

O'ZBEKISTON RESPUBLIKASIDA KIBERJINOYATLAR UCHUN JINOIY JAVOBGARLIKNI QÒLLASH MEXANIZMLARINI TAKOMILLASHTIRISH**Islomova Sadoqat Azim qizi****Nazaraliyeva Safina Nasimjon qizi**

Qarshi xalqaro universiteti Ijtimoiy-gumanitar fanlar fakulteti

Milliy g'oya, ma'naviyat asoslari va huquq ta'limi yo'nalishi 3-bosqich talabalari

Aloqa uchun: Tel.+998972799955 +998908930828

islomovasadoqat03@gmail.com safinasafi107@gmail.com<https://doi.org/10.5281/zenodo.17583460>

Anontatsiya. Ushbu maqolada O'zbekiston Respublikasida kiberjinoyatlar uchun jinoiy javobgarlikni qo'llashning huquqiy asoslari, amaldagi mexanizmlar va ularni takomillashtirish yo'llari tahlil etilgan. Axborot texnologiyalarining jadal rivojlanishi kiberxavfsizlikni ta'minlash va raqamli makonda jinoiyatlarning oldini olish masalalarini dolzarb qilib qo'ymoqda. Shu boisdan, kiberjinoyatlarga qarshi kurashishda xalqaro tajriba, milliy qonunchilik va huquqni qo'llash amaliyotini uyg'unlashtirish zarurligi asoslab berilgan. Maqolada shuningdek, jinoiyat kodeksiga kiritilishi lozim bo'lgan o'zgartishlar, tergov va sud amaliyotida raqamli dalillardan foydalanish mexanizmlari hamda huquqni muhofaza qiluvchi organlarning salohiyatini oshirish bo'yicha takliflar ilgari surilgan.

Kalit sòzlar: kiberjinoyat, kiberxavfsizlik, jinoiy javobgarlik, raqamli texnologiyalar, axborot xavfsizligi, huquqiy mexanizm, raqamli dalillar, O'zbekiston Respublikasi qonunchiligi, xalqaro tajriba, huquqni qo'llash amaliyoti.

Аннотация. В статье анализируются правовые основы применения уголовной ответственности за киберпреступления в Республике Узбекистан, существующие механизмы и пути их совершенствования. Стремительное развитие информационных технологий актуализирует вопросы обеспечения кибербезопасности и предупреждения преступлений в цифровом пространстве. В связи с этим обосновывается необходимость гармонизации международного опыта, национального законодательства и правоприменительной практики в сфере борьбы с киберпреступлениями. В статье также выдвигаются предложения по внесению изменений в Уголовный кодекс, механизм использования цифровых доказательств в следственной и судебной практике, повышению потенциала правоохранительных органов.

Ключевые слова: киберпреступность, кибербезопасность, уголовная ответственность, цифровые технологии, информационная безопасность, правовой механизм, цифровые доказательства, законодательство Республики Узбекистан, международный опыт, правоприменительная практика.

Anontation. This article analyzes the legal framework for the application of criminal liability for cybercrimes in the Republic of Uzbekistan, existing mechanisms and ways to improve them. The rapid development of information technologies makes the issues of ensuring cybersecurity and preventing crimes in the digital space relevant. Therefore, the need to harmonize international experience, national legislation and law enforcement practice in combating cybercrimes is substantiated. The article also puts forward proposals for amendments to the Criminal Code, mechanisms for using digital evidence in investigation and judicial practice, and increasing the capacity of law enforcement agencies.

Keywords: *cybercrime, cybersecurity, criminal liability, digital technologies, information security, legal mechanism, digital evidence, legislation of the Republic of Uzbekistan, international experience, law enforcement practice.*

So‘nggi yillarda axborot-kommunikatsiya texnologiyalarining jadal rivojlanishi inson faoliyatining barcha sohalariga chuqur kirib bordi. Raqamli iqtisodiyot, elektron hukumat, onlayn ta‘lim va elektron tijorat tizimlarining keng qo‘llanilishi jamiyatning samaradorligini oshirayotgan bo‘lsa-da, shu bilan birga yangi turdagi xavf-xatarlarni ham yuzaga keltirmoqda.

