

**O'ZBEKISTON RESPUBLIKASI JINOYAT
KODEKSIDA KIBER-O'G'RILIK UCHUN
JAVOBGARLIK: MAVJUD NORMALAR TAHLILI VA
TAKOMILLASHTIRISH ISTIQBOLLARI**

Kalbaeva Eldora Uzaqbaevna

*Berdaq nomidagi Qoraqalpoq davlat universiteti Yuridika fakulteti 3-
bosqich talabasi*

**CRIMINAL LIABILITY FOR CYBER THEFT IN THE
CRIMINAL CODE OF THE REPUBLIC OF
UZBEKISTAN: ANALYSIS OF EXISTING NORMS
AND PROSPECTS FOR IMPROVEMENT**

Kalbaeva Eldora Uzaqbaevna

*3rd-year student, Faculty of Law, Karakalpak State University named
after Berdakh*

**УГОЛОВНАЯ ОТВЕТСТВЕННОСТЬ ЗА КИБЕР-
КРАЖУ В УГОЛОВНОМ КОДЕКСЕ РЕСПУБЛИКИ
УЗБЕКИСТАН: АНАЛИЗ СУЩЕСТВУЮЩИХ
НОРМ И ПЕРСПЕКТИВЫ
СОВЕРШЕНСТВОВАНИЯ**

Калбаева Элдора Узақбаевна

*Студентка 3-го курса юридического факультета Каракалпакского
государственного университета имени Бердаха*



[https://orcid.org/0009-
0002-3003-1468](https://orcid.org/0009-0002-3003-1468)

[eldorakalbaeva@gmail.
com](mailto:eldorakalbaeva@gmail.com)

Annotatsiya: O'zbekiston Respublikasi raqamli transformatsiyani jadal amalga oshirayotgan bir paytda, kiberxavfsizlik tahdidlari, jumladan kiber-o'g'rilik muammosi ham dolzarblik kasb etmoqda. Ushbu maqola O'zbekiston Respublikasi Jinoyat kodeksida kiber-o'g'rilik uchun javobgarlikning amaldagi holatini baholashga qaratilgan. Unda mavjud huquqiy normalar tahlil qilinadi, qonunchilikdagi bo'shliqlar va kamchiliklar aniqlanadi hamda xalqaro tajriba asosida takomillashtirish yo'nalishlari taklif etiladi. Maqola O'zbekistonning raqamli makonda xavfsizlikni ta'minlash va barqaror raqamli iqtisodiyotni rivojlantirish borasidagi sa'y-harakatlariga hissa qo'shishni maqsad qilgan.

Kalit so'zlar: kiber-o'g'rilik, kiberxavfsizlik, jinoyat kodeksi, raqamli transformatsiya, Budapesht konvensiyasi, huquqiy bo'shliqlar, raqamli aktivlar, axborot-kommunikatsiya texnologiyalari (AKT), transchegaraviy jinoyatlar, firibgarlik.

Abstract: As the Republic of Uzbekistan rapidly implements digital transformation, cybersecurity threats, including the problem of cyber-theft, are becoming increasingly relevant. This article aims to assess the current state of liability for cyber-theft in the Criminal Code of the Republic of Uzbekistan. It analyzes existing legal norms, identifies gaps and shortcomings in legislation, and proposes directions for improvement based on international experience. The article aims to contribute to Uzbekistan's efforts in ensuring security in the digital space and developing a sustainable digital economy.

Keywords: Cyber-theft, Cybersecurity, Criminal Code, Digital transformation, Budapest Convention, Legal gaps, Digital assets, Information and communication.

Аннотация: В то время как Республика Узбекистан активно осуществляет цифровую трансформацию, угрозы кибербезопасности, включая проблему киберкраж, становятся все более актуальными. Данная статья посвящена оценке текущего состояния ответственности за киберкражу в Уголовном кодексе Республики Узбекистан. В ней анализируются действующие правовые нормы, выявляются пробелы и недостатки в законодательстве, а также предлагаются направления совершенствования на основе международного опыта. Цель статьи – внести вклад в усилия Узбекистана по обеспечению безопасности в цифровом пространстве и развитию устойчивой цифровой экономики.

