Ilmiy tadqiqotlar va ularning yechimlari jurnali
Aoka guvohnoma № 323759 ISSN: 3060-4818

O’ZBEKISTON RESPUBLIKASI QONUNCHLIGIDA KIBERJINOYATCHILIKKA QARSHI KURASH

Maxmudova Shohsanam
Toshkent davlat yuridik universiteti
Xalqaro huquq va qiyosiy
huquqshunoslik fakulteti 3-kurs talabasi
https://doi.org/10.5281/zenodo.24133717

Annotatsiya: Raqamli iqtisodiyotning jadal rivojlanishi natijasida axborot-kommunikatsiya texnologiyalari davlat boshqaruvi, bank-moliya tizimi, elektron tijorat, ta'lim va sog'liqni saqlash kabi ko'plab sohalarning ajralmas qismiga aylandi. Mazkur jarayon jamiyat taraqqiyoti uchun yangi imkoniyatlarni yaratishi bilan bir qatorda, kiberjinoyatchilikning murakkab va transmilliy shakllarini ham yuzaga keltirmoqda. Kiberhujumlar, noqonuniy kirish, fishing, zararli dasturlar, ransomware, shaxsga doir ma'lumotlarni o'g'irlash hamda sun'iy intellekt yordamida sodir etilayotgan firibgarliklar zamonaviy huquqni qo'llash amaliyotida eng dolzarb muammolardan biri sifatida namoyon bo'lmoqda.

Mazkur maqolada O'zbekiston Respublikasida kiberjinoyatchilikka qarshi kurashning huquqiy asoslari kompleks tahlil qilinadi. Tadqiqot davomida Konstitutsiya, Jinoyat kodeksi, "Kiberxavfsizlik to'g'risida"gi Qonun, "Shaxsga doir ma'lumotlar to'g'risida"gi Qonun hamda sohaga oid boshqa normativ-huquqiy hujjatlar o'rganildi. Shuningdek, Budapesht konvensiyasi, Yevropa Ittifoqi davlatlari, Estoniya, Singapur va AQSH tajribasi bilan qiyosiy tahlil o'tkazildi.

Tadqiqot natijalariga ko'ra, O'zbekistonda kiberxavfsizlikni ta'minlash bo'yicha muhim huquqiy baza yaratilgan bo'lsa-da, sun'iy intellekt, deepfake texnologiyalari, kriptoaktivlar, elektron dalillar va transchegaraviy kiberjinoyatlar bilan bog'liq huquqiy normalarni yanada takomillashtirish zarur. Shuningdek, elektron dalillar bilan ishlashning yagona protsessual mexanizmlarini ishlab chiqish, xalqaro hamkorlikni kuchaytirish hamda kiberjinoyatlarning oldini olishga qaratilgan profilaktik choralarni rivojlantirish bo'yicha ilmiy-amaliy takliflar ishlab chiqildi.

Kalit so'zlar: kiberjinoyat, kiberxavfsizlik, axborot xavfsizligi, kiberfiribgarlik, raqamli transformatsiya, Jinoyat kodeksi, Budapesht konvensiyasi, sun'iy intellekt, fishing.

I. Kirish

XXI asr axborot texnologiyalari va raqamli iqtisodiyotning jadal rivojlanishi bilan tavsiflanadi. Davlat boshqaruvi, bank-moliya tizimi, elektron tijorat, ta'lim, sog'liqni saqlash va boshqa ko'plab sohalarda raqamli texnologiyalarning keng qo'llanilishi iqtisodiy samaradorlikni oshirish, davlat xizmatlarining shaffofligini ta'minlash hamda fuqarolar uchun qulay imkoniyatlar yaratishga xizmat qilmoqda. O'zbekiston Respublikasida ham "Raqamli O'zbekiston – 2030" strategiyasi doirasida davlat xizmatlarini elektron shaklga o'tkazish, elektron hukumat tizimini rivojlantirish, raqamli iqtisodiyotni kengaytirish hamda zamonaviy axborot-kommunikatsiya texnologiyalarini joriy etish bo'yicha izchil islohotlar amalga oshirilmoqda. Biroq raqamlashtirish jarayonlarining jadallashuvi bilan bir qatorda yangi turdagi tahdidlar ham yuzaga kelmoqda. Bugungi kunda kiberjinoyatchilik dunyo miqyosida eng tez rivojlanayotgan jinoyat turlaridan biri sifatida e'tirof etilmoqda. Kompyuter tizimlariga noqonuniy kirish,

