AXBOROT TEXNOLOGIYALARI SOHASIDA SODIR ETILAYOTGAN JINOYATLARNING HUQUQIY TAVSIFI HAMDA ULARNING OLDINI OLISHGA QARATILGAN PROFILAKTIK CHORA-TADBIRLAR

Toshimov Nurg'ali Erpolatovich

O'zbekiston Respublikasi Oliy ta'lim, fan va innovatsiyalar vazirligi

Qozog'iston Respublikasi Fan va oliy ta'lim vazirligi

Notijorat aktsiyadorlik jamiyati filiali

Chirchiq shahridagi "M.Auezov nomidagi Janubiy Qozog'iston universiteti"

"Yurisprudensiya" fakulteti 1-kurs magistri

Annotatsiya: Ushbu maqola axborot texnologiyalari sohasida sodir etilayotgan jinoyatlarning huquqiy tavsifini va ularning oldini olishga qaratilgan profilaktik chora-tadbirlarni O'zbekiston Respublikasi misolida kompleks tarzda tadqiq etadi. Tadqiqot sifatiy tadqiqot paradigmasi asosida qurilgan bo'lib, hujjatli tahlil, qiyosiy huquqiy tahlil va tizimli adabiyotlar sharhi usullaridan foydalanilgan. O'zbekiston Respublikasi Jinoyat Kodeksining tegishli moddalari, xalqaro huquqiy hujjatlar — jumladan, Budapeshta Konventsiyasi (2001) va BMTning Kiberjinoyatchilikka qarshi Konventsiyasi loyihasi (2023) — hamda 2018–2023-yillar oralig'idagi 47 ta sudlov qarori tahlil qilingan. Qiyosiy tahlil doirasida O'zbekistonning kiberhimoya tizimi Germaniya, Estoniya, Qozog'iston va Singapur tizimlari bilan solishtirilgan. Natijalar shuni ko'rsatdiki, mavjud qonunchilik zamonaviy kibertahdidlarni to'liq qamrab olmaydi, sudlov amaliyotida ekspert-kriminalistik salohiyat yetarli emas va profilaktika tizimining barcha uch yo'nalishi — texnik, huquqiy-institutsional hamda ijtimoiy-tarbiyaviy — rivojlantirishni talab etadi. Tadqiqot O'zbekiston uchun milliy kiberhavfsizlik strategiyasini takomillashtirish bo'yicha amaliy tavsiyalar bilan yakunlanadi.

Kalit so'zlar: kiberjinoyatchilik, axborot xavfsizligi, huquqiy tavsif, profilaktik chora-tadbirlar, O'zbekiston, qiyosiy huquq, kiberxavfsizlik, raqamli jinoyatchilik, Jinoyat kodeksi, xalqaro hamkorlik

Abstract: This article provides a comprehensive study of the legal characterization of crimes committed in the field of information technology and preventive measures aimed at countering them, using the Republic of Uzbekistan as a case study. The research is built upon a qualitative research paradigm, employing document analysis, comparative legal analysis, and systematic literature review as primary methodological approaches. The study analyzes the relevant articles of the Criminal Code of the Republic of Uzbekistan, key international legal instruments — including the Budapest Convention on Cybercrime (2001) and the UN Convention against Cybercrime draft (2023) — as well as 47 judicial decisions issued between 2018 and 2023. Within the comparative legal framework, Uzbekistan's cybersecurity system is assessed against those of Germany, Estonia, Kazakhstan, and Singapore across five dimensions: legislative completeness, institutional capacity, international cooperation, prevention effectiveness, and digital economy integration. The findings reveal that existing legislation does not fully cover contemporary cyber threats, forensic expert capacity in judicial proceedings remains insufficient, and all three dimensions of the prevention system — technical, legal-institutional, and socio-educational — require substantial development. The article concludes

with practical recommendations for strengthening Uzbekistan's national cybersecurity strategy in alignment with international standards.

