INNOVATIONS IN TECHNOLOGY AND SCIENCE EDUCATION
ISSN 2181-371X
https://sr-journals.org/index.php/ITSE

O‘ZBEKISTONDA KIBERJINOYATLARGA QARSHI KURASH JARAYONIDA SHAXSIY MA'LUMOTLARNI HIMOYA QILISHNING HUQUQIY MUAMMOLARI VA ULARNI BARTARAF ETISH YO‘LLARI

Muallif: ***Parmonqulova Umida Toxir Qizi.***
Toshkent davlat agrar universiteti Agroiqtisodiyot,
logistika va xizmatlar fakulteti 2-bosqich talabasi.
Ilmiy rahbar: ***Atxamjonov Abbosxon Atxamjon o‘g‘li***
TDAU stajyor o‘qituvchisi.

Annotatsiya: Mazkur ilmiy maqolada O‘zbekiston Respublikasida kiberjinoyatlarga qarshi kurash jarayonida shaxsiy ma’lumotlarni himoya qilish bilan bog‘liq huquqiy muammolar tahlil qilinadi. Raqamli texnologiyalar jadal rivojlanayotgan hozirgi sharoitda shaxsiy ma’lumotlarning noqonuniy yig‘ilishi, qayta ishlanishi va tarqatilishi kiberjinoyatlarning asosiy obyektlaridan biriga aylanmoqda. Maqolada shaxsiy ma’lumotlarni himoya qilishga oid milliy qonunchilik normalari, ularning amaliyotda qo‘llanilishi hamda mavjud huquqiy bo‘shliqlar tahlil qilinadi. Shuningdek, xalqaro tajriba asosida shaxsiy ma’lumotlarni himoya qilish tizimini takomillashtirish bo‘yicha ilmiy-amaliy takliflar ishlab chiqiladi. Tadqiqot natijalari kiberxavfsizlikni ta’minlash va fuqarolarning shaxsiy hayot daxlsizligini himoya qilishga xizmat qiladi.

Kalit so‘zlar: kiberjinoyat, shaxsiy ma’lumotlar, axborot xavfsizligi, huquqiy himoya, raqamli texnologiyalar, kiberxavfsizlik.

Аннотация: В данной научной статье анализируются правовые проблемы защиты персональных данных в процессе противодействия киберпреступности в Республике Узбекистан. В условиях стремительного развития цифровых технологий незаконный сбор, обработка и распространение персональных данных становятся одними из основных объектов киберпреступлений. В статье рассматриваются нормы национального законодательства, регулирующие защиту персональных данных, практика их применения, а также существующие правовые пробелы. На основе международного опыта разработаны научно-практические предложения по совершенствованию системы защиты персональных данных. Результаты исследования направлены на обеспечение кибербезопасности и защиту неприкосновенности частной жизни граждан.

Ключевые слова: киберпреступность, персональные данные, информационная безопасность, правовая защита, цифровые технологии, кибербезопасность.

Annotation: This scientific article analyzes the legal problems of personal data protection in the process of combating cybercrime in the Republic of Uzbekistan. In the context of rapid development of digital technologies, the illegal collection, processing, and dissemination of personal data have become one of the main objects of cybercrime. The article examines national legislation regulating personal data protection, its application in practice, and existing legal gaps. Based on international experience, scientific and practical recommendations for improving the personal data protection system are proposed. The research results contribute to ensuring cybersecurity and protecting citizens’ right to privacy.

Keywords: cybercrime, personal data, information security, legal protection, digital technologies, cybersecurity.