bank kartalari orqali firibgarlik, fishing hujumlari, zararli dasturlarni tarqatish, davlat axborot tizimlariga kiberhujumlar uyushtirish, shaxsga doir ma'lumotlarni o'g'irlash va ulardan noqonuniy foydalanish nafaqat iqtisodiyotga, balki davlat xavfsizligi va jamoat tartibiga ham jiddiy tahdid solmoqda.

Kiberjinoyatlar an'anaviy jinoyatlardan o'zining transmilliy xususiyati, anonimligi, yuqori texnologik murakkabligi va qisqa vaqt ichida katta miqdordagi moddiy zarar yetkazish imkoniyati bilan farqlanadi. Jinoyatchining bir davlat hududida turib boshqa davlatdagi axborot tizimiga hujum uyushtirishi yoki uchinchi davlat serverlaridan foydalanishi huquqni muhofaza qiluvchi organlar faoliyatini murakkablashtiradi. Shu sababli kiberjinoyatchilikka qarshi kurash nafaqat milliy qonunchilik, balki xalqaro hamkorlikni ham talab qiladigan yo'nalishlardan biri hisoblanadi. So'nggi yillarda O'zbekistonda ham kiberjinoyatlar sonining sezilarli darajada oshgani kuzatilmoqda. Ichki ishlar organlari va kiberxavfsizlik sohasidagi vakolatli organlar ma'lumotlariga ko'ra, ayniqsa bank kartalari orqali firibgarlik, mobil ilovalar yordamida sodir etilayotgan aldovlar, fishing havolalari, ijtimoiy tarmoqlar orqali noqonuniy mablag' yig'ish va shaxsiy ma'lumotlarni qo'lga kiritish bilan bog'liq jinoyatlar keskin ko'paygan. Bu esa amaldagi huquqiy mexanizmlarning samaradorligini oshirish va zamonaviy tahdidlarga moslashtirish zaruratini yuzaga keltirmoqda. Mazkur muammolarni bartaraf etish maqsadida O'zbekiston Respublikasida bir qator normativ-huquqiy hujjatlar qabul qilindi. Jumladan, 2022-yilda "Kiberxavfsizlik to'g'risida"gi Qonunning qabul qilinishi mazkur sohada yagona davlat siyosatini shakllantirish, muhim axborot infratuzilmasini himoya qilish, vakolatli organlarning faoliyatini muvofiqlashtirish hamda kiberhodisalarga tezkor javob berishning huquqiy asoslarini yaratdi. Shuningdek, Jinoyat kodeksi, "Shaxsga doir ma'lumotlar to'g'risida"gi, "Axborotlashtirish to'g'risida"gi va boshqa qonunlar kiberjinoyatchilikning turli ko'rinishlariga qarshi kurashishda muhim huquqiy asos bo'lib xizmat qilmoqda.

Biroq amaliyot shuni ko'rsatmoqdaki, texnologiyalar huquqiy tartibga solishdan tezroq rivojlanmoqda. Sun'iy intellekt asosida yaratilayotgan deepfake materiallar, generativ AI vositalari yordamida sodir etilayotgan firibgarliklar, kriptoaktivlardan foydalangan holda pul yuvish, bulutli texnologiyalar orqali amalga oshirilayotgan kiberhujumlar hamda elektron dalillar bilan ishlashdagi protsessual muammolar milliy qonunchilikni yanada takomillashtirishni talab etmoqda.