Ключевые слова: киберкража, кибербезопасность, уголовный кодекс, цифровая трансформация, Будапештская конвенция, Правовые пробелы, цифровые активы, информационно-коммуникационные технологии (ИКТ), трансграничные преступления, мошенничество.

KIRISH

Axborot-kommunikatsiya texnologiyalarining (AKT) jadal rivojlanishi va internetdan foydalanuvchilar sonining ortishi butun dunyo bo'ylab jamiyatlarni kiberjinoyatchilikka nisbatan yanada zaiflashtirdi. O'zbekiston ham raqamli transformatsiya yo'lini tanlagan bir paytda, kiberjinoyatlar uning iqtisodiy barqarorligi, milliy xavfsizligi va fuqarolarining shaxsiy ma'lumotlari himoyasiga jiddiy tahdid solmoqda. Raqamli platformalar va xizmatlar biznesi fuqarolar ma'lumotlarini to'plashda faol bo'lib, bu sohada huquqiy va axloqiy nigilizm kuzatilmoqda, bu esa fuqarolarning huquq va manfaatlarini yetarli darajada himoya qilmasdan raqobatdosh ustunlikka erishish va daromad olish maqsadida yangi texnologiyalardan foydalanishga olib kelmoqda.

Kiberhujumlar va kiberjinoyatchilikning iqtisodiy va ijtimoiy oqibatlari misli ko'rilmagan darajada. Statistik ma'lumotlarga ko'ra, 2021-yilda kiberhujumlar global miqyosda 6 trillion AQSh dollariga teng moddiy zarar yetkazgan, bu esa kiberjinoyatchilikni AQSh va Xitoydan keyin dunyodagi uchinchi yirik iqtisodiyotga aylantiradi [1].

O'zbekiston hukumati raqamli texnologiyalarni iqtisodiyotning barcha sohalariga integratsiya qilish va raqamli makonda tegishli xavfsizlikni ta'minlashning barqaror yo'lida. «Shaxsga doir ma'lumotlar to'g'risida» (2019-yil) hamda «Kiberxavfsizlik to'g'risida»gi (2022-yil 15-aprel) qonunlarning qabul qilinishi mamlakatning raqamli xavfsizlik va axborot xavfsizligi sohasidagi mavqeini yanada mustahkamladi. «Kiberxavfsizlik to'g'risida»gi qonun kiberjinoyatga aniq huquqiy ta'rif berib, uni axborotga kirish, uni o'zgartirish, yo'q qilish yoki axborot tizimlari va resurslarini ishdan chiqarish maqsadida dasturiy va texnik vositalardan foydalangan holda kiberfazoda sodir

etilgan jinoyatlar to'plami sifatida belgilaydi.

Shunga qaramay, mamlakatda hali ham ko'p sonli kiberhujumlar mavjud bo'lib, bu kiberhimoyaning past darajasi, siyosiy yoki iqtisodiy motivlarning mavjudligi, kiber tahdidlarga qarshi kurashda zaif muvofiqlashtirish yoki kiberjinoyatchilar faolligining o'sishini ko'rsatishi mumkin. O'zbekistonning huquqiy bazasi, garchi progressiv bo'lsa-da, kiber tahdidlarning murakkabligiga javob berish uchun rivojlanishi kerak.

ADABIYOTLAR TAHLILI VA METODOLOGIYA

Adabiyotlar tahlili. Kiberjinoyatchilik va unga qarshi kurash masalasi jahon miqyosida va O'zbekistonda ko'plab ilmiy tadqiqotlarning diqqat markazida bo'lib kelmoqda. «Uzbek Journal of Law and Digital Policy» kabi nufuzli nashrlar kiberjinoyatchilik va kiberxavfsizlikka oid maqolalarni chop etib, bu sohadagi huquqiy va texnologik muammolarni o'rganadi. Xususan, kripto-aktivlar bilan bog'liq jinoyatlar, jumladan, kripto-aktivlarni yuvish firibgarlik jinoyati sifatida tahlil qilingan [2]. «Models and Methods in Modern Science» jurnalida chop etilgan maqolalarda O'zbekiston Respublikasi Jinoyat kodeksining kiberjinoyatlarga oid moddalari, jumladan, 169-modda 3-qismi (o'g'rilik) va 278⁵-moddasi (kompyuter sabotaji) bo'yicha tahlillar berilgan. Bu tahlillar kiberjinoyatlarning ko'pincha mulkiy jinoyatlar, masalan, firibgarlik, talonchilik, tovlamachilik bilan bog'liqligini ko'rsatadi.