Ana shunday tahdidlar qatorida kiberjinoyatlar eng xavfli va murakkab toifaga kiradi.

Kiberjinoyatlar nafaqat shaxsiy manfaatlarga zarar yetkazadi, balki davlatning axborot infratuzilmasi, iqtisodiy barqarorligi hamda milliy xavfsizligiga jiddiy tahdid soladi. Shu sababli, ushbu jinoyatlarga nisbatan samarali huquqiy choralarni qo‘llash, ularning oldini olish va jazolash mexanizmlarini takomillashtirish bugungi kunda dolzarb masalaga aylangan.

O‘zbekiston Respublikasi so‘nggi yillarda kiberxavfsizlik sohasida mustahkam huquqiy asos yaratish, xalqaro standartlarga mos mexanizmlarni joriy etish hamda huquqni muhofaza qiluvchi organlarning salohiyatini oshirish yo‘lida qator islohotlarni amalga oshirmoqda. Shu bilan birga, global miqyosdagi texnologik o‘zgarishlar va kiberjinoyatchilik usullarining murakkablashib borayotgani mavjud tizimni doimiy ravishda yangilab borishni taqozo etmoqda.

Mazkur maqolada O‘zbekiston Respublikasida kiberjinoyatlar uchun jinoiy javobgarlikni qo‘llash amaliyoti, uning huquqiy mexanizmlari va ularni yanada takomillashtirish bo‘yicha takliflar ilmiy tahlil asosida ko‘rib chiqiladi.

Zamonaviy dunyoda axborot texnologiyalari inson faoliyatining ajralmas qismiga aylangan bo‘lib, iqtisodiyot, ta‘lim, tibbiyot, boshqaruv va hatto shaxsiy muloqot sohalarini ham raqamli makonga ko‘chirdi. Biroq, bu jarayon bilan bir qatorda, texnologik imkoniyatlardan g‘arazli maqsadlarda foydalanish holatlari ham ko‘paymoqda. Ana shunday salbiy faoliyat turlari umumiy holda “kiberjinoyatlar” deb ataladi. “Kiberjinoyat” atamasi ilk bor XX asrning oxirida, internet tarmog‘ining keng tarqala boshlagan davrida paydo bo‘lgan. Bugungi kunda bu tushuncha nafaqat texnik vositalardan foydalanib sodir etilgan jinoyatlarni, balki raqamli muhitda sodir bo‘ladigan huquqbuzarliklarning keng doirasini qamrab oladi.

Birlashgan Millatlar Tashkiloti (BMT) va Yevropa Kengashi ekspertlarining ta‘riflariga ko‘ra, kiberjinoyat - bu axborot tizimlari, kompyuter tarmoqlari yoki raqamli qurilmalardan foydalanish orqali jinoyat sodir etish jarayonidir. O‘zbekiston Respublikasining amaldagi qonunchiligida “kiberjinoyat” atamasi to‘g‘ridan-to‘g‘ri belgilab qo‘yilmagan bo‘lsa-da, Jinoyat kodeksining 278¹–278³-moddalarini orqali “axborot tizimlariga noqonuniy kirish”, “kompyuter ma‘lumotlarini buzish yoki yo‘q qilish”, “axborot resurslaridan ruxsatsiz foydalanish” kabi qilmishlar kiberjinoyatlar sirasiga kiradi.

Kiberjinoyatlar o‘z mohiyatiga ko‘ra juda xilma-xil bo‘lib, ularning har biri texnik usul, maqsad va oqibat jihatidan farq qiladi. Quyida eng keng tarqalgan turlar keltirilgan:

1. Axborot tizimlariga noqonuniy kirish – begona shaxsning ruxsatisiz kompyuter yoki tarmoqqa kirish orqali ma‘lumotlarni olish, o‘zgartirish yoki yo‘q qilish.
2. Zararli dasturlar tarqatish – foydalanuvchining axborot tizimiga zarar yetkazuvchi yoki ma‘lumotlarni yashirin tarzda o‘g‘iraydigan dasturlarni joylashtirish.
3. Onlayn firibgarlik – internet orqali aldov yo‘li bilan foyda olish, soxta saytlar yoki elektron to‘lov tizimlari orqali moliyaviy zarar yetkazish.

