

Date: 1st August-2026

**KIBERJINOYATCHILIKKA QARSHI KURASHISHNING ZAMONAVIY
HUQUQIY MEXANIZMLARI**

Alimuxammadova Gulsevar Xaydar qizi

Nizomiy nomidagi O'zMPU Tarix fakulteti "Milliy g'oya, ma'naviyat asoslari va
huquq ta'limi" yo'nalishi 2-bosqich talabasi

Annotatsiya: Mazkur maqolada kiberjinoyatchilikka qarshi kurashishning zamonaviy huquqiy mexanizmlari ilmiy-nazariy va amaliy jihatdan keng tahlil etilgan. Unda kiberjinoyatlarning tushunchasi, asosiy turlari, transmilliy tabiati, elektron dalillar, raqamli kriminalistika, shaxsga doir ma'lumotlarni himoya qilish, kiberfiribgarlik, sun'iy intellektdan foydalanish bilan bog'liq yangi tahdidlar va profilaktika masalalari yoritilgan. O'zbekiston Respublikasining kiberxavfsizlik sohasidagi qonunchiligi, davlat siyosati va xalqaro huquqiy hamkorlik mexanizmlari tahlil qilinib, huquqiy mexanizmlarni takomillashtirish bo'yicha ilmiy-amaliy takliflar berilgan.

Kalit so'zlar: kiberjinoyatchilik, kiberxavfsizlik, kibermakon, elektron dalil, raqamli kriminalistika, kiberfiribgarlik, fishing, shaxsga doir ma'lumotlar, xalqaro hamkorlik, kipersavodxonlik, sun'iy intellekt.

Аннотация: В статье подробно анализируются современные правовые механизмы противодействия киберпреступности. Рассматриваются понятие и виды киберпреступлений, их транснациональный характер, электронные доказательства, цифровая криминалистика, защита персональных данных, кибермошенничество, новые угрозы искусственного интеллекта и профилактика преступлений. Анализируются законодательство Республики Узбекистан и международное правовое сотрудничество.

Ключевые слова: киберпреступность, кибербезопасность, киберпространство, электронные доказательства, цифровая криминалистика, кибермошенничество, фишинг, персональные данные, международное сотрудничество, киберграмотность, искусственный интеллект.

Abstract: This article provides an extensive scientific and practical analysis of modern legal mechanisms for combating cybercrime. It examines the concept and types of cybercrime, their transnational nature, electronic evidence, digital forensics, personal data protection, cyber fraud, emerging threats involving artificial intelligence, and prevention measures. Uzbekistan's cybersecurity legislation, public policy, and international legal cooperation are analyzed, with practical proposals for strengthening the legal response.

Keywords: cybercrime, cybersecurity, cyberspace, electronic evidence, digital forensics, cyber fraud, phishing, personal data, international cooperation, cyber literacy, artificial intelligence.

Kiberjinoyatchilik zamonaviy axborot jamiyatining eng murakkab va tez o'zgarayotgan huquqiy muammolaridan biridir. Raqamli texnologiyalarning davlat



