O‘ZBEKISTONDA KIBERJINOYATCHILIKNING BUGUNGI HOLATI VA UNGA QARSHI KURASH

Ergashev Quvonchbek Anvarovich
Termiz davlat universiteti Yuridik fakulteti
Yurisprudensiya ta’lim yo‘nalishi 1-kurs 425-guruh talabasi
E-mail: ergashevquvonch2007@gmail.com

Annotatsiya. Ushbu maqolada O‘zbekistonda kiberjinoyatchilikning bugungi holati, uning dinamikasi va ushbu turdagi jinoyatlarga qarshi kurashishning huquqiy-tashkiliy asoslari tahlil qilinadi. Tadqiqotda so‘nggi besh yillik statistik ma’lumotlar asosida kiberjinoyatlarning 68 baravarga oshishi, ayniqsa bank kartalari bilan bog‘liq ***firibgarliklarning (98%) keskin ko‘payishi sabablari o‘rganilgan. Maqolada 2026-2026 yillar davomida fuqarolarga yetkazilgan 1,9 trillion so‘mdan ortiq zarar miqdori*** va jinoyatlarning sodir etilish usullari (fishing, SMS-kodlar, onlayn savdo) atroflicha yoritilgan. Shuningdek, «Kiberxavfsizlik to‘g‘risida»gi qonun va 2026-2030 yillarga mo‘ljallangan kiberxavfsizlik strategiyasining ahamiyati muhokama qilinadi. Tadqiqot natijasida kiberjinoyatchilikka qarshi kurashishda xalqaro hamkorlikni kuchaytirish va aholining raqamli savodxonligini oshirish bo‘yicha amaliy tavsiyalar ishlab chiqilgan.

Kalit so'zlar:kiberjinoyatchilik, kiberxavfsizlik, fishing, raqamli iqtisodiyot, ***bank kartalari, firibgarlik, axborot texnologiyalari, O‘zbekiston 2026***

Аннотация.В данной статье анализируется современное состояние киберпреступности в Узбекистане, ее динамика и правовые основы борьбы с этим видом преступлений. На основе статистических данных за последние пять лет исследуются причины 68-кратного роста киберпреступлений, особенно резкого увеличения мошенничества с банковскими картами (98%). В статье подробно освещаются методы совершения преступлений (фишинг, SMS-коды, онлайн-торговля) и ущерб, нанесенный гражданам в размере более 1,9 трлн _____ в период 2021-2024 гг. Также обсуждается значение Закона «О

кибербезопасности» и Стратегии кибербезопасности на 2026-2030 годы. По результатам исследования разработаны практические рекомендации по укреплению международного сотрудничества и повышению цифровой грамотности населения для борьбы с киберпреступностью.

Ключевые слова: киберпреступность, кибербезопасность, фишинг, цифровая экономика, банковские карты, мошенничество, информационные технологии.

Abstract. This article analyzes the current state of cybercrime in Uzbekistan, its dynamics, and the legal and organizational frameworks for combating these crimes. Based on statistical data from the past five years, the study examines the reasons for the 68-fold increase in cybercrimes, particularly the sharp rise in bank card fraud (98%). The article details the methods of committing crimes (phishing, SMS codes, online trade) and the damage caused to citizens, amounting to over 1.9 trillion soums during 2021-2024. The significance of the Law 'On Cybersecurity' and the Cybersecurity Strategy for 2026-2030 are also discussed. As a result of the study, practical recommendations have been developed to strengthen international cooperation and improve digital literacy among the population to combat cybercrime effectively.

Keywords: cybercrime, cybersecurity, phishing, digital economy, bank cards, fraud, information technology, Digital Uzbekistan.

Kirish. Insoniyat taraqqiyotining hozirgi bosqichi axborot texnologiyalarining jadal rivojlanishi va barcha sohalarga raqamli yechimlarning kirib kelishi bilan xarakterlanadi. O‘zbekiston Respublikasida ham «Raqamli O‘zbekiston – 2030» strategiyasi doirasida davlat boshqaruvi, iqtisodiyot, sog‘liqni saqlash va ta’lim tizimlarini to‘liq raqamlashtirish bo‘yicha keng ko‘lamli islohotlar amalga oshirilmoqda. Biroq, texnologik imkoniyatlarning kengayishi o‘z navbatida kiberjinoyatchilik kabi yangi va murakkab tahdidlarni yuzaga keltirdi [8; 15 b]. Kiberjinoyatchilik nafaqat shaxsiy ma’lumotlarning daxlsizligiga, balki davlatning iqtisodiy xavfsizligi va barqarorligiga ham jiddiy xavf solmoqda. Bugungi kunda

internet foydalanuvchilari sonining 31 milliondan oshishi va onlayn xizmatlarning ommalashishi jinoyatchilar uchun yangi maydon yaratdi.