Hozirgi globallashuv va raqamlashtirish sharoitida kiberjinoyatlar jamiyat xavfsizligiga jiddiy tahdid soluvchi omillardan biriga aylandi. So‘nggi yillarda axborot texnologiyalari va internet tarmog‘ining jadal rivojlanishi jamiyat hayotini tubdan o‘zgartirdi. Bugungi kunda davlat boshqaruvi, bank tizimi, ta’lim, sog‘liqni saqlash, tadbirkorlik va hatto kundalik ijtimoiy munosabatlar ham raqamli muhit bilan chambarchas bog‘liq. Ushbu jarayon, bir tomondan, qulaylik va samaradorlikni oshirgan bo‘lsa, ikkinchi tomondan, yangi xavf-xatarlar — xususan, kiberjinoyatlarning ko‘payishiga sabab bo‘ldi. Kiberjinoyat deganda axborot-kommunikatsiya texnologiyalari va internet tarmog‘idan foydalanib sodir etiladigan, jamiyat va shaxs manfaatlariga zarar yetkazuvchi jinoyatlar tushuniladi. Kompyuter jinoyat paytida maqsadli yo‘naltirilgan qurol vazifasini bajarib beradi. Kiberjinoyatlar kimningdir xavfsizligi va moliyaviy saviyasiga zarar yetkazish maqsadida sodir etiladi. Bunday jinoyatlar asosan axborotni noqonuniy egallash, o‘zgartirish, yo‘q qilish yoki undan g‘arazli maqsadlarda foydalanish bilan bog‘liq bo‘ladi. Amaliyot shuni ko‘rsatadiki, kiberjinoyatlarning aksariyati shaxsiy ma’lumotlarning noqonuniy yig‘ilishi, qayta ishlanishi yoki tarqatilishi bilan bog‘liq. Fuqarolarning pasport ma’lumotlari, bank rekvizitlari, biometrik axborotlari yoki shaxsiy yozishmalarining uchinchi shaxslar qo‘liga tushishi nafaqat moddiy zarar, balki jiddiy huquqiy va ma’naviy oqibatlarni ham keltirib chiqaradi. Shaxsiy ma’lumotlar-muayyan jismoniy shaxsga taalluqli bo‘lgan, uni bevosita yoki bilvosita aniqlash imkonini beruvchi har qanday axborotlar majmuasidir. Bunday ma’lumotlarga shaxsning ism-familiyasi, tug‘ilgan sanasi, yashash manzili, telefon raqami, elektron pochta manzili, moliyaviy va biometrik ma’lumotlari kiradi. Huquqiy nuqtayi nazardan, shaxsiy ma’lumotlarni himoya qilish inson huquqlarining ajralmas qismi sanaladi. U shaxsiy hayot daxlsizligi, sha’n va qadr-qimmatni himoya qilish, shuningdek, shaxs erkinligini ta’minlash bilan uzviy bog‘liqdir. Kiberjinoyatlar sharoitida esa shaxsiy ma’lumotlarning noqonuniy muomalasi jamiyatda ishonchsizlik muhitini vujudga keltirishi mumkin. O‘zbekiston Respublikasining “Shaxsiy ma’lumotlar to‘g‘risida”gi Qonuniga muvofiq, shaxsiy ma’lumotlarga fuqaroning familiyasi, ismi, yashash manzili, biometrik va boshqa shaxsiy hayotiga daxldor ma’lumotlar kiradi. Ushbu ma’lumotlarning noqonuniy yig‘ilishi va tarqatilishi fuqarolarning shaxsiy hayoti daxlsizligi prinsipiga zid hisoblanadi.