Mazkur maqolaning asosiy maqsadi O'zbekiston Respublikasida kiberjinoyatchilikka qarshi kurashning huquqiy asoslarini kompleks tahlil qilish, mavjud qonunchilikning afzallik va kamchiliklarini aniqlash, xalqaro tajriba bilan qiyosiy tahlil o'tkazish hamda sohaga oid ilmiy-amaliy takliflarni ishlab chiqishdan iborat.

II.Metodologiya

Mazkur tadqiqot O'zbekiston Respublikasida kiberjinoyatchilikka qarshi kurashning huquqiy asoslarini kompleks tahlil qilishga qaratilgan bo'lib, unda bir- birini to'ldiruvchi ilmiy tadqiqot usullaridan foydalanildi. Maqolaning asosiy metodologik asosini normativ-huquqiy tahlil tashkil etdi. Ushbu usul yordamida O'zbekiston Respublikasi Konstitutsiyasi, Jinoyat kodeksi, "Kiberxavfsizlik to'g'risida"gi O'RQ–764-son Qonuni, "Shaxsga doir ma'lumotlar to'g'risida"gi, "Axborotlashtirish to'g'risida"gi, "Axborot erkinligi prinsiplari va kafolatlari to'g'risida"gi qonunlar hamda kiberxavfsizlik sohasini tartibga soluvchi boshqa normativ-huquqiy hujjatlar o'rganildi. Mazkur hujjatlar asosida O'zbekistonda kiberjinoyatchilikka qarshi kurashishning huquqiy mexanizmlari, davlat organlarining vakolatlari va mavjud tartib-taomillar tahlil qilindi. Maqolada qiyosiy-huquqiy usul ham

qo'llanildi. Mazkur usul orqali O'zbekiston qonunchiligi Budapesht konvensiyasi, Yevropa Ittifoqining NIS2 direktivasi, AQSHning Computer Fraud and Abuse Act (CFAA), Singapur hamda Estoniyaning kiberxavfsizlik sohasidagi qonunchiligi bilan taqqoslandi. Qiyosiy tahlil milliy qonunchilikning ustun va zaif jihatlarini aniqlash, xalqaro tajribaning ijobiy elementlarini baholash imkonini berdi. Bundan tashqari, analitik usul asosida O'zbekistonda so'nggi yillarda sodir etilgan kiberjinoyatlar tarkibi, ularning asosiy yo'nalishlari hamda amaliyotda uchrayotgan muammolar o'rganildi. Xususan, bank kartalari bilan bog'liq firibgarlik, fishing hujumlari, zararli dasturlar, noqonuniy kirish, shaxsga doir ma'lumotlarning tarqalishi hamda elektron to'lov tizimlariga qarshi qaratilgan huquqbuzarliklarning rivojlanish tendensiyalari tahlil qilindi. Shuningdek, maqolada tizimli yondashuv usulidan foydalanildi. Mazkur yondashuv asosida kiberjinoyatchilik faqat jinoyat-huquqiy hodisa sifatida emas, balki axborot xavfsizligi, davlat xavfsizligi, raqamli iqtisodiyot, moliyaviy barqarorlik va xalqaro hamkorlik bilan uzviy bog'liq kompleks ijtimoiy-huquqiy muammo sifatida o'rganildi. Shu bilan birga, zamonaviy tahdidlar – sun'iy intellekt yordamida sodir etilayotgan firibgarliklar, deepfake texnologiyalari, ransomware, kriptoaktivlar orqali noqonuniy operatsiyalar va bulutli infratuzilmalarga qaratilgan hujumlarning huquqiy jihatlari alohida baholandi. Mazkur metodlarning o'zaro uyg'unligi O'zbekistonda kiberjinoyatchilikka qarshi kurashishning amaldagi holatini har tomonlama baholash, mavjud huquqiy bo'shliqlarni aniqlash hamda ularni bartaraf etishga qaratilgan ilmiy-amaliy takliflarni ishlab chiqish imkonini berdi.