So‘nggi yillarda O‘zbekistonda kiberjinoyatlar sonining keskin o‘sishi kuzatilmoqda. Agar 2019-yilda ushbu sohada jami 863 ta jinoyat qayd etilgan bo‘lsa, 2024-yilga kelib bu ko‘rsatkich 58 800 tadan oshib ketdi [1; 1 b]. Bu kiberjinoyatchilikning umumiy jinoyatchilik tarkibidagi ulushi 6,2 foizdan 44,4 foizgacha ko‘tarilganini anglatadi. Ya’ni, bugungi kunda mamlakatimizda sodir etilayotgan har ikkita jinoyatning bittasi axborot texnologiyalari vositasida amalga oshirilmoqda. Ushbu tendensiya kiberjinoyatchilikka qarshi kurashish mexanizmlarini qayta ko‘rib chiqishni va takomillashtirishni taqozo etadi. Jinoyatchilarning usullari kundan-kunga murakkablashib, an’anaviy firibgarlikdan yuqori texnologik kiberhujumlar va ijtimoiy injeneriya usullariga o‘tmoqda.

Kiberjinoyatchilikning transmilliy xarakterga egaligi unga qarshi kurashni yanada qiyinlashtiradi. Ko‘pgina hollarda jinoyatchilar xorijiy davlatlar hududida turib, O‘zbekiston fuqarolarining mablag‘larini talon-toroj qilmoqdalar. Bu esa nafaqat milliy huquq-tartibot organlarining faolligini, balki xalqaro hamkorlikning yangi darajaga ko‘tarilishini talab qiladi. Davlatimiz rahbari tomonidan 2022-yilda imzolangan «Kiberxavfsizlik to‘g‘risida»gi qonun ushbu sohadagi huquqiy bo‘shliqlarni to‘ldirishda muhim qadam bo‘ldi. Biroq, texnologiyalar rivoji qonun ijodkorligi jarayonidan tezroq harakatlanayotgani yangi strategik yondashuvlarni talab etmoqda.

Kiberjinoyatlarning ijtimoiy-psixologik jihatlari ham alohida e’tiborga loyiq. Fuqarolarning raqamli savodxonligi pastligi, ayniqsa yoshlar va keksa yoshdagilarning internetdagi xavflardan yetarli darajada xabardor emasligi jinoyatchilar uchun qulay sharoit yaratadi. Fishing (soxta havolalar) va SMS-kodlarni qo‘lga kiritish orqali amalga oshirilayotgan o‘g‘riliklar fuqarolarning bank tizimiga bo‘lgan ishonchiga ham putur yetkazishi mumkin. Shuning uchun ham, kiberjinoyatchilikka qarshi kurashish faqatgina jazo choralarini qo‘llash emas, balki keng ko‘lamli profilaktika va ta’lim jarayonlarini ham o‘z ichiga olishi shart.

Ushbu maqolaning maqsadi O‘zbekistondagi kiberjinoyatchilikning hozirgi holatini statistik ma’lumotlar asosida tahlil qilish, uning asosiy turlari va sodir etilish usullarini o‘rganish hamda unga qarshi kurashishning samarali yo‘llarini ishlab chiqishdan iborat. Maqolada kiberxavfsizlik sohasidagi mavjud muammolar yoritilib, ularni hal etish bo‘yicha huquqiy va texnik tavsiyalar beriladi.

Mavzuga oid adabiyotlar tahlili. Kiberjinoyatchilik muammosi jahon ilmiy hamjamiyati tomonidan keng o‘rganilmoqda. Ross Anderson va Tayler Mur kabi nufuzli olimlar o‘z tadqiqotlarida kiberjinoyatchilikni yuqori rentabelli iqtisodiy soha sifatida ta’riflashgan. Ularning fikricha, axborot tizimlaridagi zaifliklar ko‘pincha texnik xatolar emas, balki noto‘g‘ri iqtisodiy rag‘batlar tufayli yuzaga keladi [15; 14 b]. Manuel Kastells esa o‘zining «Tarmoqli jamiyatning yuksalishi» asarida kiberfazoda sodir etilayotgan jinoyatlar global axborot oqimlarining nazorat qilinmasligi oqibati ekanini ta’kidlaydi. O‘zbekistonlik huquqshunos olimlardan M. Rustambayev va U. Nasimovlar kiberjinoyatlarning kriminologik tavsifiga oid ishlarida milliy qonunchilikni xalqaro standartlarga, xususan Budapesht konvensiyasi talablariga moslashtirish zarurligini ko‘rsatib o‘tishgan [14; 5 b].