4. Shaxsiy ma'lumotlarni o'g'irlash – foydalanuvchilarning parol, shaxsiy identifikatsiya raqami, bank ma'lumotlarini noqonuniy yo'l bilan qo'lga kiritish.

5. Kiberterrorizm va davlatga qarshi kiberhujumlar– strategik axborot tizimlariga (energetika, transport, mudofaa tizimlari va h.k.) zarar yetkazish orqali davlat xavfsizligiga tahdid solish.

6. Onlayn ta'qib – ijtimoiy tarmoqlarda shaxsni obro'sizlantirish, ruhiy bosim o'tkazish yoki sha'ni va qadr-qimmatiga tajovuz qilish. Bu turlar orasida eng xavflilari iqtisodiy yo'nalishdagi va davlat axborot tizimlariga qaratilgan jinoyatlar bo'lib, ular nafaqat alohida shaxs, balki butun jamiyat va davlat manfaatlariga zarar yetkazadi.

Kiberjinoyatlarning oqibatlarini ko'pincha ko'zga ko'rinmas, ammo nihoyatda jiddiy bo'ladi. Ular iqtisodiy yo'qotishlar, axborot maxfiyligining buzilishi, fuqarolarning huquqiy himoyasining susayishi hamda davlatning axborot suverenitetiga tahdid soladi. Shu sababdan, kiberjinoyatlarni aniqlash va ularning oldini olish uchun nafaqat huquqiy, balki texnologik, tashkiliy va ta'limiy choralar majmuasi zarur hisoblanadi.

Kiberjinoyat - bu axborot-kommunikatsiya vositalari, kompyuter tarmoqlari va raqamli qurilmalar yordamida sodir etiladigan huquqbuzarliklarning umumiy atamasidir. U an'anaviy jinoyatlardan mexanik jihatdan - vosita va vositachilarda; mazmunan esa - maqsad, ob'ekt va oqibatlar nuqtai nazaridan farq qiladi. Kiberjinoyatlar quyidagi xususiyatlar bilan ajralib turadi:

Virtual vositalik: jinoyatning vositasi - axborot tizimi yoki uning komponentlari; aniq fizik to'qnashuv yo'q.

Anonimlik va global xarakter: hujumchilar geografik chegaralarni chetlab o'tishi va anonim usullar orqali harakat qilishi mumkin.

Tez tarqalish: zararli kodlar yoki xakerlik operatsiyalari qisqa vaqt ichida keng tizimlarga yoyilib katta miqdorda iqtisodiy va operatsion zarar yetkazishi mumkin.

Texnik murakkablik: huquqni muhofaza qilish va ekspertiza talablarining yuqoriligi - raqamli izlarni aniqlash, saqlash va tahlil qilish qiyin.

Maxfiylik buzilishi va qaytarilmas oqibatlar: ma'lumotlarni nusxa ko'chirish yoki tarqatish qaytarilmas zarar keltirishi mumkin.

Kiberjinoyatlar ko'plab mezonlarga ko'ra guruhlanadi: maqsad, texnika, nishon va oqibat bo'yicha. Quyida amaliy jihatdan eng muhim kategoriyalar bayon etiladi:

1. Ruxsatsiz kirish: axborot tizimlariga ruxsatsiz kirish, foydalanuvchi hisoblarini buzish, serverlarga hujumlar. (Bu tur JKning tegishli moddalarida nazarda tutiladi).

2. Ma'lumotlarni o'zgartirish yoki yo'q qilish: ma'lumotlarni modifikatsiyalash, fayllarni shifrlash, ma'lumotlar bazasini buzish. Bu tur davlat yoki biznes infratuzilmasiga jiddiy zarar yetkazishi mumkin.