Keywords: cybercrime, information security, legal characterization, preventive measures, Uzbekistan, comparative law, cybersecurity, digital crime, criminal code, international cooperation

Аннотация: Настоящая статья посвящена комплексному исследованию правовой характеристики преступлений в сфере информационных технологий и профилактических мер, направленных на их предупреждение, на примере Республики Узбекистан. Исследование построено на основе качественной исследовательской парадигмы с применением методов документального анализа, сравнительно-правового анализа и систематического обзора литературы. В рамках исследования проанализированы соответствующие статьи Уголовного кодекса Республики Узбекистан, ключевые международно-правовые документы — в частности, Будапештская конвенция о киберпреступности (2001) и проект Конвенции ООН против киберпреступности (2023), — а также 47 судебных решений, вынесенных в период с 2018 по 2023 год. В рамках сравнительного правового анализа система кибербезопасности Узбекистана сопоставлена с аналогичными системами Германии, Эстонии, Казахстана и Сингапура по пяти критериям: полнота законодательства, институциональный потенциал, уровень международного сотрудничества, эффективность профилактики и степень интеграции в цифровую экономику. Результаты исследования свидетельствуют о том, что действующее законодательство не охватывает в полной мере современные киберугрозы, судебно-экспертный потенциал в рамках судопроизводства остаётся недостаточным, а все три направления системы профилактики — техническое, правово-институциональное и социально-воспитательное — нуждаются в существенном развитии. Статья завершается практическими рекомендациями по совершенствованию национальной стратегии кибербезопасности Узбекистана в соответствии с международными стандартами.

Ключевые слова: киберпреступность, информационная безопасность, правовая характеристика, профилактические меры, Узбекистан, сравнительное право, кибербезопасность, цифровая преступность, уголовный кодекс, международное сотрудничество

KIRISH

Zamonaviy raqamli jamiyatda axborot-kommunikatsiya texnologiyalarining jadal rivojlanishi iqtisodiy, ijtimoiy va siyosiy hayotning barcha sohalarini qamrab olmoqda. Internet tarmoqlarining globallashuvi, sun'iy intellekt tizimlarining kengayishi va raqamli moliyaviy infratuzilmalarning shakllanishi bilan bir qatorda, ushbu muhitdan noqonuniy maqsadlarda foydalanuvchi jinoyatchilik faoliyati ham misli ko'rilmagan ko'lamga erishmoqda. Kiberjinoyatchilik bugungi kunda nafaqat alohida shaxslar, balki davlat institutlari, moliyaviy tashkilotlar va kritik infratuzilmalar uchun ham jiddiy tahdid manbai bo'lib qolmoqda (Wall, 2007; Brenner, 2010).Jahon miqyosida kiberjinoyatchilikdan ko'rilayotgan zarar yildan yilga o'sib bormoqda. Morgan (2020) tomonidan o'tkazilgan tadqiqotga ko'ra, 2021-yilga kelib kiberjinoyatchilikdan yetkazilgan global zarar yillik 6 trillion AQSh dollaridan oshib ketgan bo'lib, bu ko'rsatkich an'anaviy tashkiliy jinoyatchilik ko'rsatkichlaridan sezilarli darajada yuqoridir. O'zbekiston Respublikasida ham raqamlashtirish siyosatining kuchayib borishi fonida kiberjinoyatchilik holatlarining soni yil sayin ortib borayotganligi qayd etilmoqda (O'zbekiston Respublikasi Ichki Ishlar Vazirligi, 2022). Kiberjinoyatchilik muammosi ko'p qirrali xususiyatga

ega bo'lib, uni faqatgina texnik yoki huquqiy nuqtayi nazardan baholash yetarli emas. Bu borada kompleks yondashuv — ya'ni jinoyatlarning huquqiy tavsifini, texnik mexanizmlarini va ijtimoiy-iqtisodiy omillarini birgalikda tahlil qilish — ilmiy hamjamiyat oldidagi dolzarb vazifalardan biri hisoblanadi (Yar & Steinmetz, 2019). Amaldagi qonunchilik bazasi esa ko'pincha texnologik taraqqiyot sur'atidan orqada qoladi, bu esa jinoyatchilarning qonuniy bo'shliqlardan foydalanishiga zamin yaratadi (Clough, 2015).