Mahalliy tadqiqotchilar, jumladan B. Mamajonov va Sh. Suyunovlar kiberjinoyatchilikning O‘zbekistondagi o‘ziga xos xususiyatlarini tahlil qilib, asosiy e’tiborni bank-moliya sohasidagi kiberfiribgarliklarga qaratganlar. Ularning tadqiqotlarida ijtimoiy injeneriya usullarining samaradorligi fuqarolarning axborot xavfsizligi madaniyati bilan bog‘liqligi isbotlangan. Shuningdek, so‘nggi yillarda sun’iy intellekt va dipfeyk texnologiyalari yordamida sodir etilayotgan jinoyatlar bo‘yicha xalqaro tajriba tahlili ham dolzarb ahamiyat kasb etmoqda. Adabiyotlar tahlili shuni ko‘rsatadiki, kiberjinoyatchilikka qarshi kurashda faqat texnik yondashuv yetarli emas, balki huquqiy, iqtisodiy va ijtimoiy omillarning kompleks hamkorligi zarurdir.

Metodologiya. Ushbu tadqiqotda kiberjinoyatchilik holatini tahlil qilish uchun bir qator ilmiy metodlardan foydalanildi. Birinchidan, O‘zbekiston Respublikasi Ichki ishlar vazirligi (IIV) Kiberjinoyatlar markazi va Kiberxavfsizlik markazi

tomonidan taqdim etilgan 2019-2024 yillar oralig‘idagi rasmiy statistik ma’lumotlar asosida miqdoriy tahlil amalga oshirildi. Bu kiberjinoyatlarning o‘sish dinamikasini va umumiy jinoyatchilik tarkibidagi o‘rnini aniqlash imkonini berdi. Ikkinchidan, qiyosiy-huquqiy metod yordamida O‘zbekistonning «Kiberxavfsizlik to‘g‘risida»gi qonuni va xalqaro normativ hujjatlar (Budapesht konvensiyasi) o‘rtasidagi muvofiqlik darajasi o‘rganildi.

Uchinchi bosqichda kiberjinoyatlarning sodir etilish usullari bo‘yicha guruhlash va tasniflash metodi qo‘llanildi. Bunda bank kartalari bilan bog‘liq o‘g‘riliklar, fishing hujumlari va ijtimoiy injeneriya holatlari alohida toifalarga ajratilib tahlil qilindi. Tadqiqot davomida jinoyat natijasida yetkazilgan moddiy zararning iqtisodiy hisob-kitoblari ko‘rib chiqildi. Shuningdek, raqamli dalillarni to‘plash va saqlash jarayonidagi muammolar ekspertlar fikrlari asosida tahlil qilindi. Tadqiqot ob’ekti sifatida O‘zbekistonning milliy kibermakoni va undagi huquqiy munosabatlar olindi.

Metodologik asos sifatida tizimli yondashuv tanlandi, bu esa kiberjinoyatchilikni nafaqat huquqbuzarlik, balki texnologik va ijtimoiy hodisa sifatida kompleks o‘rganishga xizmat qildi. Tadqiqot jarayonida internetdagi ochiq manbalar, xalqaro kibertahdidlar monitoringi xizmatlari (Kasperskiy laboratoriyasi hisobotlari) ma’lumotlaridan ham foydalanildi. Bu metodlar majmuasi tadqiqot natijalarining xolisligi va ilmiy asoslanganligini ta’minladi.

Tahlil va natija. O‘zbekistonda kiberjinoyatchilikning o‘sish sur’atlari xalqaro tendensiyalardan ham tezroq ekani kuzatilmoqda. Tahlillar shuni ko‘rsatadiki, so‘nggi besh yil ichida kiberjinoyatlar soni 68 baravarga ko‘paygan. Masalan, 2019-yilda atigi 18 turdagi kiberjinoyatlar qayd etilgan bo‘lsa, 2025-yilga kelib ularning turlari 62 taga yetgan. Bu esa jinoyatchilarning yangi texnologiyalarni (AI, Deepfake) o‘zlashtirib, usullarini diversifikatsiya qilayotganidan dalolat beradi.