Maxfiy ma’lumotlar qonuniy tarzda himoyalangan holatda yuz beruvchi kiberjinoyatlar bilan bog‘liq ko‘pgina jinoyatlar mavjud. Xalqaro miqyosda asosan, nodavlat subyektlar kiberjinoyatlar, jumladan, josuslik, moliyaviy o‘g‘irlik va boshqa transchegaraviy jinoyatlar bilan shug‘ullanadi. Xalqaro chegaralarni kesib o‘tuvchi va kamida bitta milliy davlatning xatti-harakatlarini o‘z ichiga olgan kiberjinoyatlar ba’zan kiberurush deb ataladi. Uorren Baffet kiberjinoyatni „insoniyatning birinchi raqamli muammosi“deb ta’riflaydi va „insoniyat uchun real xavf tug‘diradi“, deya qo‘shimcha qilib o‘tadi. 2014-yilda chop etilgan hisobotda jahon iqtisodiyotiga yetkazilgan yillik zarar 445 milliard dollarni tashkil qilgan. Cybersecurity Ventures tomonidan 2016-yilgi hisobotda kiberjinoyatlar natijasida yetkazilgan global zararlar 2021-yilga kelib yiliga 6 trillion dollargacha, 2025-yilga kelib esa 10,5 trillion dollargacha ko‘tarilishi bashorat qilingan edi.2012-yilda AQShda onlayn kredit va debet kartalaridagi firibgarlik oqibatida taxminan 1,5 milliard dollar yo‘qotilgan. 2018-yilda Strategik va xalqaro tadqiqotlar markazi (CSIS) tomonidan McAfee bilan hamkorlikda o‘tkazilgan tadqiqot shuni ko‘rsatadiki, har yili global YaIMning qariyb bir foizi, ya’ni 600 milliard dollarga yaqini kiberjinoyatlar tufayli yo‘qoladi. Jahon Iqtisodiy Forumi 2020 Global Risk hisobotida uyushgan kiberjinoyatlar idoralari jinoiy faoliyatni onlayn qilish uchun kuchlarni birlashtirayotganini tasdiqladi, shu bilan birga ularning aniqlash va jinoiy javobgarlikka tortilish ehtimoli AQShda 1 foizdan kamroqni tashkil qiladi.

An’anaviy jinoyatchilikning kamayishi bilan global hamjamiyatlar kiberjinoyatlarning muntazam o‘sishiga guvoh bo‘lishda davom etmoqda. Xususan, kompyuterga yo‘naltirilgan jinoyatlar kiberjinoyatlarni tavsiflashda alohida ahamiyatga egadir. Bu jinoyatlar tanlangan jinoyatchilar guruhi tomonidan sodir etiladi. Kompyuterni qurol sifatida ishlatadigan jinoyatlardan farqli o‘laroq, bu jinoyatlar aybdorlarning texnik bilimlarini talab qiladi. Shunday qilib, texnologiya rivojlanishi bilan

jinoyatning tabiati ham o‘zgaradi. Bu jinoyatlar nisbatan yangi bo‘lib, kompyuterlar mavjud bo‘lgan vaqtdan beri mavjud bo‘lib, bu jamiyat va umuman dunyo ushbu jinoyatlarga qarshi kurashga qanchalik tayyor emasligini tushuntiradi. Internetda har kuni sodir bo‘ladigan ko‘plab jinoyatlar mavjud. Bu kamdan-kam hollarda yolg‘izlar tomonidan amalga oshiriladi, buning o‘rniga u katta sindikat guruhlarini o‘z ichiga oladi. Asosan kompyuter tarmoqlariga qaratilgan jinoyatlarga quyidagilar kiradi: Kompyuter viruslari; xizmatni rad etish hujumlari; zararli dastur (zararli kod); axborot urushi; firibgarlik; spam; noqonuniy yoki haqoratli kontentni, jumladan, ta’qib va tahdidlarni targ‘ib qilish; tijoriy maqsadlarda (spam) ommaviy elektron pochta xabarlarini so‘ralmagan holda yuborish va boshqalar.