O'zbekiston Respublikasida kiberjinoyatchilikka oid huquqiy tartibga solish masalasi yaqin yillarda alohida e'tiborga sazovor bo'lmoqda. "Axborot xavfsizligi to'g'risida"gi Qonun (2022), O'zbekiston Respublikasi Jinoyat Kodeksining tegishli moddalari hamda "Elektron tijorat to'g'risida"gi Qonun (2015) kiberjinoyatchilik sohasida huquqiy asos yaratadi. Biroq, Sun'iy intellekt asosidagi yangi jinoyatchilik usullarining paydo bo'lishi va yurisdiktsiyalararo muammolar mavjud huquqiy mexanizmlarni takomillashtirish zaruratini ko'rsatmoqda (Sarre et al., 2018; O'zbekiston Respublikasi Adliya Vazirligi, 2023). Ushbu maqolaning asosiy maqsadi axborot texnologiyalari sohasidagi jinoyatlarni huquqiy jihatdan tasniflash, ularning sodir etilish mexanizmlari va ijtimoiy oqibatlarini tahlil qilish, shuningdek, O'zbekiston sharoitida samarali profilaktik chora-tadbirlar tizimini asoslashdan iborat. Tadqiqot doirasida xalqaro va milliy huquqiy hujjatlar qiyosiy tahlil qilinib, amaliyotda sinovdan o'tgan eng ilg'or profilaktika modellari ko'rib chiqiladi.

ADABIYOTLAR SHARHI

Kiberjinoyatchilik sohasidagi ilmiy adabiyotlar tahlili ushbu hodisaning ko'p qirrali tabiatini va tadqiqotchilar o'rtasida yagona konseptual çarçevaning hali shakllanmaganligini ko'rsatadi. Kiberjinoyatchilik tushunchasiga ilmiy ta'rif berish masalasi adabiyotlarda turlicha yondashuvlar bilan ifodalangan. Wall (2007) kiberjinoyatchilikni "kompyuter tarmoqlari yordamida yoki ularga qarshi yo'naltirilgan har qanday noqonuniy faoliyat" sifatida ta'riflaydi. Kengroq yondashuv tarafdori bo'lgan Gordon va Ford (2006) esa kiberjinoyatchilikni ikki asosiy toifaga ajratadilar: birinchi toifa — bevosita kompyuter tizimlariga qaratilgan jinoyatlar (hacking, DDoS hujumlar, zararli dasturlar tarqatish); ikkinchi toifa — kompyuter va internet vositalar sifatida xizmat qiladigan an'anaviy jinoyatlar (firibgarlik, tahdid, pornografiya tarqatish). Ushbu ikkilik tasnif keyingi ko'plab tadqiqotlarda asos sifatida qabul qilingan (Brenner, 2010; McGuire & Dowling, 2013).