Quyidagi jadvalda 2019-2025-yillardagi kiberjinoyatchilik holatining asosiy indikatorlari qiyosiy ko‘rsatilgan.

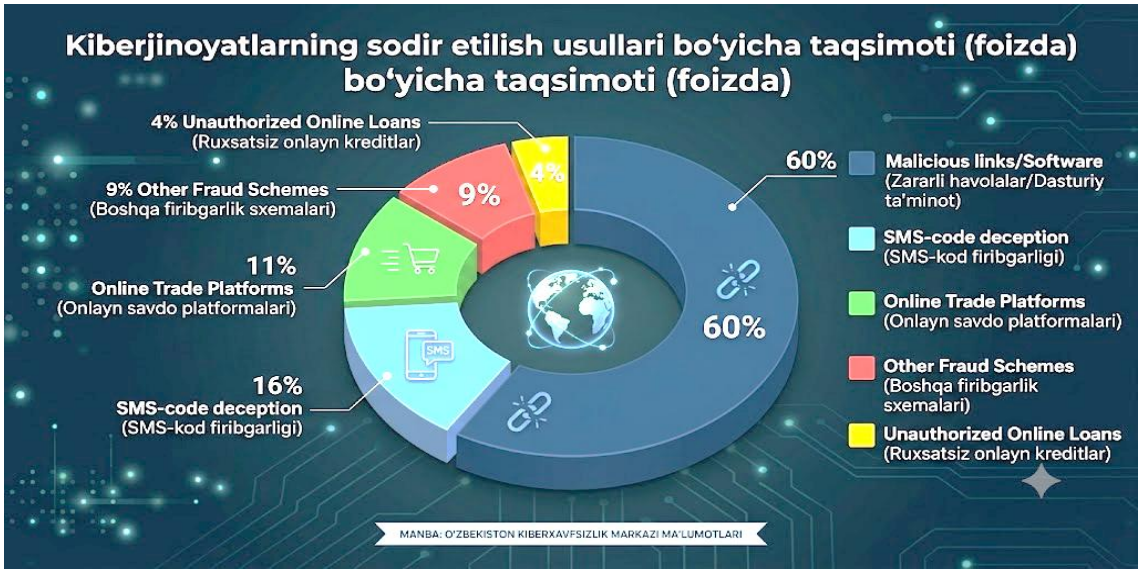
1-jadval

Kiberjinoyatchilikning 6 yillik dinamikasi (2019-2025-yy.)

Ko‘rsatkichlar	2019 yil	2024 yil	O‘sish sur’ati
Jinoyatlarning umumiy soni	863 ta	58 800 ta	68 baravar
Jinoyat turlari soni	18 tur	62 tur	3.4 baravar
Umumiy jinoyatchilikdagi ulushi	1.2%	44.4%	37 baravar
Fuqarolarga yetkazilgan zarar	12 mlrd so‘m	603 mlrd so‘m	50 baravar

Ushbu raqamlar kiberjinoyatchilikning naqadar dolzarb muammoga aylanganini yaqqol ko‘rsatadi. Ayniqsa, 2025-yilda kiberjinoyatlar soni 2024-yilga nisbatan 9,1 baravarga oshganligi xavotirli holatdir. Tadqiqot natijalariga ko‘ra, kiberjinoyatlarning 98 foizi aynan bank kartalari bilan bog‘liq o‘g‘rilik va firibgarliklardan iborat. Bu holat mamlakatda naqd pulsiz hisob-kitoblar tizimi rivojlanishi bilan kiberjinoyatchilarning qiziqishi ham oshganini anglatadi.

Kiberjinoyatlarning sodir etilish usullari bo‘yicha tahlil shuni ko‘rsatadiki, 60 foiz holatlarda jinoyatchilar zararli havolalar va dasturlar yuborish orqali mobil qurilma boshqaruvini qo‘lga kiritadilar. 16 foiz holatlarda esa «ijtimoiy injeneriya» usuli bilan, ya’ni fuqaroni aldab, uning mobil ilovaga kirish SMS-kodini olish orqali jinoyat sodir etiladi. Shuningdek, onlayn savdo platformalaridagi firibgarliklar (11%) va fuqarolar nomiga ruxsatsiz onlayn kredit rasmiylashtirish (4%) kabi yangi turlar ham keng tarqalmoqda.



