LAW, POLICY AND SOCIETY ПРАВО, ПОЛИТИКА И ОБЩЕСТВО - HUQUQ, SIYOSAT VA JAMIYAT
ILMIY-TAHLILIY JURNAL
Issue - 5(2026) / ISSN 3030-3052 Available at www.uznauka.uz

JAMIYAT XAVFSIZLIGIGA TAHDID SOLUVCHI KIBERJINOYATLARNING TUSHUNCHASI, KELIB CHIQISH TARIXI VA RIVOJLANISH TENDENSIYASI: TAQQOSLAMA HUQUQIY TAHLIL

Saidov Abdunabi Vali o‘g‘li
Toshkent davlat yuridik universiteti magistranti
Elektron pochta: saidovabdunabi2000@gmail.com

Annotatsiya. *Ushbu maqolada jamiyat xavfsizligiga tahdid soluvchi kiberjinoyatlarning huquqiy tushunchasi, kelib chiqish tarixi, rivojlanish bosqichlari va hozirgi tendensiyalar keng qamrovli tahlil qilinadi. Xorijiy davlatlar — AQSh, Yevropa Ittifoqi, Rossiya Federatsiyasi va Qozog‘iston — tajribasi tahlil qilingan. O‘zbekiston Respublikasining kiberxavfsizlik sohasidagi milliy qonunchiligining holati va takomillashtirish yo‘llari belgilab berilgan. Xalqaro huquqiy hujjatlar va milliy qonunchilikning o‘zaro muvofiqligiga doir tavsiyalar ishlab chiqilgan.*

Kalit so‘zlar: *kiberjinoyat, kiberxavfsizlik, axborot xavfsizligi, Budapesht konvensiyasi, raqamli tahdid, milliy qonunchilik, jinoyat-huquqiy himoya.*

KIRISH

XXI asrda raqamli texnologiyalar insoniyat hayotining barcha sohalarini qamrab oldi. Axborot-kommunikatsiya texnologiyalari (AKT) iqtisodiyot, ta’lim, sog‘liqni saqlash, davlat boshqaruvi va fuqarolik jamiyatida muhim o‘rin egalladi. Biroq ushbu rivojlanish bilan parallel ravishda yangi turdagi jinoyatlar — kiberjinoyatlar — tobora keng tarqalmoqda va ular jamiyat xavfsizligiga jiddiy tahdid solmoqda. O‘zbekiston Respublikasi Prezidenti Shavkat Mirziyoyev Oliy Majlisga Murojaatnomasida ta’kidlaganidek:

“Kiberxavfsizlik masalasi bugungi kunda davlat suvereniteti, iqtisodiy barqarorlik va fuqarolarimiz xavfsizligiga bevosita ta’sir ko‘rsatadigan strategik

masalaga aylangan" [1]. Mazkur e'tirof kiberjinoyatchilikka qarshi kurashning milliy siyosat darajasiga ko'tarilganidan dalolat beradi.

Kiberjinoyatlarni o'rganish bir qancha jihatdan dolzarb ahamiyat kasb etadi. **Birinchidan**, kiberjinoyatlardan jahon iqtisodiyotiga yetkazilayotgan yillik zarar 2023-yilda 8 trillion AQSH dollaridan oshdi [13]. **Ikkinchidan**, ushbu jinoyatlar milliy chegaradan tashqarida, ya'ni transchegaraviy xarakter kasb etganligi sababli ularga qarshi kurashda xalqaro hamkorlik muqarrar. **Uchinchidan**, O'zbekiston "Raqamli O'zbekiston – 2030" strategiyasi doirasida jadal raqamli transformatsiya yo'lini bosib o'tmoqda [18], bu esa kiberxavfsizlik masalasini yanada dolzarb qilmoqda.

Maqolaning maqsadi — kiberjinoyatlarning huquqiy tushunchasi va kelib chiqish tarixini o'rganish, xorijiy davlatlar tajribasiga taqqoslama tahlil o'tkazish hamda O'zbekiston qonunchiligini takomillashtirish bo'yicha ilmiy asoslangan tavsiyalar ishlab chiqishdan iborat.