Date: 1st August-2026



boshqaruvi, bank-moliya tizimi, elektron tijorat, ta'lim, sog'liqni saqlash va kundalik ijtimoiy munosabatlarga keng joriy etilishi jamiyat uchun katta qulayliklar yaratmoqda. Biroq raqamlashtirish jarayoni bilan birga axborot tizimlariga noqonuniy aralashish, ma'lumotlarni o'g'irlash, onlayn firibgarlik, zararli dasturlar tarqatish va boshqa kiberjinoyatlar uchun yangi imkoniyatlar ham paydo bo'lmoqda. Shu sababli kiberjinoyatchilikka qarshi kurashish davlatning huquqiy siyosati, xavfsizlik siyosati va fuqarolarning raqamli madaniyatini birlashtiruvchi kompleks yo'nalishga aylanmoqda. Kiberjinoyatlarning asosiy xususiyatlaridan biri ularning chegarasizligi hisoblanadi. Jinoyat sodir etuvchi shaxs bir davlat hududida joylashgan bo'lsa, hujum qilinayotgan server boshqa mamlakatda, jabrlanuvchi esa uchinchi davlatda bo'lishi mumkin. Natijada jinoyatning yurisdiksiyasini aniqlash, dalillarni olish, gumon qilinuvchini aniqlash va javobgarlikka tortish murakkablashadi. Bundan tashqari, raqamli izlar tez o'zgartirilishi yoki yo'q qilinishi mumkin. Ushbu holat huquqni muhofaza qiluvchi organlardan zamonaviy texnologiyalarni bilish, raqamli kriminalistika va xalqaro hamkorlikdan samarali foydalanishni talab qiladi. Kiberjinoyat tushunchasi keng bo'lib, axborot-kommunikatsiya texnologiyalari jinoyatning nishoni yoki uni sodir etish vositasi bo'lgan qilmishlarni qamrab oladi ya'ni noqonuniy kirish, axborot tizimiga aralashish, ma'lumotlarni o'zgartirish yoki yo'q qilish, zararli dasturlar tarqatish, fishing, onlayn firibgarlik, shaxsni raqamli tarzda taqlid qilish va maxfiy ma'lumotlarni o'g'irlash shular jumlasiga kirib, ushbu jinoyatlarning shakllari texnologik taraqqiyotga mos ravishda yangilanib borayotganligi sababli jinoyat-huquqiy normalarni ham doimiy ravishda takomillashtirish zarur. Kiberjinoyatchilikka qarshi kurashishda huquqiy mexanizm tushunchasi bir nechta o'zaro bog'liq elementlarni qamrab olib, jinoyat sodir etilishini oldini olish, kiberhujumni aniqlash, hodisaga tezkor javob qaytarish, elektron dalillarni to'plash, aybdor shaxsni aniqlash, tergov o'tkazish, sudda dalillarni baholash, javobgarlikni belgilash va zarur hollarda xalqaro huquqiy yordamdan foydalanishdir. Shu jihatdan zamonaviy huquqiy mexanizm faqat jazo chorasi bilan cheklanmay, jinoyatning oldini olish va raqamli muhit xavfsizligini ta'minlashga ham xizmat qilishi kerak.

O'zbekiston Respublikasida kiberxavfsizlikni ta'minlashning muhim huquqiy asoslaridan biri 2022-yil 15-apreldagi O'RQ-764-son "Kiberxavfsizlik to'g'risida"gi qonun, kiberxavfsizlik sohasidagi munosabatlarni tartibga solish, kiberhujumlarning oldini olish, axborot tizimlari va resurslarini himoya qilish hamda vakolatli subyektlarning huquq va majburiyatlarini belgilashga xizmat qiladi. Qonunchilikning mavjudligi davlat organlari, tashkilotlar va fuqarolarning raqamli xavfsizlik bo'yicha mas'uliyatini huquqiy jihatdan mustahkamlash imkonini beradi. Kiberxavfsizlik sohasidagi huquqiy mexanizmlar axborot tizimlari va resurslarini himoya qilish bilan bir qatorda, muhim axborot infratuzilmasini muhofaza qilishga ham qaratilishi lozim. Chunki energetika, bank-moliya, telekommunikatsiya, transport va davlat boshqaruvi tizimlariga qarshi hujumlar alohida shaxsga emas, balki jamiyat va davlatning barqaror faoliyatiga zarar yetkazishi mumkin va shu sababli muhim infratuzilma obyektlarida axborot xavfsizligi talablarini joriy etish, xavflarni baholash va hodisalarga javob berish rejalarini ishlab chiqish huquqiy