III. Natijalar

Tadqiqot natijalari O'zbekiston Respublikasida kiberjinoyatchilikka qarshi kurashning huquqiy bazasi izchil shakllanib borayotganini ko'rsatdi. Xususan, "Kiberxavfsizlik to'g'risida"gi Qonunning qabul qilinishi davlat organlari, muhim axborot infratuzilmasi operatorlari hamda boshqa tashkilotlarning kiberxavfsizlikni ta'minlash sohasidagi huquq va majburiyatlarini belgilab berdi. Mazkur qonun kiberhodisalarning oldini olish, ularni aniqlash va oqibatlarini bartaraf etish bo'yicha yagona davlat siyosatini shakllantirishda muhim huquqiy asos bo'lib xizmat qilmoqda. Shu bilan birga, Jinoyat kodeksida axborot texnologiyalari sohasidagi huquqbuzarliklar uchun javobgarlik nazarda tutilgan bo'lib, ular kompyuter axborotidan noqonuniy foydalanish, axborot tizimlariga ruxsatsiz kirish, elektron ma'lumotlarni o'zgartirish yoki yo'q qilish, zararli dasturlar yaratish va tarqatish kabi qilmishlarni qamrab oladi. Biroq amaliyotda sodir etilayotgan ko'plab kiberjinoyatlar, xususan bank kartalari orqali firibgarlik, ijtimoiy tarmoqlar orqali aldov, fishing va soxta internet resurslari orqali mablag'larni o'zlashtirish holatlari ko'pincha umumiy firibgarlik tarkibi bo'yicha kvalifikatsiya qilinmoqda. Bu esa kiberjinoyatlarning o'ziga xos xususiyatlarini to'liq aks ettirmaydi. Tahlillar shuni ko'rsatdiki, O'zbekistonda eng ko'p uchrayotgan kiberjinoyatlar qatoriga bank kartalari bilan bog'liq firibgarlik, fishing hujumlari, mobil ilovalar orqali sodir etilayotgan aldovlar, ijtimoiy tarmoqlarda soxta akkauntlar yaratish, zararli dasturlar yordamida ma'lumotlarni qo'lga kiritish hamda noqonuniy elektron to'lov operatsiyalari kiradi. So'nggi yillarda fuqarolar tomonidan masofaviy bank xizmatlari va elektron to'lov tizimlaridan foydalanishning ortishi mazkur turdagi jinoyatlarning ko'payishiga ham sabab bo'ldi. Natijalar shuningdek, kiberjinoyatlarni tergov qilishda elektron dalillar bilan ishlash amaliyotida ayrim muammolar mavjudligini ko'rsatdi. Elektron axborotning tez o'zgarishi yoki yo'qolishi, serverlarning xorijiy davlatlarda joylashganligi hamda jinoyatchilarning anonim texnologiyalardan foydalanishi tergov organlari faoliyatini murakkablashtirmoqda. Elektron dalillarni yig'ish, saqlash va baholash bo'yicha

yagona protsessual standartlarning yetarli darajada shakllanmagani ayrim hollarda isbotlash jarayoniga salbiy ta'sir ko'rsatmoqda.

Qiyosiy-huquqiy tahlil natijalari rivojlangan davlatlarda kiberjinoyatchilikka qarshi kurashish faqat jinoiy javobgarlik bilan cheklanmasligini ko'rsatdi. Estoniya va Singapur tajribasida muhim axborot infratuzilmasini himoya qilish, majburiy xavfsizlik auditi, real vaqt rejimida kiberhodisalarni monitoring qilish va davlat-xususiy sektor hamkorligiga katta e'tibor qaratiladi. AQSH va Yevropa Ittifoqida esa elektron dalillar almashinuvi, tezkor xalqaro hamkorlik va maxsus kibertergov bo'linmalarining faoliyati samarali yo'lga qo'yilgan.

Tahlillar asosida O'zbekiston qonunchiligida takomillashtirilishi lozim bo'lgan bir qator masalalar aniqlandi. Jumladan, "kiberjinoyat" tushunchasining yagona huquqiy ta'rifini belgilash, sun'iy intellekt va deepfake texnologiyalari yordamida sodir etiladigan jinoyatlar uchun alohida huquqiy normalarni ishlab chiqish, elektron dalillar bilan ishlashning protsessual tartibini yanada aniqroq belgilash hamda transchegaraviy kiberjinoyatlarni tergov qilish bo'yicha xalqaro hamkorlik mexanizmlarini rivojlantirish zarur.