Tadqiqot metodologiyasi: qiyosiy-huquqiy tahlil, tizimli tahlil, tarixiy-huquqiy metod, formal-mantiqiy metod va induktiv-deduktiv usullardan foydalanilgan.

KIBERJINOYAT TUSHUNCHASI: NAZARIY-HUQUQIY TAHLIL

Kiberjinoyat (cybercrime) atamasi o'zida ikki tushunchani birlashtiradi: kibermakon (cyberspace) va jinoyat (crime). Ushbu tushuncha huquq fani, kriminologiya va axborot texnologiyalari fanlarining kesishmasida shakllangan bo'lib, hali ham yagona xalqaro ta'rifga ega emas.

O'zbekiston Respublikasining "Kiberxavfsizlik to'g'risida"gi Qonunida kiberjinoyatchilik "axborotni egallash, uni o'zgartirish, yo'q qilish yoki axborot tizimlari va resurslarini ishdan chiqarish maqsadida kibermakonda dasturiy

LAW, POLICY AND SOCIETY ПРАВО, ПОЛИТИКА И ОБЩЕСТВО - HUQUQ, SIYOSAT VA JAMIYAT
ILMIY-TAHLILIY JURNAL
Issue - 5(2026) / ISSN 3030-3052 Available at www.uznauka.uz

ta’minot va texnik vositalardan foydalanilgan holda amalga oshiriladigan jinoyatlar yig‘indisi” sifatida ta’riflanadi [2]. Ushbu ta’rif uch muhim element — axborot, kibermakon va jinoyatni o‘z ichiga oladi.

Xalqaro huquqda kiberjinoyatlarning yagona ta’rifi yo‘q. Biroq, Budapesht Konvensiyasi (2001) ushbu sohadagi asosiy xalqaro-huquqiy hujjat sifatida kiberjinoyatlarni quyidagi guruhlarga ajratadi: internet va boshqa kompyuter tarmoqlari orqali sodir etilgan jinoyatlar, mualliflik huquqlarining buzilishi, kompyuter firibgarligi, bolalar pornografiyasi va tarmoq xavfsizligini buzish bilan bog‘liq jinoyatlar [3].

O‘zbek olimi B.A.Tursunov ushbu tushunchani yanada kengaytirgan holda unga “axborot tizimlaridan foydalanish orqali sodir etiluvchi va shaxs, jamiyat hamda davlat manfaatlariga zarar yetkazuvchi jinoyatlar majmui” sifatida ta’rif beradi [4]. Rus huquqshunos olimasi T.V.Klenova esa kiberjinoyatni “axborot muhitida sodir etiladigan, jinoyat-huquqiy jihatdan taqiqlangan va ijtimoiy xavfli xatti-harakat” deb ta’riflaydi [5].

Kiberjinoyatning huquqiy tabiatini anglashda uning o‘ziga xos belgilarini ajratib ko‘rsatish muhim bo‘lib, bular: **a)** maxsus vosita (kompyuter, tarmoq, dastur) dan foydalanish; **b)** kibermakonda amalga oshirilishi; **v)** yashirin tarzda sodir etish darajasining yuqoriligi (latency); **g)** transchegaraviy xususiyatga egaligidir.

KIBERJINOYATLARNING KELIB CHIQISH TARIXI VA RIVOJLANISH BOSQICHLARI

Kiberjinoyatlar tarixi kompyuter texnologiyalarining paydo bo‘lishi bilan bevosita bog‘liq. Ushbu rivojlanishni beshta asosiy bosqichga bo‘lish maqsadga muvofiq.

LAW, POLICY AND SOCIETY ПРАВО, ПОЛИТИКА И ОБЩЕСТВО - HUQUQ, SIYOSAT VA JAMIYAT
ILMIY-TAHLILIY JURNAL
Issue - 5(2026) / ISSN 3030-3052 Available at www.uznauka.uz

Birinchi bosqich (1960–1970-yillar) — "Hacker madaniyati" davri. AQShning yirik universitetlari — MIT, Stanford, Carnegie Mellon — da "xaker" subkulturasi paydo bo'ldi. Bu davrda kompyuter tizimlari asosan ilmiy muassasalar, harbiy va davlat tashkilotlarida mavjud bo'lib, ularga ruxsatsiz kirish holatlari kuzatildi. Jinoyatlar moliyaviy maqsaddan emas, texnologik qiziquvchanlikdan yuzaga keldi.