Yar va Steinmetz (2019) o'zlarining keng qamrovli asarida kiberjinoyatchilikni ijtimoiy-kriminologik nuqtayi nazardan ko'rib chiqib, an'anaviy kriminologik nazariyalarning — xususan, tortishish nazariyasi (strain theory), nazorat nazariyasi (control theory) va differentsial uyushma nazariyasining (differential association theory) — raqamli muhitga qanchalik mos kelishini muhokama qiladi. Ularning xulosasiga ko'ra, mavjud kriminologik nazariyalar kiberjinoyatchilikni qisman tushuntira olsa-da, raqamli muhitning o'ziga xos xususiyatlari — anonimlik, geografik chegaralarning yo'qligi va jinoyat izlarini yo'q qilish imkoniyati — yangi nazariy çarçevalarni ishlab chiqishni taqozo etadi. Kiberjinoyatchilikni xalqaro miqyosda tartibga solish borasidagi eng muhim hujjat — 2001-yilda Budapeshta shahrida imzolangan Kiberjinoyatchilik to'g'risidagi Konventsiya (Budapest Convention on Cybercrime) — bugungi kunda 68 davlat tomonidan ratifikatsiya qilingan bo'lib, xalqaro huquqiy hamkorlikning asosiy vositasi hisoblanadi (Council of Europe, 2001). Clough (2015) ushbu konventsiyani tahlil qilib, uning to'rt asosiy yo'nalishni — kompyuter tizimlariga qarshi jinoyatlar, kompyuter bilan bog'liq jinoyatlar, kontent jinoyatlari va mualliflik huquqi buzilishlarini — qamrab olishini ta'kidlaydi. Biroq, konventsiyaga kiruvchi davlatlar soni hali ham cheklangan bo'lib, xususan Xitoy va Rossiya kabi yirik raqamli iqtisodiyotlar ushbu hujjatni imzolamaganligi samarali xalqaro

hamkorlikka to'siq yaratmoqda (Sarre et al., 2018). Yevropa Ittifoqining 2016-yilgi NIS Direktivi (Network and Information Security Directive) va 2018-yilgi GDPR (General Data Protection Regulation) kiberjinoyatchilikka qarshi kurashda tartibga solishning yangi avlodini ifodalaydi. Cavelty (2018) ushbu me'yoriy hujjatlarni tahlil qilib, GDPRning shaxsiy ma'lumotlarni himoya qilish sohasida dunyo miqyosida de-fakto standart bo'lib borayotganini ta'kidlaydi. Qolaversa, Schmitt (2017) tomonidan tahrirlab chiqilgan Tallinn Qo'llanmasi (Tallinn Manual 2.0) davlatlarning kiberhujumlarga nisbatan xalqaro huquq doirasidagi huquq va majburiyatlarini tizimli ravishda bayon etib, kiberjinoyatchilik va kiber urush o'rtasidagi huquqiy chegarani belgilashga urinadi.

O'zbekiston Respublikasida kiberjinoyatchilikka oid huquqiy baza so'nggi o'n yil ichida sezilarli darajada rivojlandi. Ma’murjonov (2021) milliy qonunchilikdagi o'zgarishlarni tahlil qilib, O'zbekiston Respublikasi Jinoyat Kodeksining 278–283-moddalari axborot xavfsizligiga qarshi jinoyatlar uchun javobgarlikni nazarda tutishini, biroq ushbu moddalarning amaldagi ijrosida sezilarli muammolar mavjudligini ko'rsatadi. Xususan, ekspert-kriminalistik tekshiruv imkoniyatlarining cheklanganligi va huquqni muhofaza qilish organlarining kasbiy tayyorgarlik darajasi ham muammolar orasida tilga olinadi. Mustaqil Davlatlar Hamdo'stligi (MDH) doirasida 2001-yilda imzolangan Axborot sohasidagi jinoyatchilikka qarshi hamkorlik to'g'risidagi Shartnoma mintaqaviy huquqiy asos sifatida xizmat qiladi (MDH Ijroiya Qo'mitasi, 2001). Tursunov (2020) ushbu shartnomaning amaliy samaradorligini baholab, texnik hamkorlik mexanizmlari va ma'lumot almashish tartiblari borasida hali ko'plab muammolar yechimini kutayotganini ta'kidlaydi. Markaziy Osiyo mintaqasida Qozog'iston va Rossiya qiyosida O'zbekistonning kiberjinoyatchilikka qarshi qonunchilik bazasi nisbatan rivojlanish bosqichida ekanligini Ergashev (2022) ham o'z tadqiqotida qayd etib o'tadi.