Qayd etish joizki, ijtimoiy tarmoqlar bugungi hayotimizning ajralmas qismiga aylanib ulgurgan. Ular orqali bemalol kerakli ma’lumotlarga tezkorlik bilan ega bo‘lishimiz, yangiliklardan xabar topishimiz, bilim va tajriba almashishimiz mumkin. Biroq bu qulayliklar ortida turli xavf-xatarlar, ayniqsa, kiberfiribgarlik holatlari ham yo‘q emas. So‘nggi yillarda bunday firibgarlarning ijtimoiy tarmoqlarda soxta hisoblar ochib, foydalanuvchilarning ishonchiga kirish va pullarini o‘marish holatlari tobora avj olmoqda. Ular shaxsiy ma’lumotlarni o‘g‘irlab sotish, bank kartasi ma’lumotlarini aldov yo‘li bilan qo‘lga kiritish, yolg‘on sovrinlar yutganlik haqida xabar yuborib, odamlarni chuv tushirishmoqda. Yana bir xavfli holat esa fayl ko‘rinishida tarqatilayotgan zararli dasturlardir. Masalan, Telegram orqali “1 soatda 2 million so‘m toping”, “Mahallada pul tarqatilyapti”, “Rasmlaringiz internetga tarqalib ketdi” kabi sarlavhalar ostida xabarlar yuborilyapti. Ba’zi foydalanuvchilar ushbu faylni ochishi bilan firibgarlar hujumiga uchrab, oradan ko‘p o‘tmay pul mablag‘lari yechib olinyapti. Bunday holatlar albatta kiber jinoyat hisoblanadi va ularga qarshi qonuniy choralar ko‘riladi. — Oldinlari yurtimizda kiberjinoyatlar unchalik keng tarqalmagan, jinoyatchilar nigohi faqat yirik tashkilotlariga qaratilgan bo‘lsa, hozir oddiy fuqarolar ham nishonga olinmoqda, — deydi Toshkent shaxar Ichki ishlar vazirligi akademiyasi doktoranti, katta leytenant Manzura Axmedova. — Ayni paytda kiberjinoyatlar bilan bog‘liq arizalar soni sezilarli darajada oshgan. Ichki ishlar vazirligi va kiberxavfsizlik markazlarining ma’lumotlariga ko‘ra, kuniga o‘rtacha 80 — 100 ta ariza kelib tushmoqda. Bu son yildan-yilga ortib borayotgani ham achinarli hol. Arizalarning asosiy qismi bank kartalari orqali pul o‘g‘irlanishi, soxta sahifalar orqali aldash, ijtimoiy tarmoqlarda shaxsiy ma’lumotlarni o‘g‘irlatish va shantaj bilan aloqador. Shu bois, fuqarolardan hushyor bo‘lish, aldanib qolmaslik, buning uchun esa har qanday holatda ham e’tiborli bo‘lishni so‘ragan bo‘lardik.

O‘zbekistonda kiberxavfsizlikni ta’minlash masalasi tobora dolzarb ahamiyat kasb etib, bu borada qator muammolar mavjudligi kuzatilmoqda. Ushbu muammolar, avvalo, aholining kiberxavfsizlik borasidagi xabardorlik darajasining pastligi, texnologik imkoniyatlarning yetarli emasligi, huquqiy bazaning doimiy takomillashtirilishga muhtojligi hamda xalqaro hamkorlikning yetarli darajada rivojlanmaganligi bilan bog‘liq. Eng muhim muammolardan biri — aholi va tashkilotlar orasida kiberxavfsizlik madaniyatining yetarli darajada shakllanmaganligidir. Ko‘plab foydalanuvchilar shaxsiy ma’lumotlarni himoya qilish qoidalariga rioya qilmasligi, fishing, zararli dasturlar va ijtimoiy muhandislik usullari orqali sodir etiladigan jinoyatlarga nisbatan yetarli ehtiyot choralarini ko‘rmasligi kiberjinoyatchilar uchun qulay sharoit yaratmoqda. Shuningdek, texnologik nomutanosiblik muammosi ham dolzarb hisoblanadi. Kiberjinoyatchilar zamonaviy va murakkab texnologiyalardan faol foydalanayotgan bir paytda, ayrim davlat va xususiy sektor axborot tizimlarida himoya mexanizmlarining eskirganligi yoki yetarli darajada rivojlanmaganligi kuzatiladi. Bu holat muhim axborot resurslarining zaiflashuviga olib kelishi mumkin. Huquqiy bazaning samaradorligi masalasi ham alohida e’tiborga loyiq. Kiberjinoyatlarni aniqlash, tergov qilish va ularga nisbatan javobgarlikni qo‘llash jarayonlarida qonunchilik normalarini zamon talablariga mos ravishda takomillashtirib borish zarurati mavjud. Kiberjinoyatlarning murakkab va tez o‘zgaruvchan xususiyati huquqni muhofaza qiluvchi organlardan yuqori darajadagi moslashuvchanlikni talab etadi. Bundan tashqari, davlat va xususiy sektordagi muhim axborot infratuzilmalarining yetarli darajada himoyalanmaganligi ham jiddiy xavf tug‘diradi. Energetika, moliya, transport va davlat boshqaruvi tizimlarida axborot xavfsizligini ta’minlash milliy xavfsizlikning ajralmas qismi hisoblanadi.