Ikkinchi bosqich (1980–1990-yillar) — Shaxsiy kompyuterlar davri. 1988-yilda Robert Morris tomonidan yaratilgan "Morris Worm" Internetga ulangan 6000 dan ortiq kompyuterga zarar yetkazdi. Bu voqea kiberjinoyat tarixida birinchi yirik hodisa sifatida qayd etildi. 1986-yilda AQShda "Kompyuter firibgarligi va suiiste'mol qilish to'g'risida"gi Qonun (CFAA) qabul qilindi [6].

Uchinchi bosqich (1990–2000-yillar) — Internet inqilobi. WWW (World Wide Web) ning keng tarqalishi kiberjinoyatlarni yangi bosqichga ko'tardi. Bank karta ma'lumotlarini o'g'irlash, fishing-hujumlar (phishing), zararli dasturlar (malware) ommaviy tus oldi. Budapesht Konventsiyasi (2001) qabul qilindi [3].

To'rtinchi bosqich (2000–2010-yillar) — Davlat darajasidagi kiberhujumlar. 2007-yilda Estoniyaga, 2008-yilda Gruziyaga uyushtirilgan keng ko'lamdagi kiberhujumlar davlat infratuzilmasini zaif holatga olib keldi. 2010-yilda Eron yadro dasturiga qarshi "Stuxnet" virusi ishlatildi.

Beshinchi bosqich (2010-yillardan bugungi kungacha) — To'lov dasturlari va AI texnologiyalari. "Ransomware" hujumlarining ortishi, ijtimoiy muhandislik usullarining rivojlanishi, sun'iy intellektdan foydalangan holda amalga oshiriladigan kiberhujumlar va IoT zaifliklaridan foydalanish hozirgi davrning asosiy belgilaridir [17].

LAW, POLICY AND SOCIETY ПРАВО, ПОЛИТИКА И ОБЩЕСТВО - HUQUQ, SIYOSAT VA JAMIYAT
ILMIY-TAHLILIY JURNAL
Issue - 5(2026) / ISSN 3030-3052 Available at www.uznauka.uz

KIBERJINOYATLARGA QARSHI KURASHDA XORIJIY DAVLATLAR QONUNCHILIGI TAHLILI

Amerika Qo‘shma Shtatlari. AQSh kiberxavfsizlik qonunchiligi jahonning eng rivojlangan tizimlaridan biri hisoblanadi. 1986-yilda qabul qilingan va keyinchalik takomillashtirilgan “Kompyuter firibgarligi va suiiste’mol qilish to‘g‘risida”gi Qonun (CFAA, 18 U.S.C. §1030) [6] kiberjinoyatchilik sohasida asosiy qonunchilik hujjati hisoblanadi. Mazkur qonun ruxsatsiz kirish (unauthorized access), davlat kompyuterlariga tajovuz, moliyaviy firibgarlik va zararli dasturlarni tarqatishni jinoyat sifatida belgilaydi. Qonunga ko‘ra, davlat infratuzilmasiga zarar yetkazish uchun 10 yildan 20 yilgacha ozodlikdan mahrum qilish jazosi belgilangan.

Bundan tashqari, AQShda Milliy kiberxavfsizlik agentligi (CISA) faoliyat ko‘rsatadi.

Yevropa Ittifoqi. YI 2013-yilda Axborot tizimlariga hujumlarga qarshi direktiva (2013/40/EU) [7] qabul qilingan. Ushbu direktiva a’zo davlatlarda milliy qonunlarni mustahkamlash, og‘irroq jinoiy jazolar va vakolatli organlar o‘rtasida hamkorlikni kuchaytirish orqali kiberjinoyatchilikka qarshi kurashish va axborot xavfsizligini ta’minlashga qaratilgan.