3. Zararli dasturlar tarqatish: foydalanuvchi qurilmasiga maxfiy kirish yoki ma'lumotlarni o'g'irlash uchun mo'ljallangan dasturlarni tarqatish.

4. Moliyaviy va onlayn firibgarlik: to'lov ma'lumotlarini o'g'irlash, soxta to'lov sahifalari yoki identifikatsiya bilgilaridan foydalanib moliyaviy zarar yetkazish.

5. Shaxsiy ma'lumotlarni o'g'irlash va identifikatsiya o'g'irligi: parollar, davlat identifikatorlari, bank ma'lumotlarini noqonuniy qo'lga kiritish va ular bilan noqonuniy operatsiyalarni amalga oshirish.

6. Kiberterrorizm va strategik infratuzilmaga hujumlar: energetika, transport, sog'liqni saqlash kabi tizimlarga hujum qilib fuqarolarning xavfsizligiga yoki davlat funksiyalariga tahdid solish.

7. Axborot manipulyatsiyasi va noto'g'ri xabar tarqatish: siyosiy yoki ijtimoiy beqarorlikni keltirib chiqarish maqsadida onlayn manipulyatsiyalardan foydalanish.

O'zbekistonning jinoyat va ma'muriy javobgarlik tizimi so'nggi yillarda axborot texnologiyalari sohasidagi tahdidlarni hisobga olib yangilandi. Kiberxavfsizlik va axborot sohasini tartibga soluvchi bir qator asosiy hujjatlar mavjud.

1. O'zbekiston Respublikasi Jinoyat kodeksi - axborot-texnologiyalar yordamida sodir etiladigan jinoyatlar (jumladan, axborot tizimlariga ruxsatsiz kirish, ma'lumotlarni buzish) uchun alohida moddalar belgilangan. Jinoyat kodeksi mazkur huquqbuzarliklarni maxsus boblar orqali tartibga soladi.

2. "Kiberxavfsizlik to'g'risida"gi qonun kiberxavfsizlik sohasidagi munosabatlarni keng qamrovda tartibga solish, tizimlar xavfsizligini ta'minlash va javobgarlik mexanizmlarini belgilashga qaratilgan. Ushbu Qonun kiberxavfsizlik siyosati, operatorlar majburiyatlari va favqulodda holatlar bo'yicha norma va mexanizmlarni belgilaydi.

3. "Axborotlashtirish to'g'risida"gi Qonun va boshqa normativ aktlar - axborot tizimlarini joriy etish, ma'lumotlarni himoya va axborot resurslaridan foydalanish qoida-me'yorlari. So'nggi yillarda qabul qilingan qaror va farmoyishlar (masalan, 2024 va 2025 yillardagi normativ yangilanishlar) axborot texnologiyalari sohasida javobgarlikni kuchaytirish va ishlash mexanizmlarini takomillashtirishga xizmat qilmoqda.

Jinoyat kodeksi axborot sohasidagi huquqbuzarliklarni aniqlash va jazolash uchun maxsus mexanizmlar belgilaydi. Amaliy nuqtai nazardan quyidagilar muhim:

Maxsus modda va kategoriyalar: axborot tizimlariga ruxsatsiz kirish, axborot resurslarini buzish, ruxsatsiz foydalanish kabi xatti-harakatlar alohida modda yoki modda guruhlari bilan jazolanadi. Bu moddalarning talqini va qo'llanilishi amalda tergovning texnik jihatlariga moslashtirilishi kerak. Jazolar va protsessual choralar: jazo choralari moddaga va oqibatga qarab jarima, ozodlikdan mahrum etish yoki ma'lum huquqlardan mahrum qilish kabi ko'rinishda belgilangan. Protssesual jihatdan esa dastlabki tekshiruv, raqamli izlarni saqlash va ekspertizalar muhim rol o'ynaydi.

Raqamli dalillarning ta'limi va yaroqliligi: jinoyat protsessi doirasida raqamli dalillarni to'g'ri yig'ish, zanjirlash va ekspertiza qilish uchun maxsus protseduralar zarur - bu dalillarning sudda qabul qilinishini ta'minlaydi.