Natijalar shuni tasdiqlaydiki, kiberjinoyatchilikka qarshi samarali kurashish faqat qonunchilikni takomillashtirish bilangina emas, balki fuqarolarning raqamli savodxonligini oshirish, davlat organlari va xususiy sektor o'rtasidagi hamkorlikni kuchaytirish, zamonaviy texnologiyalarni joriy etish hamda kiberxavfsizlik sohasida malakali mutaxassislar tayyorlash bilan ham chambarchas bog'liq.

IV. Muhokama

Tadqiqot natijalari O'zbekiston Respublikasida kiberjinoyatchilikka qarshi kurashish bo'yicha so'nggi yillarda muhim huquqiy va institutsional islohotlar amalga oshirilganini ko'rsatdi. Xususan, **"Kiberxavfsizlik to'g'risida"gi Qonun**ning qabul qilinishi, axborot tizimlarini himoya qilish bo'yicha davlat siyosatining shakllantirilishi hamda vakolatli organlarning faoliyati ushbu yo'nalishdagi huquqiy asoslarni sezilarli darajada mustahkamladi. Biroq raqamli texnologiyalarning jadal rivojlanishi natijasida kiberjinoyatlarning shakllari va sodir etilish usullari ham murakkablashib bormoqda. Bu esa qonunchilikni muntazam ravishda zamonaviy tahdidlarga moslashtirish zarurligini ko'rsatadi.

Tahlillar shuni ko'rsatdiki, amaldagi qonunchilikda axborot tizimlariga noqonuniy kirish, zararli dasturlar yaratish, elektron ma'lumotlarni o'zgartirish va boshqa qator huquqbuzarliklar uchun javobgarlik belgilangan bo'lsa-da, sun'iy intellekt texnologiyalaridan foydalanilgan firibgarliklar, deepfake mahsulotlari, kriptoaktivlar orqali sodir etilayotgan jinoyatlar hamda bulutli texnologiyalar bilan bog'liq huquqbuzarliklarni tartibga soluvchi maxsus normalar yetarli darajada rivojlanmagan. Natijada ayrim yangi turdagi kiberjinoyatlar umumiy jinoyat tarkiblari doirasida kvalifikatsiya qilinmoqda, bu esa huquqni qo'llash amaliyotida turlicha yondashuvlarning yuzaga kelishiga sabab bo'lmoqda.

Qiyosiy tahlil natijalari shuni ko'rsatadiki, Estoniya, Singapur, AQSH va Yevropa Ittifoqi davlatlarida kiberjinoyatchilikka qarshi kurashish faqat jinoiy javobgarlikni kuchaytirish bilan cheklanmaydi. Ushbu davlatlarda muhim axborot infratuzilmasini himoya qilish, kiberhodisalarni real vaqt rejimida monitoring qilish, elektron dalillar bilan ishlashning aniq protsessual mexanizmlarini joriy etish hamda davlat va xususiy sektor o'rtasidagi hamkorlikni rivojlantirish ustuvor yo'nalish sifatida e'tirof etilgan. Mazkur tajribalar O'zbekiston uchun ham muhim amaliy ahamiyat kasb etadi. Kiberjinoyatlarning aksariyati transchegaraviy xususiyatga ega bo'lganligi sababli dalillar turli davlatlarda joylashgan serverlarda saqlanishi mumkin. Bu esa xalqaro huquqiy yordam mexanizmlaridan samarali foydalanish,

elektron dalillarni yig'ish va saqlash bo'yicha yagona protsessual standartlarni ishlab chiqishni talab etadi. Shu nuqtai nazardan Budapesht konvensiyasida nazarda tutilgan hamkorlik mexanizmlarini milliy amaliyotga bosqichma-bosqich implementatsiya qilish maqsadga muvofiq hisoblanadi.