Rossiya Federatsiyasi. Rossiyada kiberjinoyatlar sohasidagi asosiy hujjat — “Axborot, axborot texnologiyalari va axborotni muhofaza qilish to‘g‘risida”gi 149-FZ-son Federal Qonun (2006) hamda Jinoyat kodeksining 28-bobi [8] hisoblanadi. Rossiya Budapesht konvensiyasini imzolamagan bo‘lib, o‘zining mustaqil kiberxavfsizlik tizimini shakllantirgan.

Qozog‘iston Respublikasi. Qozog‘iston Jinoyat kodeksining 205–213-moddalari axborot texnologiyalari sohasidagi jinoyatlarni tartibga soladi

LAW, POLICY AND SOCIETY ПРАВО, ПОЛИТИКА И ОБЩЕСТВО - HUQUQ, SIYOSAT VA JAMIYAT
ILMIY-TAHLILIY JURNAL
Issue - 5(2026) / ISSN 3030-3052 Available at www.uznauka.uz

[10]. Mazkur moddalar axborot tizimlariga noqonuniy kirish, zararli kompyuter dasturlarini yaratish va tarqatish, axborotlashtirish obyekti faoliyatini buzish kabi qilmishlarni jinoyat sifatida belgilaydi.

O‘ZBEKISTON RESPUBLIKASIDA JAMIYAT XAVFSIZLIGIGA TAHDID SOLUVCHI KIBERJINOYATLARGA QARSHI KURASHISHGA OID HUQUQIY ASOSLAR

O‘zbekistonda kiberxavfsizlik qonunchiligi so‘nggi yillarda sezilarli darajada takomillashib bormoqda. Mazkur sohadagi asosiy hujjatlar quyidagilardan iborat.

Birinchidan, O‘zbekiston Respublikasi Jinoyat kodeksining XX[1] bobi Axborot texnologiyalari sohasidagi jinoyatlar deb nomlangan bo‘lib, 278[1]-278[9]-moddalari [11] kiberjinoyatlar uchun javobgarlikni belgilaydi.

Ikkinchidan, 2022-yilda qabul qilingan “Kiberxavfsizlik to‘g‘risida”gi Qonun [2] kiberxavfsizlik sohasidagi huquqiy munosabatlarni tartibga soluvchi maxsus qonun sifatida muhim ahamiyat kasb etadi. Qonun kiberxavfsizlikni ta’minlashning asosiy prinsiplarini, subyektlarining huquq va majburiyatlarini, shuningdek kiberxavfsizlikni ta’minlashga doir boshqa munosabatlarni tartibga soladi.

Uchinchidan, Prezidentimizning 2020-yil 15-iyundagi PQ-4751-son qarori [12] axborot xavfsizligi tizimini yanada mustahkamlashga yo‘naltirilgan. “Raqamli O‘zbekiston – 2030” Farmoni esa raqamli iqtisodiyot bilan parallel ravishda kiberxavfsizlikni ta’minlashni ustuvor vazifa sifatida belgilaydi [18].

Milliy qonunchilikda bir qator kamchiliklar mavjudligi huquqshunoslar tomonidan e’tirof etilmoqda [15]: “kiberjinoyat” tushunchasiga aniq ta’rifning mavjud emasligi; yangi turdagi kiberhujumlar (DDoS, ransomware, deepfake)

Issue - 5(2026) / ISSN 3030-3052 Available at www.uznauka.uz

uchun alohida jinoiy javobgarlik normalarining mavjud emasligi; provayder javobgarligi masalasining to‘liq tartibga solinmaganligi; elektron dalillarni sudda qabul qilish tartibining aniq belgilanmaganligiga, Jinoyat kodeksida aynan qaysi jinoyatlar jamiyat xavfsizligiga tahdid soluvchi kiberjinoyatlarga kirishi mavhumligi va jamiyat xavfsizligiga tahdid soluvchi jinoyatlar aniq belgilab berilmaganligiga doir muammolar mavjud.