Kiberjinoyatlarning transmilliy xususiyatga ega ekanligi esa xalqaro hamkorlikning muhimligini yanada oshiradi. Axborot almashish, tajriba va ilg‘or amaliyotlarni o‘rganish bo‘yicha xalqaro darajadagi hamkorlik yetarli bo‘lmasa, kiberjinoyatlarga qarshi samarali kurashish qiyinlashadi. Mazkur muammolarni bartaraf etish uchun, avvalo, ta’lim va xabardorlikni oshirishga qaratilgan tizimli chora-tadbirlarni amalga oshirish lozim. Aholi, davlat xizmatchilari va xususiy sektor vakillari uchun muntazam treninglar tashkil etish, shaxsiy ma’lumotlarni himoya qilish bo‘yicha amaliy ko‘nikmalarni shakllantirish muhim ahamiyatga ega. Shu bilan birga, huquqiy-normativ bazani mustahkamlash, kiberjinoyatlarga qarshi kurashish bo‘yicha mavjud qonunlarni doimiy ravishda takomillashtirib borish zarur. Texnologik infratuzilmani rivojlantirish, zamonaviy monitoring va hodisalarni boshqarish tizimlarini joriy etish ham kiberxavfsizlik darajasini oshirishga xizmat qiladi.

Hozirgi vaqtga kelib mamlakatimizda kiberjinoyatlarga qarshi kurashishda oddiy xususiyatga ega ammo dolzarb hisoblangan bir qancha muammolar ham mavjud, xususan, internet-do‘konlar, mobil ilovalar va ijtimoiy tarmoqlar orqali shaxsiy ma’lumotlarning ruxsatsiz yig‘ilishi va uchinchi shaxslarga uzatilishi holatlari amaliyotda tez-tez uchramoqda. Bunday vaziyatlarda fuqarolarning buzilgan huquqlarini tiklash mexanizmlari murakkab va uzoq davom etuvchi jarayon bo‘lib qolmoqda. Ikkinchidan, kiberjinoyatlar uchun belgilangan javobgarlik choralari har doim ham yetarli darajada profilaktik ahamiyat kasb etmaydi. Ayrim hollarda sanksiyalarning yengilligi yoki huquqni qo‘llash amaliyotidagi sustlik jinoyatlarning qayta sodir etilishiga olib kelmoqda. Bu esa shaxsiy ma’lumotlarni himoya qilish tizimini yanada kuchaytirish zaruratini ko‘rsatadi. Shuningdek, shaxsiy ma’lumotlarni himoya qilish sohasida aholining huquqiy savodxonligi yetarli darajada shakllanmaganligi ham jiddiy muammo hisoblanadi. Ko‘plab fuqarolar o‘z shaxsiy ma’lumotlarini internet resurslarida joylashtirishda ehtiyotsizlikka yo‘l qo‘ymoqda, bu esa kiberjinoyatchilar uchun qulay sharoit yaratmoqda. Amaliyotda shaxsiy ma’lumotlarning noqonuniy tarqatilishi natijasida yetkazilgan zarar ko‘pincha huquqiy bahosiz qolmoqda.