Bundan tashqari, kiberjinoyatchilikka qarshi kurashish faqat huquqni muhofaza qiluvchi organlarning vazifasi emas. Mazkur jarayonda davlat organlari, bank-moliya sektori, telekommunikatsiya operatorlari, axborot texnologiyalari kompaniyalari hamda fuqarolarning o'zaro hamkorligi muhim o'rin tutadi. Ayniqsa, aholining raqamli savodxonligini oshirish, fishing va boshqa internet firibgarligi usullari haqida muntazam xabardor qilish profilaktik choralarning eng samarali yo'nalishlaridan biri hisoblanadi.

Umuman olganda, tadqiqot natijalari O'zbekiston Respublikasida kiberjinoyatchilikka qarshi kurashning huquqiy mexanizmlari shakllanganini ko'rsatsa-da, zamonaviy texnologiyalar rivojlanishi bilan bog'liq yangi tahdidlarga mos ravishda qonunchilikni takomillashtirish, xalqaro hamkorlikni kengaytirish hamda huquqni qo'llash amaliyotini modernizatsiya qilish zarurligini tasdiqlaydi.

V.Xulosa

Xulosa qilib aytganda, kiberjinoyatchilik zamonaviy axborot jamiyatining eng dolzarb huquqiy va texnologik muammolaridan biri hisoblanadi. Raqamli iqtisodiyotning rivojlanishi, elektron davlat xizmatlari, internet-bank xizmatlari va elektron tijoratning kengayishi bilan bir qatorda kiberjinoyatlar soni ham ortib bormoqda. Shu sababli kiberjinoyatchilikka qarshi kurashish davlat xavfsizligi, iqtisodiy barqarorlik va axborot makonini himoya qilishning muhim yo'nalishiga aylanmoqda.

Tadqiqot natijalari O'zbekiston Respublikasida ushbu sohada mustahkam huquqiy asos yaratilganligini ko'rsatdi. Xususan, "Kiberxavfsizlik to'g'risida"gi Qonun, Jinoyat kodeksi hamda axborot xavfsizligiga oid boshqa normativ-huquqiy hujjatlar kiberjinoyatlarning oldini olish va ularga qarshi kurashishning asosiy mexanizmlarini belgilab bergan. Biroq sun'iy intellekt, deepfake texnologiyalari, kriptoaktivlar, bulutli infratuzilmalar va transchegaraviy kiberhujumlar bilan bog'liq yangi tahdidlar milliy qonunchilikni izchil ravishda takomillashtirib borishni talab etmoqda.

Muallifning fikricha, O'zbekistonda kiberjinoyatchilikka qarshi kurash samaradorligini oshirish uchun birinchi navbatda "kiberjinoyat" tushunchasining yagona huquqiy ta'rifini qonunchilikda mustahkamlash, elektron dalillar bilan ishlashning yagona protsessual tartibini ishlab chiqish, sun'iy intellekt yordamida sodir etiladigan jinoyatlar uchun alohida javobgarlik mexanizmlarini yaratish hamda Budapesht konvensiyasi standartlariga mos xalqaro hamkorlikni rivojlantirish maqsadga muvofiqdir.

Bundan tashqari, kiberjinoyatchilikning oldini olishda huquqiy choralar bilan bir qatorda profilaktik tadbirlarni kuchaytirish, davlat organlari va xususiy sektor o'rtasida axborot almashish tizimini rivojlantirish, huquqni muhofaza qiluvchi organlarning texnik salohiyatini oshirish hamda aholining raqamli savodxonligini yuksaltirish zarur. Aynan kompleks yondashuvgina O'zbekistonda xavfsiz va barqaror raqamli muhitni shakllantirish hamda kiberjinoyatchilikka qarshi kurash samaradorligini oshirishga xizmat qiladi.