Date: 1st August-2026



siyosatning muhim yo‘nalishidir. Shaxsga doir ma‘lumotlarni huquqiy himoya qilish kiberjinoyatchilikka qarshi kurashishning yana bir muhim yo‘nalishidir. 2025-yil 30-apreldagi Prezidentning PQ-153-son qarori axborot texnologiyalari yordamida sodir etiladigan jinoyatlarga qarshi kurashish faoliyatini kuchaytirishga qaratilgan muhim huquqiy hujjatdi hisoblanib, unda kiberjinoyatlarning oldini olish, huquqni muhofaza qiluvchi organlarning faoliyatini takomillashtirish, banklar va to‘lov tashkilotlari bilan hamkorlikni rivojlantirish, aholining kibermadaniyatini oshirish kabi yo‘nalishlarga e‘tibor qaratilgan bo‘lib, mazkur yondashuv jinoyat sodir etilgandan keyin javobgarlik qo‘llash bilan bir qatorda profilaktik choralarni ham kuchaytiradi. 2026-yil 10-martdagi PF-38-son Farmon bilan O‘zbekiston Respublikasining 2026–2030-yillarga mo‘ljallangan Kiberxavfsizlik strategiyasi tasdiqlangani ushbu yo‘nalishdagi davlat siyosatining izchil rivojlanayotganini ko‘rsatadi. Strategik yondashuv davlat axborot tizimlari va muhim axborot infratuzilmasini himoya qilish, kiberhodisalarni monitoring qilish, kiberjinoyatlarning oldini olish, mutaxassislar tayyorlash, aholining kibersavodxonligini oshirish va xalqaro hamkorlikni kuchaytirishga qaratilgan. Bunday kompleks yondashuv kiberxavfsizlikni texnik masala bilan cheklamaslikni taqozo etadi. Elektron dalillar kiberjinoyatlarni tergov qilishning eng muhim vositalaridan biridir. Bolalar va yoshlarning internetdan faol foydalanishi kiberxavfsizlik masalasida alohida e‘tibor talab qiladi. Yoshlar fishing, onlayn firibgarlik, kiberbulling, shaxsiy ma‘lumotlarning noqonuniy tarqalishi va boshqa xavflarga duch kelishi mumkin. Shu bois ta‘lim muassasalarida raqamli xavfsizlik va huquqiy madaniyat bo‘yicha tizimli tushuntirish ishlarini olib borish, ota-onalar va pedagoglarning raqamli savodxonligini oshirish ham kiberjinoyatchilik profilaktikasining muhim qismidir.

Kiberjinoyatlarning transmilliy xususiyati xalqaro huquqiy hamkorlikni kuchaytirishni talab qiladi. Jinoyatchi, jabrlanuvchi va elektron dalil turli davlatlarda joylashgan bo‘lishi mumkin. Bunday vaziyatda o‘zaro huquqiy yordam, tezkor axborot almashish, elektron dalillarni so‘rash, ekstraditsiya va qo‘shma tergov mexanizmlari muhim ahamiyatga ega. Xalqaro hamkorlikning samaradorligi milliy qonunchilikning xalqaro standartlarga uyg‘unligi bilan chambarchas bog‘liq. 2024-yil 24-dekabrda BMT Bosh Assambleyasi Kiberjinoyatchilikka qarshi konvensiyani qabul qildi va xalqaro huquqiy hujjat kiberjinoyatlarning oldini olish, elektron dalillar bilan ishlash va davlatlar o‘rtasidagi hamkorlikni rivojlantirishga qaratilgan. Konvensiyaning qabul qilinishi raqamli jinoyatchilikning global muammoga aylanganini va davlatlar o‘rtasidagi muvofiqlashtirilgan yondashuv zarurligini ko‘rsatadi. Profilaktika kiberjinoyatchilikka qarshi kurashishning eng samarali yo‘nalishlaridan biridir. Kiberhujum sodir bo‘lgandan keyin zarar ko‘rgan tizimni tiklashdan ko‘ra, xavfni oldindan aniqlash va himoya choralarni ko‘rish iqtisodiy va huquqiy jihatdan samaraliroqdir. Shu sababli tashkilotlarda xavfsizlik siyosatini ishlab chiqish, xodimlarni o‘qitish, muntazam audit o‘tkazish, zaxira nusxalarini saqlash va hodisalarga javob berish rejalarini ishlab chiqish muhimdir negaki, kibersavodxonlik fuqarolarning kiberjinoyatlardan himoyalani darajasiga bevosita ta‘sir qiladi. Kuchli parol, ikki bosqichli autentifikatsiya, shubhali havolalarni tekshirish,