Xalqaro amaliyot shuni ko‘rsatadiki, kiberjinoyatlarga qarshi kurashda shaxsiy ma’lumotlarni himoya qilish alohida ustuvor ahamiyat kasb etadi. Rivojlangan davlatlarda ushbu sohada mustaqil nazorat organlari faoliyat yuritadi hamda ma’lumotlarni qayta ishlash ustidan qat’iy monitoring o‘rnatilgan. Xalqaro tajriba shaxsiy ma’lumotlarni himoya qilishning aniq va tushunarli standartlari mavjud bo‘lgan taqdirdagina kiberxavfsizlik siyosati samarali bo‘lishini tasdiqlaydi. Shuningdek, xalqaro hamkorlikni kengaytirish, davlat-xususiy sektor o‘rtasidagi hamkorlikni mustahkamlash hamda muhim infratuzilma xodimlarini kiberxavfsizlik bo‘yicha attestatsiya va sertifikatsiyadan o‘tkazish ushbu sohadagi barqarorlikni ta’minlashga yordam beradi. O‘zbekistonda “Kiberxavfsizlik to‘g‘risida”gi Qonun (O‘RQ-764) qabul qilinishi bu yo‘nalishda muhim qadam bo‘lsa-da, kiberjinoyatchilikning doimiy rivojlanib borishini inobatga olgan holda, mazkur sohada chora-tadbirlarni uzluksiz ravishda takomillashtirib borish zarur. Albatta, har qanday ish qonun bilan qat’iy belgilab qo‘yilsa, natijadorlik yanada oshadi. Shu ma’noda, yaqinda davlatimiz rahbari tomonidan imzolangan “Axborot texnologiyalari yordamida sodir etiladigan jinoyatlarga qarshi kurashish faoliyatini yanada kuchaytirishga qaratilgan chora-tadbirlar to‘g‘risida”gi qarori ham muhim ahamiyatga ega. Mazkur qonun axborot texnologiyalari orqali sodir etilayotgan jinoyatlarga qarshi kurashish faoliyatini kuchaytirishga qaratilgan bo‘lib, bunda banklar va to‘lov tashkilotlari kiberxavfsizlik talablariga rioya qilmaslik natijasida yuzaga kelgan zararlar uchun moliyaviy javobgarlikka tortilishi belgilangan. Shuningdek, soxta qo‘ng‘iroqlarga qarshi tizim ishlab chiqilmoqda, bu orqali firibgarlarning telefon orqali aldovlariga chek qo‘yish ko‘zda tutilgan.

O‘zbekistonda shaxsiy ma’lumotlarni himoya qilishning huquqiy asoslari bir qator normativ-huquqiy hujjatlar bilan mustahkamlangan. Jumladan, O‘zbekiston Respublikasi Konstitutsiyasida shaxsning sha’ni va qadr-qimmati, shaxsiy hayoti daxlsizligi kafolatlangan. Shuningdek, Jinoyat kodeksida axborot xavfsizligiga qarshi jinoyatlar uchun javobgarlik belgilangan bo‘lib, bu normalar kiberjinoyatlarga qarshi kurashda muhim ahamiyat kasb etadi. Shu bilan birga, kiberjinoyatlar transmilliy xususiyatga ega bo‘lgani sababli, faqat milliy qonunchilik bilan cheklanib qolish yetarli

emas. Xalqaro-huquqiy hujjatlar va xorijiy davlatlar tajribasi shaxsiy ma'lumotlarni himoya qilish mexanizmlarini takomillashtirishda muhim manba bo'lib xizmat qiladi.

XULOSA.