Kiberjinoyatlarni ochish va sudda isbotlash bir qancha o'ziga xos protsessual muammolarni yuzaga keltiradi. Dalilni himoya va saqlash muammosi: raqamli dalillar oson o'zgartirilishi yoki yo'qolishi mumkin; shuning uchun dalil zanjiri (chain of custody) va hash-metodlari qo'llanilishi talab etiladi. Texnik ekspertizalarning yetishmasligi: mamlakatda yetarlicha malakali kiber-ekspertlar, laboratoriyalar va texnik jihozlar talab darajasida bo'lishi shart. Xalqaro ma'lumot almashinuvi: ko'p jinoyatlar chegara bo'ylab amalga oshirilgani sababli chet el organlari bilan tezkor ma'lumot almashinuvi va huquqiy yordam mexanizmlari muhim. O'zbekiston xalqaro hamkorlikni kengaytirib, muvofiqlashtirilgan tartiblarni mustahkamlashga e'tibor qaratmoqda.

O'zbekiston Respublikasida so'nggi yillarda kiberjinoyatlarni aniqlash, ularning oldini olish va jinoiy javobgarlikni ta'minlash sohasida bir qator islohotlar amalga oshirilgan. 2022-yilda qabul qilingan "Kiberxavfsizlik to'g'risida"gi Qonun mamlakatda axborot xavfsizligini mustahkamlash, tizimli nazoratni kuchaytirish va javobgarlik mexanizmlarini aniqlashtirishda muhim bosqich bo'ldi.

Shuningdek, "Raqamli O'zbekiston – 2030" strategiyasi doirasida raqamli muhit xavfsizligini ta'minlash, davlat axborot resurslarini himoya qilish va fuqarolarning shaxsiy ma'lumotlarini kafolatlash masalalari davlat siyosati darajasiga ko'tarildi. Biroq amaliyotda hali ham qator tizimli muammolar saqlanib qolmoqda. Avvalo, kiberjinoyatlarni aniqlash va tergov qilishda texnik vositalar hamda maxsus mutaxassislar yetishmovchiligi mavjud. Ayrim holatlarda jinoyat izlari - raqamli dalillar - to'g'ri yig'ilmagani yoki saqlanmagani sababli sudda ularning ishonchliligi shubha ostida qoladi. Raqamli dalillarni ekspertiza qilish, ularni protsessual jihatdan mustahkamlash va sudda dalil sifatida tan olish amaliyoti hali yetarli darajada yo'lga qo'yilmagan. Kiberjinoyatlarga qarshi kurashish mexanizmlarini takomillashtirish bir nechta asosiy yo'nalishlarda olib borilishi lozim.

Birinchidan, Jinoyat kodeksiga zamonaviy raqamli jinoyatlar shakllarini aniq belgilovchi yangi modda va izohlarni kiritish zarur. Masalan, kriptovalyuta bilan bog'liq firibgarlik, raqamli shaxsni o'g'irlash, onlayn ta'qib va zararli kontent tarqatish kabi xatti-harakatlar uchun javobgarlik mexanizmlarini aniq va to'liq shaklda belgilash talab etiladi. Ikkinchidan, huquqni muhofaza qiluvchi organlar tarkibida kiberjinoyatlarga ixtisoslashgan maxsus bo'linmalar faoliyatini kuchaytirish va ularni zamonaviy texnik vositalar bilan ta'minlash muhimdir. Har bir tergovchi yoki prokuror raqamli dalillarni to'plash, saqlash va tahlil qilish bo'yicha maxsus malakaga ega bo'lishi kerak. Shu maqsadda, O'zbekiston Respublikasi Ichki ishlar vazirligi va