Fishing va ijtimoiy muhandislik. Hadnagy (2018) ijtimoiy muhandislik asosidagi kiberjinoyatchilikni keng tahlil qilib, jinoyatchilarning psixologik manipulyatsiya usullaridan — ishonch uyg'otish, qo'rqitish va shoshilish his-tuyg'ularini qo'zg'atish — qanchalik mahorat bilan foydalanishini ko'rsatadi. Proofpoint (2023) tadqiqotiga ko'ra, global kiberhujumlarning 84 foizi aynan ijtimoiy muhandislik elementlarini o'z ichiga oladi.

To'lov dasturlari (Ransomware). Liska va Gallo (2017) to'lov dasturlarining evolyutsiyasini kuzatib, ularning dastlabki oddiy shifrlovchi dasturlardan hozirgi "Ransomware-as-a-Service" (RaaS) modeligacha bo'lgan yo'lni tavsiflab beradi. IBM Security (2023) hisobotiga ko'ra, to'lov dasturlari hujumlarining o'rtacha ko'rgazmasi 4,54 million dollarni tashkil etadi va bu ko'rsatkich yil sayin o'sib bormoqda.

Moliyaviy kiberjinoyatchilik. Button va Cross (2017) onlayn firibgarliklarning turlarini va ularning qurbonlarga yetkazadigan moliyaviy hamda psixologik ta'sirini batafsil o'rganib chiqadi. Ularning tadqiqoti shuni ko'rsatadiki, kiberjinoyatchilik qurbonlari nafaqat moddiy zarar ko'radi, balki uyat, aybdorlik va ishonchni yo'qotish hissi kabi ikkilamchi travmani ham boshdan kechiradi.

Profilaktika sohasidagi adabiyotlarda uchta asosiy yondashuv ustunlik qiladi. Birinchidan, situatsion jinoyat profilaktikasi (Situational Crime Prevention — SCP) nazariyasi kiberjinoyatchilikka ham tatbiq etilmoqda: Clarke (1997) tomonidan ishlab chiqilgan va Yar (2005) tomonidan raqamli muhitga moslashtirilgan ushbu yondashuv jinoyat sodir etish uchun zarur sharoit va imkoniyatlarni kamaytirish orqali profilaktika qilishni tavsiya etadi. Ikkinchidan, Newman va Clarke (2003) "SCAREM" modeli asosida kiber muhitdagi profilaktika choralarini — masalan, ikki bosqichli autentifikatsiya va nol ishonch (zero-trust) arxitekturasini —

asoslaydi. Uchinchidan, Mitre ATT&CK va NIST Cybersecurity Framework kabi sanoat standartlari tashkilotlar uchun profilaktika va javob berish tizimini belgilash imkonini beradi (NIST, 2018). Davlat-xususiy sheriklik (public-private partnership) modelining kiberjinoyatchilikka qarshi kurashda ahamiyatini Hathaway va Klimburg (2012) ta'kidlagan bo'lib, ular Internet xizmat ko'rsatuvchilar, moliyaviy tashkilotlar va huquqni muhofaza qilish organlari o'rtasidagi ma'lumot almashish mexanizmlarini samarali profilaktikaning asosi sifatida ko'rsatadi. O'zbekiston sharoitida ushbu yondashuvning joriy etilish imkoniyatlarini Xoliqov (2023) maxsus o'rgangan bo'lib, uning xulosalariga ko'ra, tarmoqlararo hamkorlikning yo'lga qo'yilishi kiberjinoyatchilikni aniqlash vaqtini o'rtacha 40 foizga qisqartirishi mumkin.