1-rasm. Kiberjinoyatlarning sodir etilish usullari bo‘yicha taqsimoti (foizda)

2021-2025-yillar davomida kiberjinoyatchilar tomonidan fuqarolarning jami 1,9 trln so‘mdan ortiq mablag‘i o‘g‘irlangan. Faqatgina 2025-yilning o‘zida bu zarar 603 mlrd so‘mni tashkil etgan. Bu iqtisodiy zarar nafaqat fuqarolarning farovonligiga, balki davlatning raqamli iqtisodiyotga o‘tish jarayoniga ham salbiy ta’sir ko‘rsatmoqda. Jinoyatchilar ko‘pincha Telegram, Instagram va Facebook kabi ijtimoiy tarmoqlar orqali o‘z tuzoqlarini qurishadi, bu erda «yutuqli o‘yinlar», «arzun mahsulotlar» yoki «yordam pullari» haqidagi yolg‘on xabarlar asosiy qurol bo‘lib xizmat qiladi.

Huquqiy tahlil natijalari shuni ko‘rsatdiki, O‘zbekiston kiberxavfsizlikni ta’minlash borasida muhim qonunlarni qabul qilgan bo‘lsa-da, kiberjinoyatchilikning transmilliy xarakteri sababli tergov jarayonlari qiyin kechmoqda. IIV tomonidan 2025-yil boshidan buyon 483 ta fishing saytlari va 1508 ta zararli havolalar bloklangani ijobiy natijadir. Biroq, jinoyatdan yetkazilgan zararni undirish darajasi hali ham pastligicha qolmoqda, chunki mablag‘lar darhol kriptovalyutalarga aylantirilib, mamlakatdan olib chiqib ketilmoqda.

Muhokama. Tahlil natijalari shuni ko‘rsatadiki, O‘zbekistonda kiberjinoyatchilik an’anaviy jinoyatchilikni siqib chiqarmoqda. Har ikki jinoyatning biri internet orqali sodir etilishi huquq-tartibot organlari faoliyatini tubdan raqamlashtirish zarurligini ko‘rsatadi. Birinchi navbatda, fuqarolarning raqamli savodxonligi masalasini ko‘rib chiqish lozim. Nega jinoyatchilar bunchalik oson muvaffaqiyatga erishmoqda? Sababi – oddiy «kibergigiyena» qoidalariga rioya qilmaslikdir. Ko‘p hollarda fuqarolar o‘z ixtiyori bilan SMS-kodlarni begonalarga berishadi yoki shubhali havolalarga kirib, bank kartasi ma’lumotlarini kiritishadi.

Huquqiy jihatdan, 2026-2030 yillarga mo‘ljallangan kiberxavfsizlik strategiyasi o‘z vaqtida qabul qilingan hujjatdir. Unda nazarda tutilgan Adliya, Energetika vazirliklari va Soliq qo‘mitasida maxsus kiberxavfsizlik bo‘linmalarining tashkil etilishi davlat organlari himoyasini kuchaytiradi. Biroq, xususiy sektorda,

ayniqsa onlayn do‘konlar va to‘lov tizimlarida xavfsizlik standartlari hali ham past darajada qolmoqda. Shuningdek, kriptoaktivlar aylanmasi sohasidagi jinoyatlarning (2424 ta holat) ko‘payishi yangi turdagi raqamli monitoring tizimlarini talab qiladi.

Xalqaro hamkorlik masalasi ham o‘ta dolzarbdir. Kiberjinoyatchilar ko‘pincha VPN xizmatlari va xorijiy serverlardan foydalanishi ularni aniqlashni qiyinlashtiradi. O‘zbekistonning Budapesht konvensiyasiga qo‘shilishi borasidagi sa’y-harakatlar ushbu muammoni hal qilishda kalit rolini o‘ynashi mumkin. Budapesht konvensiyasi raqamli dalillarni xalqaro miqyosda almashish va transmilliy kiberjinoyatchilarni birgalikda ta’qib qilish mexanizmini taklif etadi. Muhokama qilinishi kerak bo‘lgan yana bir jihat – banklarning mas’uliyati. Ko‘p hollarda o‘g‘irlik sodir etilganidan so‘ng mablag‘ni qaytarish imkoni bo‘lmaydi. Banklar va to‘lov tizimlari shubhali tranzaksiyalarni (anti-fraud tizimlari) avtomatik to‘xtatish texnologiyalarini yanada kuchaytirishi zarur.