Mazkur tadqiqot natijalari shuni ko'rsatadiki, raqamli texnologiyalar rivoji sharoitida kiberjinoyatlarga qarshi kurash va shaxsiy ma'lumotlarni huquqiy jihatdan himoya qilish masalasi davlat xavfsizligi hamda shaxs huquq va erkinliklarini ta'minlash bilan uzviy bog'liqdir. O'zbekistonda mazkur sohada muayyan huquqiy asoslar shakllantirilgan bo'lsa-da, ularni amaliyotda qo'llash mexanizmlarini takomillashtirish, huquqni muhofaza qiluvchi organlarning institutsional va texnik salohiyatini kuchaytirish zarurati saqlanib qolmoqda. Shu bois, kiberxavfsizlikni ta'minlash bo'yicha milliy siyosatni xalqaro standartlar bilan uyg'unlashtirish, huquqiy, tashkiliy va ma'rifiy chora-tadbirlarni kompleks ravishda amalga oshirish kiberjinoyatlarga qarshi samarali kurashning muhim sharti hisoblanadi. Tahlillar shuni ko'rsatadiki, mavjud qonunchilik bazasi muayyan darajada shakllangan bo'lsa-da, amaliyotda uni qo'llashda muammolar saqlanib qolmoqda. Xususan, aholining huquqiy va raqamli savodxonligi yetarli darajada emasligi, texnik va kadrlar salohiyatining cheklanganligi, shuningdek, kiberjinoyatlarning transmilliy xususiyatga ega ekani huquqni muhofaza qiluvchi organlar faoliyatini murakkablashtirmoqda. Shu bois, faqat jazolash mexanizmlariga tayanish kutilgan natijani bermaydi. Mazkur muammolarni bartaraf etish uchun shaxsiy ma'lumotlarni himoya qilishga oid qonunchilikni xalqaro standartlar asosida takomillashtirish, kiberxavfsizlik bo'yicha maxsus mutaxassislar tayyorlash, aholiga mo'ljallangan doimiy o'quv va axborot kompaniyalarini yo'lga qo'yish muhim ahamiyat kasb etadi. Shuningdek, xalqaro hamkorlikni kuchaytirish va ilg'or xorijiy tajribani joriy etish kiberjinoyatlarga qarshi kurash samaradorligini oshirishga xizmat qiladi. Umuman olganda, kiberjinoyatlarga qarshi kurash va shaxsiy ma'lumotlarni himoya qilish masalasi kompleks yondashuvni talab etadi. Davlat, jamiyat va har bir fuqaroning mas'uliyatli ishtiroki bilangina raqamli makonda huquq va erkinliklarning ishonchli himoyasini ta'minlash mumkin.

"Raqamli makonda shaxsiy ma'lumotlarning himoyasi — bu texnik masala emas, balki inson huquqlarini ta'minlashning zamonaviy shaklidir."

FOYDALANILGAN ADABIYOTLAR VA RESURSLAR RO'YXATI:

1. O'zbekiston Respublikasi Jinoyat kodeksi. – lex.uz.
2. O'zbekiston Respublikasi "Kiberxavfsizlik to'g'risida"gi Qonuni
3. O'zbekiston Respublikasi Prezidentining 153-sonli "Axborot texnologiyalari yordamida sodir etilgan jinoyatlarga qarshi kurashni kuchaytirish chora-tadbirlari to'g'risida"gi qarori.
4. O'zbekiston Respublikasi Prezidentining "O'zbekiston–2030" strategiyasini amalga oshirish chora-tadbirlari to'g'risida"gi farmoni.
5. O'zbekiston Respublikasi Oliy sudi Plenumining "Firibgarlikka oid ishlar bo'yicha sud amaliyoti to'g'risida"gi qarori.
6. Ichki ishlar vazirligi huzuridagi Kiberxavfsizlik markazi statistik tahlillari, 2019–2024-yillar.
7. Daryo.uz analitik maqolasi: "O'zbekistonda kiberjinoyatlar soni 25 baravarga oshdi", 2024-yil 27-avgust. – daryo.uz.
8. Budapesht Konvensiyasi – Kiberjinoyatlar to'g'risidagi Yevropa Kengashi konvensiyasi. – coe.int.