METODOLOGIYA

Ushbu tadqiqot axborot texnologiyalari sohasidagi jinoyatlarning huquqiy tavsifini va profilaktik chora-tadbirlarini kompleks tarzda o'rganishga yo'naltirilgan bo'lib, sifatiy tadqiqot paradigmasi (qualitative research paradigm) asosida qurilgan. Tadqiqotda ko'p usulli (multi-method) sifatiy yondashuv qo'llanilgan bo'lib, u uch asosiy komponentni o'z ichiga oladi: hujjatli tahlil (document analysis), qiyosiy huquqiy tahlil (comparative legal analysis) va tizimli adabiyotlar sharhi (systematic literature review). Ushbu yondashuv huquqshunoslik va kriminologiya sohasidagi tadqiqotlarda keng qo'llanilib, murakkab ijtimoiy-huquqiy hodisalarni chuqur tushunishga imkon beradi (Creswell & Creswell, 2018). Tadqiqot epistemologik jihatdan interpretivizm (interpretivism) paradigmasiga tayanadi, ya'ni kiberjinoyatchilikka oid huquqiy normalar va ijtimoiy amaliyot o'rtasidagi bog'liqlik kontekstga bog'liq holda talqin qilinadi. Shu bilan birga, tadqiqot dizayni Yin (2018) tavsiya etgan holat tahlili (case study) metodologiyasining qiyosiy versiyasiga ham asoslanadi — xususan, bir necha davlatlarning huquqiy tajribasi solishtirilib, O'zbekiston uchun eng mos yondashuvlar aniqlangan. Ma'lumot to'plash jarayonida birlamchi va ikkilamchi manba turlari qo'llanilgan. Birlamchi manbalar qatoriga O'zbekiston Respublikasining normativ-huquqiy hujjatlari — jumladan, Jinoyat Kodeksi (1994, o'zgartishlar bilan), "Axborot xavfsizligi to'g'risida"gi Qonun (2022), "Elektron tijorat to'g'risida"gi Qonun (2015) va "Shaxsga doir ma'lumotlar to'g'risida"gi Qonun (2019) — matnlari kiradi va ular to'liq o'qib tahlil qilindi. Xalqaro manbalar sifatida Budapeshta Konventsiyasi (2001), Yevropa Ittifoqining NIS2 Direktivi (2022) va BMTning Kiberjinoyatchilikka qarshi Konventsiyasi loyihasi (2023) o'rganildi. Sudlov amaliyoti materiallariga kelsak, O'zbekiston Respublikasi Oliy sudi tomonidan 2018–2023-yillar oralig'ida axborot xavfsizligi jinoyatlari bo'yicha chiqarilgan 47 ta qaror tahlil qilindi. Ikkilamchi manbalar sifatida xalqaro ilmiy jurnallar — *Journal of Cybersecurity* (Oxford), *Crime, Law and Social Change* (Springer), *International Journal of Law and Information Technology* (Oxford) — hamda Interpol, Europol va UNODC tashkilotlarining yillik hisobotlari ishlatildi.

Adabiyotlar sharhi PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) protokoli asosida amalga oshirildi (Moher et al., 2009). Qidiruv Scopus, Web of Science, HeinOnline va Google Scholar ma'lumotlar bazalarida 2000–2024-yillar oralig'ini qamrab oldi. Qidiruv so'zlari sifatida "cybercrime AND legal framework", "information technology crime AND prevention", "cyber law AND Central Asia", "kiberjinoyatchilik AND O'zbekiston" kalit iboralari ishlatildi. Dastlab 1,247 ta manba aniqlandi. Sarlavha va annotatsiya darajasida sifat mezonlari asosida saralash natijasida 384 ta manba to'liq matn ko'rinishida o'qildi. Yakuniy tahlilga mavzu aloqadorligi, nashr sifati (peer-reviewed), til (o'zbek, rus, ingliz) va vaqt oralig'i mezonlari asosida 112 ta manba kiritildi. Bundan tashqari, O'zbekistonga oid milliy manbalar alohida to'plam sifatida ko'rib chiqildi, chunki ular xalqaro indekslash tizimlarida yetarlicha ifodalanmagan (Tursunov, 2020). Qiyosiy huquqiy tahlil metodologiyasi Zweigert va Kötz (1998) tomonidan ishlab chiqilgan funksional qiyoslash (functional comparison) tamoyiliga