Xususan, Jinoyat kodeksining **VI bo‘limi**da Jamoat xavfsizligi va jamoat tartibiga qarshi jinoyatlar keltirib o‘tilgan, **XVII bob** esa “Jamoat xavfsizligiga qarshi jinoyatlar” deb nomlangan bo‘lsada, Kodeksda qaysi jinoyatlar jamiyat xavfsizligiga tahdid soluvchi jinoyatlar yoki jamiyat xavfsizligiga tahdid soluvchi kiberjinoyatlar hisoblanishi aniq ko‘rsatib o‘tilmagan.

Vaholanki, Kodeksning 2-moddasiga asosan Jinoyat kodeksining vazifalari shaxsni, uning huquq va erkinliklarini, **jamiyat va davlat manfaatlarini**, mulkni, tabiiy muhitni, tinchlikni, insoniyat xavfsizligini jinoiy tajovuzlardan qo‘riqlash, shuningdek jinoyatlarning oldini olish, fuqarolarni respublika Konstitutsiyasi va qonunlariga rioya qilish ruhida tarbiyalashdan iboratdir.

O‘z navbatida, bunday jinoyatlarni jamoat xavfsizligiga tahdid soluvchi jinoyatlardan farqlab olish va aniq ro‘yxatini tuzish uchun ham avvalo “jamiyat” va “jamoat” atamalariga Kodeksning **sakkizinchi bo‘limi**da ta’rif berilishi lozim.

“Jamiyat” va **“jamoat”** so‘zlari arab tilidan olingan bo‘lib, “**jamiyat**” katta miqyosdagi odamlar guruhi bo‘lgan millat, davlat, xalqni nazarda tutsa, “**jamoat**” kichik yoki o‘rta hajmli guruhni nazarda tutadi, qamrov darajasiga ko‘ra, “jamiyat” keng ma’noga ega bo‘lib, ijtimoiy, iqtisodiy, siyosiy tizimlarni qamrab olsa, “jamoat” nisbatan ancha kichik bo‘lgan torroq doirani, muayyan joy, maqsad bilan bog‘liq bo‘lgan kishilar guruhini qamrab oladi.

LAW, POLICY AND SOCIETY ПРАВО, ПОЛИТИКА И ОБЩЕСТВО - HUQUQ, SIYOSAT VA JAMIYAT
ILMIY-TAHLILIY JURNAL
Issue - 5(2026) / ISSN 3030-3052 Available at www.uznauka.uz

KIBERJINOYATLARNING RIVOJLANISH TENDENSIYALARI VA XALQARO HAMKORLIK

Hozirgi kunda kiberjinoyatchilikda bir qancha muhim tendensiyalar kuzatilmoqda. UNODC ma'lumotlariga ko'ra [16], kiberjinoyatlar ulushi barcha transchegaraviy xarakterdagi uyushgan jinoyatlar ichida yildan-yilga ortib bormoqda.

Birinchi tendensiya: **Sun'iy intellektdan foydalanish.** Kiberjinoyatchilar AI va mashinali o'qitishni fishing-hujumlarni takomillashtirish, zararli dasturlarni yaratish va "deepfake" texnologiyalarini amalga oshirishda qo'llayapti [14].

Ikkinchi tendensiya: **To'lov dasturlari (Ransomware) epidemiyasi.** Ransomware hujumlari, xususan davlat organlari, kasalxonalar va moliya institutlariga qarshi, tizimli muammo sifatida tartibga solinishi zarur.

Uchinchi tendensiya: **Narsalar interneti (IoT) zaifliklari.** 2026-yilga kelib dunyo bo'ylab 30 milliarddan ortiq IoT qurilmasi ishga tushirilishi kutilmoqda. Ushbu qurilmalarning ko'pchiligi yetarlicha himoya mexanizmlariga ega emasligi kiberjinoyatchilar uchun yangi imkoniyatlar yaratmoqda [19].

To'rtinchi tendensiya: **Davlatlararo kiberkonfliktlar.** Davlatlar tomonidan homiylik qilingan kiberhujumlar xalqaro huquqda yangi masalalarni yuzaga keltirmoqda.