Bosh prokuratura tizimida kiberxavfsizlik akademiyasi yoki o'quv markazlarini tashkil etish amaliy jihatdan dolzarbdir. Uchinchidan, raqamli dalillar bilan ishlash bo'yicha yagona protsessual standartishlab chiqish zarur. Hozirda dalillarni yig'ish va saqlash bo'yicha yagona texnik reglament yo'qligi sababli, sudlar bu dalillarni turlicha talqin qilmoqda. To'rtinchidan, xalqaro hamkorlik va axborot almashinuvi tizimini kengaytirish talab etiladi. O'zbekiston Interpol, va MDH davlatlari bilan mavjud hamkorlik asosida kiberjinoyatlarni oldini olish bo'yicha tezkor ma'lumot almashish protokollarini joriy etishi zarur. Shuningdek, qo'shni davlatlar bilan qo'shma tergov guruhlarini tashkil etish mexanizmini yo'lga qo'yish ham muhim amaliy choradir. Beshinchidan, jamiyatda kiberxavfsizlik madaniyatini shakllantirish zarur.

Aksariyat kiberjinoyatlar texnik sababdan emas, balki inson omili – e'tiborsizlik, xabardorlikning pastligi yoki oddiy ehtiyotsizlik natijasida sodir bo'ladi. Shu bois, o'quv yurtlari, davlat idoralari va xususiy tashkilotlarda axborot xavfsizligi bo'yicha muntazam o'quv mashg'ulotlari o'tkazish, ommaviy axborot vositalarida profilaktik kampaniyalar tashkil etish foydali natija beradi. Kiberjinoyatlarga qarshi kurashish faqat jazolash bilan emas, balki oldini olish, ogohlantirish va profilaktika bilan uyg'un bo'lishi lozim. Shu maqsadda, davlat organlari, fuqarolik jamiyati institutlari va IT sohasi vakillari o'rtasida o'zaro hamkorlikni mustahkamlash talab etiladi.

Kiberjinoyatlar bugungi kunda davlatlar suvereniteti, iqtisodiy barqarorlik va fuqarolar xavfsizligiga tahdid soluvchi eng jiddiy xavflardan biri sifatida e'tirof etilmoqda. Ularning tezkor rivojlanishi, murakkab texnik tabiati va global xarakteri sababli, bu sohada milliy qonunchilikni muntazam yangilab borish zarur. O'zbekiston Respublikasi kiberjinoyatlarga qarshi kurashish yo'lida sezilarli yutuqlarga erishgan bo'lsa-da, xalqaro tajriba va texnologik rivojlanish sur'atlarini inobatga olgan holda, mavjud mexanizmlarni yanada takomillashtirish dolzarbdir. Xulosa qilib aytganda, samarali kiberjinoyatlarga qarshi kurashish tizimini yaratish uchun quyidagilar ustuvor yo'nalish sifatida e'tirof etilishi lozim:

- jinoiy javobgarlikni belgilovchi normativ-huquqiy bazani takomillashtirish;
- raqamli dalillar bilan ishlash standartlarini ishlab chiqish;

- tergov va sud organlarining texnik salohiyatini kuchaytirish;
- xalqaro hamkorlik va axborot almashinuvi tizimini mustahkamlash;
- fuqarolarda kiberxavfsizlik madaniyatini shakllantirish.

Ana shu yo‘nalishlarda kompleks yondashuvni qo‘llash, kiberjinoyatlarga qarshi kurashni nafaqat huquqiy, balki axloqiy va ijtimoiy jarayon sifatida tashkil etish, O‘zbekiston Respublikasining axborot makonidagi barqarorligini ta‘minlaydi va milliy xavfsizlikning muhim omillaridan biriga aylanadi.

Foydalanilgan adabiyotlar ro‘yxati

1. Ozbekiston Respublikasi Konstitutsiyasi <https://lex.uz/docs/-6445145>
2. O‘zbekiston Respublikasi Jinoyat kodeksi <https://lex.uz/docs/-111453>
3. O‘zbekiston Respublikasi Kiberxavfsizlik to‘g‘risidagi qonun <https://lex.uz/uz/docs/-5960604>
4. O‘zbekiston Respublikasi Axborotlashtirish to‘g‘risidagi qonun <https://lex.uz/docs/-83472>
5. O‘zbekiston Respublikasi Prezidenti farmoni “Raqmli O‘zbekiston – 2030” <https://lex.uz/ru/docs/-5030957>