Xalqaro tajribalarni qiyosiy tahlil qilish O'zbekiston uchun muhim ahamiyatga ega. Budapesht konvensiyasi kiberjinoyatchilik va elektron dalillar bo'yicha eng dolzarb xalqaro kelishuvlardan biri bo'lib, u kompyuterlarga qarshi va kompyuterlar yordamida sodir etilgan jinoyatlarni jinoyat deb hisoblashni nazarda tutadi hamda tergov va elektron dalillarni ta'minlash uchun protsessual huquqiy

vositalarni taqdim etadi. Shunindek, Singapur va Estoniya kabi davlatlar kiberjinoyatchilikka qarshi kurashda proaktiv, ko'p darajali va integrativ huquqiy bazani yaratgan bo'lib, raqamli savodxonlik va xalqaro hamkorlikka katta e'tibor qaratadi [3]. Bu tadqiqotlar kiberjinoyat qonunchiligining doimiy takomillashtirilishi va texnologik taraqqiyotga moslashishi zarurligini ko'rsatadi.

Metodologiya. Ushbu maqolada normativ-huquqiy, qiyosiy-huquqiy va tizimli tahlil usullari qo'llanilgan. Normativ-huquqiy tahlil O'zbekiston Respublikasining amaldagi qonunchilik hujjatlarini, xususan, Jinoyat kodeksi, «Kiberxavfsizlik to'g'risida»gi qonun va «Shaxsga doir ma'lumotlar to'g'risida»gi qonun kabi birlamchi manbalarni chuqur o'rganishga qaratilgan. Bu qonunlar kiberjinoyatlarni tartibga solishning huquqiy asosini belgilaydi.

Qiyosiy-huquqiy tahlil kiber-o'g'rilik uchun javobgarlikni belgilashda xalqaro tajribani, jumladan, Budapesht konvensiyasi hamda AQSh, Yevropa Ittifoqi, Singapur, Estoniya, Germaniya va Buyuk Britaniya kabi davlatlarning qonunchiligini o'rganishga xizmat qiladi. Bu qiyosiy o'rganish O'zbekiston qonunchiligidagi mavjud bo'shliqlarni aniqlash va xalqaro eng yaxshi amaliyotlar asosida takomillashtirish bo'yicha asosli takliflar ishlab chiqish imkonini beradi.

Tizimli yondashuv kiber-o'g'rilikni nafaqat jinoiy-huquqiy, balki kiberxavfsizlik, raqamli huquq va raqamli gigiyena kabi kengroq kontekstda ko'rib chiqishga yordam beradi.

MUHOKAMA

Kiber-o'g'rilikning huquqiy ta'rifi va tasnifi. O'zbekiston qonunchiligida «kiberjinoyat» tushunchasi «Kiberxavfsizlik to'g'risida»gi O'RQ-764-sonli Qonun (2022-yil 15-aprel) bilan aniq belgilangan. Unga ko'ra, kiberjinoyat – axborotni egallash, uni o'zgartirish, yo'q qilish yoki axborot tizimlari va resurslarini ishdan chiqarish maqsadida dasturiy va texnik vositalardan foydalangan holda kiberfazoda sodir etilgan jinoyatlar to'plamidir. Bu ta'rif kiberjinoyatlarning keng doirasini qamrab oladi, ammo «kiber-o'g'rilik» atamasi alohida, mustaqil jinoyat tarkibi sifatida Jinoyat kodeksida to'g'ridan-to'g'ri ta'riflanmagan.

Aksincha, kiber-o'g'rilik holatlari ko'pincha Jinoyat kodeksining umumiy mulkiy jinoyatlarga oid moddalari, xususan, 169-moddasi (o'g'rilik) yoki 168-moddasi (firibgarlik) doirasida ko'rib chiqiladi.