Xalqaro hamkorlik masalasida ta'kidlash joizki, O'zbekiston Budapesht Konvensiyasiga qo'shilmagan. Huquqshunos U.A.Nazarov fikriga ko'ra, Konvensiyaga qo'shilish milliy kiberxavfsizlik tizimini mustahkamlash va xalqaro huquqiy yordamni tezlashtirishda muhim qadam bo'lar edi [20].

MUAMMO VA TAVSIYALAR

Issue - 5(2026) / ISSN 3030-3052 Available at www.uznauka.uz

Olib borilgan huquqiy tahlil asosida O‘zbekiston qonunchiligini takomillashtirish bo‘yicha quyidagi ilmiy asoslangan tavsiyalar ishlab chiqildi:

1. **Qonunchilikni yangilash.** O‘zbekiston Respublikasi Jinoyat kodeksiga DDoS-hujumlar, ransomware, deepfake jinoyatlari va IoT qurilmalariga tajovuz uchun alohida jinoiy javobgarlik normalarini kiritish lozim.

Shuningdek, Jinoyat kodeksi sakkizinchi bo‘limiga “jamiyat” “jamoat”, “kiberjinoyat” atamalariga doir ta’riflar kiritilishi darkor.

2. **Xalqaro shartnomalar tizimiga qo‘shilish.** Budapesht konvensiyasiga qo‘shilish yoki unga kuzatuvchi sifatida faol ishtirok etish xalqaro huquqiy yordam mexanizmlaridan samarali foydalanish imkonini beradi.

3. **Elektron dalillar qonunchiligini rivojlantirish.** Elektron dalillarning yuridik kuchini belgilovchi, ularni yig‘ish, saqlash, tekshirish va sud jarayoniga kiritish tartibini tartibga soluvchi alohida qonun-normativ hujjat qabul qilinishi zarur.

4. **Ixtisoslashgan sud va sudlov tizimi.** Kiberjinoyatlar bo‘yicha ixtisoslashtirilgan prokuratura bo‘linmalari va raqamli kriminalistika ekspertlari kadrlar tayyorlashning alohida yo‘nalishi sifatida joriy etilishi maqsadga muvofiq.

5. **Xususiy sektor bilan hamkorlik.** AQSh va YI tajribasiga ko‘ra, davlat — xususiy sektor sherikligini (PPP) kiberxavfsizlik sohasida institutsional qonunchilik asosida tartibga solish samarali natijalar beradi.

XULOSA

Kiberjinoyatlar — raqamli asrning eng murakkab va ko‘p qirrali muammolaridan biri bo‘lib, ular shaxs, jamiyat va davlat xavfsizligiga tahdid solmoqda.

LAW, POLICY AND SOCIETY ПРАВО, ПОЛИТИКА И ОБЩЕСТВО - HUQUQ, SIYOSAT VA JAMIYAT
ILMIY-TAHLILIY JURNAL
Issue - 5(2026) / ISSN 3030-3052 Available at www.uznauka.uz

Jamiyat xavfsizligiga tahdid soluvchi kiberjinoyatlar esa qamrovi va zarar yetkazishi jihatidan shaxs yoki guruhga emas, balki katta miqyosdagi odamlar guruhi bo‘lgan davlat yoki jamiyatga qaratilgan kibermakonda sodir etiladigan jinoyatlar hisoblanadi.

Ushbu maqolada o‘tkazilgan huquqiy tahlil shuni ko‘rsatadiki, dunyodagi yetakchi davlatlar — AQSh, YI, Rossiya va Qozog‘iston — kiberjinoyatlarga qarshi kurashda turli yondashuvlarni q ‘llashsa-da, ularning barchasida umumiy tendensiya kuzatiladi: qonunchilikni doimiy yangilab borish, ixtisoslashgan organlar tuzish va xalqaro hamkorlikni kuchaytirish.