Yuqoridagi tahlillar asosida quyidagi takliflar yuzaga keldi:

- Jinoyat kodeksida "kiberjinoyat" tushunchasiga yagona huquqiy ta'rif berish;
- sun'iy intellekt, deepfake va kriptoaktivlar bilan bog'liq jinoyatlar uchun maxsus normalarni ishlab chiqish;

- elektron dalillarni yig'ish, saqlash va baholashning yagona protsessual standartlarini joriy etish;
- Budapesht konvensiyasi standartlari asosida xalqaro hamkorlikni kengaytirish;
- davlat organlari, banklar va IT kompaniyalari o'rtasida kiberhodisalar to'g'risida tezkor axborot almashish tizimini rivojlantirish;
- aholining raqamli savodxonligini oshirishga qaratilgan doimiy profilaktik dasturlarni amalga oshirish.

FOYDALANILGAN ADABIYOTLAR:

1. O'zbekiston Respublikasi Konstitutsiyasi. – T.: O'zbekiston, 2023.
2. O'zbekiston Respublikasining Jinoyat kodeksi. – T.: Adolat, 1994 (2025-yil holatiga ko'ra o'zgartirish va qo'shimchalar bilan).
3. O'zbekiston Respublikasining **"Kiberxavfsizlik to'g'risida"gi Qonuni**. O'RQ–764-son, 15-aprel 2022-yil.
4. O'zbekiston Respublikasining **"Shaxsga doir ma'lumotlar to'g'risida"gi Qonuni**. O'RQ–547-son, 2-iyul 2019-yil.
5. O'zbekiston Respublikasining **"Axborotlashtirish to'g'risida"gi Qonuni**. O'RQ–560-II, 11-dekabr 2003-yil.
6. O'zbekiston Respublikasining **"Axborot erkinligi prinsiplari va kafolatlari to'g'risida"gi Qonuni**. O'RQ–439-II, 12-dekabr 2002-yil.
7. O'zbekiston Respublikasi Prezidentining **"Raqamli O'zbekiston – 2030" strategiyasini amalga oshirish chora-tadbirlari to'g'risida"**gi Farmoni.
8. Council of Europe. **Convention on Cybercrime (Budapest Convention)**. Budapest, 23 November 2001.
9. United Nations Office on Drugs and Crime (UNODC). Comprehensive Study on Cybercrime. New York, 2013.
10. United Nations Office on Drugs and Crime (UNODC). Global Programme on Cybercrime. Vienna, 2024.
11. International Telecommunication Union (ITU). Global Cybersecurity Index 2024. Geneva, 2024.
12. European Union Agency for Cybersecurity (ENISA). ENISA Threat Landscape 2024. Brussels, 2024.
13. National Institute of Standards and Technology (NIST). Cybersecurity Framework (CSF 2.0). Gaithersburg, 2024.
14. Europol. Internet Organised Crime Threat Assessment (IOCTA) 2024. Hague, 2024.
15. INTERPOL. Global Cybercrime Strategy 2022–2027. Lyon, 2022.
16. OECD. Digital Security Risk Management for Economic and Social Prosperity. Paris, 2023.
17. ISO/IEC 27001:2022. Information Security, Cybersecurity and Privacy Protection — Information Security Management Systems — Requirements. Geneva, 2022.
18. Jalolov Sh.R. **Kiberjinoyatlarga qarshi kurashishda inson huquqlarini ta'minlash** // IQRO jurnali. 2025. №18(2). 472–477-bet.

19. Xolmurodov Sh. **Kiberjinoyatlar va ularni oldini olish muammolari**. – Toshkent: Yuridik adabiyotlar, 2021.
20. To'xtayev M. **Axborot xavfsizligi va jinoyat huquqi**. – Toshkent, 2022.
21. O'zbekiston Respublikasi Ichki ishlar vazirligi. **Kiberjinoyatchilikka qarshi kurashish bo'yicha statistik ma'lumotlar**. 2024.
22. O'zbekiston Respublikasi Raqamli texnologiyalar vazirligi. **Kiberxavfsizlik sohasidagi yillik hisobot**. 2024.
23. CERT-UZ. O'zbekistonda kiberxavfsizlik hodisalari bo'yicha yillik tahliliy hisobot. 2024.
24. Lex.uz – O'zbekiston Respublikasi milliy qonunchilik bazasi.
25. Cybersecurity Ventures. Official Cybercrime Report 2024. Cybersecurity Ventures, 2024.