Masalan, mobil telefonini yo'qotib qo'ygan fuqaroning SIM kartasi orqali bank kartasidan ruxsatsiz pul yechib olingan holatda, Jinoyat kodeksining 169-moddasi 3-qismi bilan jinoiy ish qo'zg'atiladi. Bu misol shuni ko'rsatadiki, an'anaviy o'g'rilik moddasi raqamli muhitda sodir etilgan jinoyatlarga tatbiq etilishi mumkin. Biroq, raqamli aktivlarning nomoddiy tabiati, transchegaraviy xususiyati va kiberjinoyatlarning murakkab modus operandi an'anaviy huquqiy tushunchalarni qo'llashda muammolarni keltirib chiqaradi [3]. Kiberjinoyatchilikning harakatlantiruvchi kuchlari va operatsiya sohalari an'anaviy jinoyatlardan sezilarli darajada farq qiladi, bu esa huquqiy tizimdan yanada moslashuvchan va transmilliy yondashuvni talab qiladi.

O'zbekiston Respublikasi Jinoyat kodeksidagi mavjud normalar tahlili. O'zbekiston Respublikasi Jinoyat kodeksining XX¹ bobi «Axborot texnologiyalari sohasidagi jinoyatlar» deb nomlanadi va bir qator kiberjinoyatlarni o'z ichiga oladi. Bu bobdagi moddalar kiberxavfsizlikni ta'minlashga qaratilgan muhim huquqiy asosni tashkil etadi. Ushbu bobdagi 278¹–278⁹-moddalar axborot xavfsizligini ta'minlash, elektron ma'lumotlarni, kompyuter tizimlarini va raqamli infratuzilmani noqonuniy aralashuvlardan himoya qilishga qaratilgan.

Lekin, ushbu moddalar kiberfazodagi turli jinoyatlarni qamrab olsa-da, ular «kiber-o'g'rilik»ni alohida jinoyat tarkibi sifatida to'liq aks ettirmaydi. Ko'pincha, raqamli aktivlarni o'g'rilash holatlari yuqorida keltirilgan moddalar yoki Jinoyat kodeksining 169-moddasi (o'g'rilik) kabi umumiy moddalar orqali kvalifikatsiya qilinadi. Bu esa raqamli o'g'rilikning o'ziga xos xususiyatlarini, masalan, ma'lumotlarning yo'q qilinishi, o'zgartirilishi yoki bloklanishi emas, balki bevosita o'zlashtirilishini to'liq aks ettirishda qiyinchiliklar tug'diradi.

Mavjud kamchiliklar va huquqiy bo'shliqlar. O'zbekistonning kiberjinoyatchilikka qarshi kurashish bo'yicha huquqiy bazasida sezilarli yutuqlarga erishilgan bo'lsa-da, bir qator kamchiliklar va huquqiy bo'shliqlar mavjud bo'lib, ular kiber-o'g'rilik kabi jinoyatlarga qarshi kurashish samaradorligiga ta'sir qiladi:

- **Qonunchilikdagi bo'shliqlar:** Amaldagi qonunlar, jumladan, Jinoyat kodeksi, kripto-valyuta firibgarligi, sun'iy intellektga

asoslangan hujumlar, ransomware (ma'lumotlarni shifrlash va to'lov talab qilish) va deepfake firibgarligi kabi yangi tahdidlarni yetarli darajada qamrab olmaydi. Bu yangi jinoyat turlari uchun aniq ta'riflar va jazo choralari yo'qligi huquqni qo'llovchi organlarning ishini murakkablashtiradi.

- **Yurisdiktsion cheklovlar:** Kiberjinoyatlarning transchegaraviy xususiyati xalqaro hamkorlik shartnomalarining yetarli emasligi sababli ularni ta'qib qilishni qiyinlashtiradi. Jinoyatchilar turli yurisdiksiyalarda joylashgan bo'lishi mumkin, bu esa dalillarni yig'ish, ekstraditsiya va transchegaraviy huquqni muhofaza qilishda qiyinchiliklar tug'diradi.
- **Aholining xabardorligi pastligi:** Kiberxavfsizlik xavflari haqida aholining umumiy xabardorligi pastligi ijtimoiy muhandislik va fishing hujumlariga nisbatan zaiflikni oshiradi. Ko'pchilik fuqarolar o'z shaxsiy ma'lumotlarini himoya qilishning asosiy qoidalariga rioya qilmaydi, bu esa ularni kiber-o'g'rilik qurboniga aylantiradi.
- **Yagona ta'rifning yo'qligi:** «Kiberjinoyat»ning global miqyosda qabul qilingan yagona ta'rifining yo'qligi va «kiberjinoyat» hamda «kompyuter bilan bog'liq jinoyatlar» tushunchalari o'rtasidagi farqni aniqlashdagi qiyinchiliklar huquqiy amaliyotda noaniqliklarni keltirib chiqaradi.