O‘zbekiston Respublikasi so‘nggi yillarda kiberxavfsizlik sohasida sezilarli qadamlar tashladi: “Kiberxavfsizlik to‘g‘risida”gi Qonun qabul qilindi, Jinoyat kodeksiga kiberjinoyatlarga oid normalar kiritildi, “Raqamli O‘zbekiston – 2030” strategiyasi e’lon qilindi. Biroq texnologiyalarning tez rivojlanishi milliy qonunchilikni muntazam takomillashtirib borish zarurligini taqozo etmoqda.

Yuqorida bayon etilgan tavsiyalar amalga oshirilganda, O‘zbekiston nafaqat o‘z fuqarolarini kiberjinoyatlardan himoya qilish samaradorligini oshiradi, balki xalqaro kiberxavfsizlik hamjamiyatida munosib o‘rin egallaydi. Bu esa Prezident Mirziyoyev tomonidan belgilab berilgan “Yangi O‘zbekiston” — qonun ustuvorligi va raqamli rivojlanish maqsadlariga xizmat qiladi.

FOYDALANILGAN ADABIYOTLAR

1. O‘zbekiston Respublikasi Prezidenti Sh.M.Mirziyoyevning Oliy Majlisga Murojaatnomasi. 29-dekabr 2023-yil. — Toshkent, 2023.

2. O‘zbekiston Respublikasi “Kiberxavfsizlik to‘g‘risida”gi Qonuni. 15-aprel 2022-yil, ORQ-764-son. — Toshkent: Adolat, 2022.

3. Budapest Convention on Cybercrime. Council of Europe. ETS No.185. — Budapest, 23 November 2001.

4. Tursunov B.A. Kiberjinoyatchilikka qarshi kurashning huquqiy asoslari. — Toshkent: TDYuU nashriyoti, 2021. — 180 b.

5. Кленова Т.В. Понятие киберпреступления в российском уголовном праве // Вектор науки. — 2022. — №3. — С. 42–49.

6. Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030 (1986, as amended 2022).

7. Directive 2013/40/EU of the European Parliament and of the Council on attacks against information systems. — OJ L 218, 14.8.2013.

8. Федеральный закон РФ “Об информации, информационных технологиях и о защите информации”. № 149-ФЗ от 27 июля 2006 г.

9. Cybersecurity Law of the People's Republic of China. 7 November 2016.

10. Qozog‘iston Respublikasi Jinoyat kodeksi. 3-iyul 2014-yil, Ω5-son.

11. O‘zbekiston Respublikasi Jinoyat kodeksi. — Toshkent: Adolat, 2024.

12. O‘zbekiston Respublikasi Prezidentining 2020-yil 15-iyundagi “O‘zbekiston Respublikasida kiberxavfsizlikni ta’minlash tizimini yanada takomillashtirishga doir qo‘shimcha chora-tadbirlar to‘g‘risida”gi PQ-4751-son qarori.

13. Interpol. Cybercrime: A Threat to All. Global Report 2023. — Lyon: Interpol, 2023. — P. 5–20.

14. Mirzayev X.N., Qodirov A.S. Raqamli iqtisodiyotda axborot xavfsizligi muammolari // Huquq va jamiyat. — 2023. — №2. — B. 45–52.

15. Ergashev A.A. O‘zbekistonda kiberxavfsizlik siyosatini shakllantirishning huquqiy jihatlari // Davlat va huquq. — 2022. — №4. — B. 71–78.

16. UNODC. Comprehensive Study on Cybercrime. — Vienna: United Nations, 2023. — P. 30–44.

17. Cybersecurity Ventures. Cybercrime Report 2023: Global Damage Costs. — Northampton, MA, 2023.

18. O‘zbekiston Respublikasi Prezidentining 2021-yil 19-apreldagi “Raqamli O‘zbekiston – 2030” PF-6079-son Farmoni.

19. Xoliqov D.B. Kiberjinoyatchilikda anonim tizimlardan foydalanish va huquqiy muammolar // Yuridik fanlar axborotnomasi. — 2023. — №1. — B. 88–95.

20. Nazarov U.A. Xalqaro kiberxavfsizlik huquqi: shakllanish va rivojlanish tendensiyalari. — Toshkent: TDYU, 2022. — B. 112.