Tadqiqot natijasida quyidagi xulosalarga kelindi:

Birinchidan, O‘zbekistonda kiberjinoyatchilik kriminogen vaziyatning asosiy omiliga aylangan va uning o‘sish sur’ati (68 baravar) favqulodda choralarni talab qiladi.

Ikkinchidan, jinoyatlarning mutlaq ko‘pchiligi (98%) bank kartalari bilan bog‘liqligi aholining moliyaviy-raqamli savodxonligini oshirishni milliy xavfsizlik darajasidagi masalaga aylantiradi.

Uchinchidan, kiberjinoyatlarning sodir etilish usullari murakkablashib, sun’iy intellekt elementlari kirib kelmoqda.

Ushbu muammolarni bartaraf etish uchun quyidagi tavsiyalar taklif etiladi:

1. O‘rta maktab va oliy ta’lim tizimida «Raqamli gigiyena» darslarini majburiy joriy etish orqali aholi xabardorligini tizimli oshirish.

2. «Kiberxavfsizlik to‘g‘risida»gi Budapesht konvensiyasiga a’zo bo‘lish jarayonini jadallashtirish va xalqaro raqamli forensics (ekspertiza) hamkorligini yo‘lga qo‘yish.

3. Bank va to‘lov tizimlariga sun’iy intellektga asoslangan anti-firibgarlik (Anti-fraud) tizimlarini majburiy o‘rnatish bo‘yicha qat’iy talablar qo‘yish.

4. Kiberjinoyatlarni tergov qiluvchi xodimlar (kiberpolitsiya) uchun doimiy malaka oshirish kurslarini tashkil etish va raqamli laboratoriyalar sonini ko‘paytirish.

5. Kiberjinoyat oqibatida yetkazilgan zararni qoplash bo‘yicha maxsus sug‘urta mexanizmlarini ishlab chiqish.

Kiberjinoyatchilikka qarshi kurashish faqatgina huquq-tartibot organlarining vazifasi emas, balki davlat, jamiyat va xususiy sektorning birgalikdagi strategik vazifasidir. Faqatgina kompleks yondashuv orqali O‘zbekistonning raqamli suverenitetini va fuqarolarning kibermakonidagi xavfsizligini ta’minlash mumkin.

Foydalanilgan adabiyotlar

1. O‘zbekiston Respublikasining 2022-yil 15-apreldagi «Kiberxavfsizlik to‘g‘risida»gi O‘RQ-764-son Qonuni.
2. O‘zbekiston Respublikasi Prezidentining 2020-yil 5-oktabrdagi «Raqamli O‘zbekiston – 2030» strategiyasini tasdiqlash va uni samarali amalga oshirish chora-tadbirlari to‘g‘risida»gi PF-6079-son Farmoni.
3. IIV Kiberjinoyatlar markazi: 2024-yil yakunlari bo‘yicha statistik hisoboti. Spot.uz (2025).
4. Mirziyoyev Sh.M. «Raqamli texnologiyalar sohasida jinoyatlarga qarshi kurashish strategiyasi – 2030». (2026).
5. Nasimov U.U. «Kiberjinoyatlar: muammo, tahlil va yechimlar». Toshkent Davlat Yuridik Universiteti, (2023).
6. Ziyodul M. «Kiberjinoyatlar: tushunchasi, asosiy xususiyatlari va profilaktikasi». UZA ilmiy maqolalar to‘plami, (2026).
7. Kaspersky Cybersecurity Report 2023-2024: Central Asia and CIS dynamics.
8. Rustambayev M.X. O‘zbekiston Respublikasi Jinoyat huquqi kursi. Toshkent, (2021).
9. Suyunov Sh.Sh. «Kiberjinoyatlarning sabablari va oldini olish choralari». IIV Akademiyasi axborotnomasi, (2023).

10. Budapest Convention on Cybercrime (2001) and its relevance to New Uzbekistan Strategy.
11. Gazeta.uz. «2021-2024 yillarda kiberjinoyatlardan yetkazilgan zarar 1,9 trln so‘mga yetdi». (2025).
12. Digital Uzbekistan 2030: Challenges of Cyber-governance and Security. International Journal of Information Security, (2024).
13. Global Cybersecurity Index 2024: Uzbekistan's position and trends.
14. Karimov A. «Raqamli forensics: nazariya va amaliyot». Ilmiy xabarnoma, (2024).
15. Anderson R., Moore T. «The Economics of Information Security». Science Magazine, (2021).