NATIJARAR

O'zbekiston qonunchiligining kiber-o'g'rilik holatlariga tatbiq etilishi samaradorligi. O'zbekiston kiberxavfsizlik sohasida sezilarli yutuqlarga erishgan bo'lsa-da, jumladan, «Kiberxavfsizlik to'g'risida»gi va «Shaxsga doir ma'lumotlar to'g'risida»gi qonunlarni qabul qilgan bo'lsa-da, Jinoyat kodeksining kiber-o'g'rilik holatlariga tatbiq etilishi ko'pincha harakatlarni an'anaviy jinoyat turlari, masalan, 169-modda (o'g'rilik) yoki 168-modda (firibgarlik) bo'yicha qayta kvalifikatsiyalashni talab qiladi. Bu yondashuv, garchi huquqiy asosni ta'minlasa-da, raqamli aktivlar o'g'rilanishining o'ziga xos xususiyatlari, jumladan, aktivlarning nomoddiy tabiati, transchegaraviy xususiyati va jinoyatchilarning global miqyosdagi faoliyatini to'liq hisobga olmasligi mumkin. Jinoyat kodeksining XX¹ bobidagi mavjud moddalar asosan

ruxsatsiz kirish, tizimga aralashish va zararli dasturlarga qaratilgan bo'lib, raqamli aktivlarni bevosita o'zlashtirishni alohida o'g'rilik shakli sifatida aniq belgilamaydi. Bu esa huquqni qo'llovchi organlar uchun yangi va murakkab kiber-o'g'rilik turlarini samarali tergov qilish va jinoiy javobgarlikka tortishda muammolar tug'diradi.

Xalqaro tajribalarning tahlili va O'zbekiston uchun xulosalar. Xalqaro tajribalarni o'rganish O'zbekiston uchun kiber-o'g'rilik qonunchiligini takomillashtirish bo'yicha muhim yo'nalishlarni ko'rsatadi.

Kiberjinoyatchilik bo'yicha Yevropa Kengashining Budapesht konvensiyasi (2001-yil) eng dolzarb xalqaro kelishuvlardan biri bo'lib, u kompyuterlarga qarshi va kompyuterlar yordamida sodir etilgan jinoyatlarni jinoyat deb hisoblashni nazarda tutadi. Konvensiya tergov va elektron dalillarni ta'minlash uchun protsessual huquqiy vositalarni taqdim etadi, shuningdek, xalqaro hamkorlikni kuchaytirishga qaratilgan. Ushbu konvensiyaga to'liq a'zo bo'lish O'zbekistonga xalqaro hamkorlikni sezilarli darajada kuchaytirish va huquqiy bazasini global standartlarga moslashtirish imkoniyatini beradi.

O'zbekiston uchun xulosalar: Qiyosiy tahlil quyidagilarni taqozo etadi:

- **Qonunchilikni yangilash:** Jinoyat kodeksining doirasini kengaytirish, kripto-aktivlarni o'g'rilash, sun'iy intellektga asoslangan firibgarlik kabi yangi kiber-o'g'rilik turlari uchun aniq ta'riflar va jazo choralari kiritish muhimdir.

- **Huquqiy ta'riflarni aniqlashtirish:** Raqamli aktivlarning o'ziga xos xususiyatlarini qamrab oluvchi huquqiy ta'riflarning aniq va ravshan bo'lishini ta'minlash zarur.

- **Xalqaro hamkorlikni kuchaytirish:** O'zbekistonning Budapesht konvensiyasiga to'liq qo'shilishi va o'zaro huquqiy yordam shartnomalarini kuchaytirish transchegaraviy kiberjinoyatlarga qarshi kurashishda samaradorlikni oshiradi.

