359

19. European Parliament & Council of the European Union. (2022). Directive (EU) 2022/2555 of 14 December 2022 (NIS2 Directive). https://eur-lex.europa.eu/eli/dir/2022/2555/oj

20. European Parliament & Council of the European Union. (2016). Regulation (EU) 2016/679 of 27 April 2016 (General Data Protection Regulation), Art. 33. https://eur-lex.europa.eu/eli/reg/2016/679/oj

21. Cybersecurity Act 2018 (No. 9 of 2018), s. 15. Singapore Statutes Online. https://sso.agc.gov.sg/Act/CA2018

22. Cyber Security Agency of Singapore. (n.d.). *Cybersecurity audit requirements for Critical Information Infrastructure: FAQs*. https://csa.gov.sg/faqs/cybersecurity-audit-cii

23. United Nations General Assembly. (2024, 24 December). *United Nations Convention against Cybercrime* (A/RES/79/243). UNODC. https://unodc.org/unodc/en/cybercrime/convention/home.html

24. United Nations Convention against Cybercrime. (n.d.). United Nations Treaty Collection, Ch. XVIII-16. https://treaties.un.org/doc/Publication/MTDSG/Volume%20II/Chapter%20XVIII/XVIII-16.en.xml

25. Central Asian Countries Strengthen Regional Cooperation on Electronic Evidence. (n.d.). *UzDaily*. https://uzdaily.ru/en/central-asian-countries-strengthen-regional-cooperation-on-electronic-evidence/ ; see also: https://projects.osce.org/node/601158

26. European Commission’s assessment on the request for accession of Uzbekistan to the Council of Europe Convention on Cybercrime (58649/EU XXVIII.GP). (2026, 13 February). COPEN. https://www.parlament.gv.at/gegenstand/XXVIII/EU/58649