Date: 1st August-2026



noma'lum fayllarni ochmaslik va bank ma'lumotlarini begonalarga bermaslik oddiy, ammo samarali profilaktik choralar hisoblanadi. Huquqiy targ'ibot bilan birga bunday amaliy ko'nikmalarni shakllantirish davlat, ta'lim muassasalari, banklar va xususiy sektorning hamkorligini talab qiladi. Kiberjinoyatchilikka qarshi kurashishda davlat organlari va xususiy sektor o'rtasidagi hamkorlik ham muhim. Banklar va to'lov tashkilotlari moliyaviy firibgarlik alomatlarini tez aniqlash, shubhali tranzaksiyalarni tahlil qilish va qonuniy asosda tegishli organlarga ma'lumot taqdim etish orqali jinoyatlarning oldini olishga hissa qo'shadi. Telekommunikatsiya operatorlari esa tarmoq xavfsizligi va kiberhodisalarni aniqlashda muhim rol o'ynaydi. Huquqiy mexanizmlarni takomillashtirishda kiberjinoyatlarning yangi shakllariga moslashuvchan yondashuv zarur. Texnologik rivojlanish qonunchilikdan tezroq kechishi mumkinligi sababli huquqiy normalar umumiy xavflarni qamrab oladigan, biroq inson huquqlarini himoya qiladigan tarzda ishlab chiqilishi lozim. Shu bilan birga, tergov organlari, prokuratura va sudlar uchun elektron dalillarni baholash bo'yicha yagona amaliy standartlarni shakllantirish zarur. Ilmiy nuqtayi nazardan kiberjinoyatchilikka qarshi kurashishning samarali modeli profilaktika, aniqlash, tergov, sudlov va xalqaro hamkorlik bosqichlarining uzviyligini ta'minlashi kerak. Birinchi bosqichda xavflar aniqlanadi va himoya chorasi ko'riladi. Ikkinchi bosqichda kiberhodisa tezkor aniqlanadi. Uchinchi bosqichda elektron dalillar protsessual talablar asosida mustahkamlanadi. Keyingi bosqichda aybdorning harakatlariga huquqiy baho beriladi va zarur hollarda xalqaro hamkorlik mexanizmlari ishga tushiriladi. Kiberxavfsizlikni ta'minlashda huquqiy javobgarlikning muqarrarligi ham muhim ahamiyatga ega. Jinoyatchilar raqamli muhit anonimligi sabab javobgarlikdan qochish mumkin degan tasavvurga ega bo'lmasligi kerak. Buning uchun huquqni muhofaza qiluvchi organlarning texnik imkoniyatlari, tezkor ma'lumot almashish tizimlari va tergovchilarning maxsus bilimlari rivojlantirilishi zarur. Biroq javobgarlikni qo'llash jarayonida aybsizlik prezumpsiyasi va protsessual kafolatlar to'liq saqlanishi lozim.

Umuman olganda, xulosa qilsak, raqamli muhitda xavfsizlikni ta'minlash huquq, texnologiya va jamiyatning birgalikdagi sa'y-harakatini talab qiladi va qonunchilik qanchalik mukammal bo'lmasin, uni amalga oshiradigan malakali kadrlar, zamonaviy texnik infratuzilma va huquqiy madaniyat yetarli bo'lmasa, kiberjinoyatchilikka qarshi kurashish samarasi pasayadi. Shu bois davlat siyosati kompleks yondashuvga asoslanishi kerak. Kiberjinoyatchilikka qarshi kurashish zamonaviy huquq tizimining eng dolzarb yo'nalishlaridan biridir. Uning texnologik murakkabligi, transmilliy xususiyati va elektron dalillarning o'ziga xosligi huquqiy mexanizmlarni muntazam takomillashtirishni talab etadi. O'zbekistonning kiberxavfsizlik sohasidagi qonunchiligi, davlat siyosati va 2026–2030-yillarga mo'ljallangan strategik yondashuvlari ushbu yo'nalishda muhim asos yaratmoqda. Kelgusida raqamli kriminalistika, elektron dalillar, xalqaro huquqiy yordam, profilaktika va kiber savodxonlikni rivojlantirish bilan bir qatorda, shaxsiy hayot daxlsizligi va boshqa inson huquqlarini ta'minlashga ham alohida e'tibor qaratish lozim. Kiberxavfsizlikning barqaror modeli faqat jazolash emas, balki xavfni oldindan aniqlash,

Date: 1st August-2026

fuqarolarni himoya qilish, tashkilotlarning mas'uliyatini oshirish va xalqaro hamkorlikni kuchaytirishga asoslanishi kerak.

FOYDALANILGAN ADABIYOTLAR:

1. Lex.uz O'zbekiston Respublikasining 2022-yil 15-apreldagi O'RQ-764-son "Kiberxavfsizlik to'g'risida"gi Qonuni.
2. Lex.uz O'zbekiston Respublikasi Prezidentining 2025-yil 30-apreldagi PQ-153-son qarori.
3. Lex.uz O'zbekiston Respublikasi Prezidentining 2026-yil 10-martdagi PF-38-son Farmoni.
4. Lex.uz O'zbekiston Respublikasining "Shaxsga doir ma'lumotlar to'g'risida"gi Qonuni.
5. Lex.uz O'zbekiston Respublikasi Jinoyat kodeksi.
6. Lex.uz O'zbekiston Respublikasi Jinoyat-protsessual kodeksi.
7. United Nations. United Nations Convention against Cybercrime. A/RES/79/243.