- **Aholining xabardorligini oshirish:** Fuqarolarni raqamli gigiyena va kiberxavfsizlikning eng yaxshi amaliyotlari bo'yicha o'qitish, ularning kiber tahdidlarga nisbatan zaifligini kamaytiradi.

XULOSA

O'zbekiston Respublikasi Jinoyat kodeksida kiber-o'g'rilik uchun javobgarlikni tahlil qilish shuni ko'rsatadiki, mamlakatda kiberjinoyatchilikka

qarshi kurashish uchun asosiy huquqiy baza mavjud bo'lsa-da, u raqamli makondagi tahdidlarning dinamik rivojlanish sur'atiga to'liq moslasha olmayapti. «Kiberxavfsizlik to'g'risida»gi qonun kiberjinoyat tushunchasini belgilab bergan bo'lsa-da, «kiber-o'g'rilik» alohida jinoyat tarkibi sifatida ajratilmagan, bu esa amaliyotda qiyinchiliklar tug'dirmoqda. Raqamli aktivlarni o'g'rilash holatlari ko'pincha an'anaviy mulkiy jinoyatlarga oid moddalar (masalan, JK 169-moddasi) bo'yicha kvalifikatsiya qilinadi, bu esa raqamli o'g'rilikning o'ziga xos xususiyatlarini to'liq aks ettirmaydi. Qonunchilikdagi bo'shliqlar, xususan, kriptovalyuta firibgarligi, sun'iy intellektga asoslangan hujumlar va deepfake kabi yangi tahdidlarning yetarli darajada qamrab olinmaganligi, shuningdek, huquqni qo'llovchi organlarda resurslar va mutaxassislar yetishmovchiligi, transhegaraviy xususiyatdagi jinoyatlarni ta'qib qilishdagi yurisdiksiyon cheklovlar va aholining kiberxavfsizlik bo'yicha past xabardorligi asosiy kamchiliklar hisoblanadi.

Jinoyat kodeksini takomillashtirish, xalqaro hamkorlikni kuchaytirish, salohiyatni oshirish va mutaxassislarni tayyorlash, aholining raqamli savodxonligini oshirish kabi chora-tadbirlarni amalga oshirish O'zbekistonning kiberjinoyatlarga qarshi kurashish salohiyatini sezilarli darajada oshiradi, raqamli makonda xavfsizlikni ta'minlaydi va raqamli iqtisodiyotning barqaror rivojlanishiga mustahkam huquqiy asos yaratadi.

FOYDALANILGAN ADABIYOTLAR:

1. Zoilboev, J. (2022, avgust). Kiberxavfsizlik, raqamli huquq va raqamli gigiyena – kiberjinoyatchilikka qarshi muqobil yechim. Jamiyat va innovatsiyalar jurnali, 3(6/S), 12-24. <https://doi.org/10.47689/2181-1415-vol3-iss6/S-pp12-24>
2. Uzbek Journal of Law and Digital Policy - IRSHAD JOURNALS, <https://irshadjournals.com/index.php/ujldp>
3. Duha, R. (2024, avgust). Punishment for Cybercrime: A Major Challenge in Modern Legal Systems. Verdict: Journal of Law Science, https://www.researchgate.net/publication/391130350_Punishment_for_Cybercrime_A_Major_Challenge_in_Modern_Legal_Systems

QONUN HUJJATLARI:

1. O'zbekiston Respublikasi Jinoyat kodeksi. (1994-yil 22-sentyabr, 201-I-sonli Qonuni bilan tasdiqlangan). (Oxirgi o'zgartirish va qo'shimchalar bilan).
2. O'zbekiston Respublikasining «Kiberxavfsizlik to'g'risida»gi Qonuni. (2022-yil 21-aprel, O'RQ-764-son).
3. O'zbekiston Respublikasining «Shaxsga doir ma'lumotlar to'g'risida»gi Qonuni. (2019-yil 2-iyul, O'RQ-547-son).
4. Kiberjinoyatchilik to'g'risidagi Konvensiya (Budapesht konvensiyasi). (2001-yil 23-noyabr).