asoslanadi. Solishtirishga O'zbekiston bilan birga quyidagi davlatlar huquqiy tizimlari kiritildi: Germaniya (rivojlangan kiberhimoya qonunchiligi namunasi sifatida), Estoniya (raqamli davlat boshqaruvi va kiberhimoya integratsiyasi bo'yicha), Qozog'iston (mintaqaviy o'xshashlik va MDH huquqiy an'anasi bo'yicha) hamda Singapur (rivojlanayotgan iqtisodiyotlar orasidagi ilg'or kiberhimoya tajribasi sifatida). Solishtirishning asosiy o'lchov ko'rsatkichlari sifatida qonunchilik to'liqligi, institutsional salohiyat, xalqaro hamkorlik darajasi va profilaktika samaradorligi tanlandi (Deflem, 2010).

Yig'ilgan ma'lumotlar tahlilida tematik tahlil (thematic analysis) usuli qo'llanildi. Braun va Klark (2006) tomonidan ishlab chiqilgan olti bosqichli tematik tahlil modeli — ma'lumotlar bilan tanishish, dastlabki kodlash, mavzularni izlash, mavzularni ko'rib chiqish, mavzularni aniqlash va nomini qo'yish, hamda hisobot yozish — ketma-ket amalga oshirildi. Kodlash jarayonida NVivo 14 dasturiy ta'minoti ishlatildi, bu esa katta hajmdagi sifatiy ma'lumotlarni tizimli ravishda qayta ishlash imkonini berdi (Bazeley & Jackson, 2013). Huquqiy hujjatlar tahlilida matn tahlili (content analysis) usuli ham qo'llanildi. Xususan, Jinoyat Kodeksining tegishli moddalari va xalqaro konventsiyalar o'rtasidagi terminologik hamda mazmuniy farqlar aniqlash uchun qiyosiy matris (comparative matrix) tuzildi. Qiyosiy matris to'rtta o'lcham bo'yicha shakllantirildi: jinoyat tarkibining elementlari, sanksiyalar darajasi, protsessual normalar va xalqaro hamkorlik mexanizmlari. Tadqiqotning ishonchliligi (reliability) va asosliligi (validity) ta'minlash maqsadida bir necha chora ko'rildi. Birinchidan, triangulyatsiya (triangulation) usuli qo'llanilib, bir xil hodisa turli manbalar va usullar orqali o'rganildi (Denzin, 1978). Ikkinchidan, ekspert ko'rib chiqishi (expert review) doirasida tadqiqot natijalari O'zbekiston Respublikasining huquq fakulteti o'qituvchilari va kiberhimoya mutaxassislari bilan muhokama qilindi. Uchinchidan, audit izi (audit trail) — ya'ni ma'lumot to'plash, kodlash va xulosalash bosqichlarini to'liq hujjatlashtirib borish — tadqiqotning takrorlanish imkonini oshirdi (Lincoln & Guba, 1985). Tadqiqot bir qator cheklovlarga ega ekanligi tan olinishi lozim. Birinchidan, O'zbekistondagi sudlov amaliyotiga oid to'liq statistik ma'lumotlarning ochiq manbalarda cheklangan holda mavjudligi miqdoriy tahlil o'tkazish imkonini qisqartirdi. Ikkinchidan, milliy manbalarning aksariyati o'zbek va rus tillarida bo'lganligi sababli, ularning xalqaro ilmiy hamjamiyat bilan solishtirilishi muayyan tarjima muammolarini keltirib chiqarishi mumkin (Tursunov, 2020). Uchinchidan, kiberjinoyatchilik sohasidagi texnologik o'zgarishlar juda tez sur'atda sodir bo'lganligi bois, tadqiqot natijalari ma'lum vaqt oralig'i bilan cheklanishi tabiiy holdir (Brenner, 2010). Ushbu cheklovlar hisobga olinib, xulosalar ifodalashda ehtiyotkorlik va ishonchlilik darajasi ko'rsatilgan. Nihoyat, tadqiqot jarayonida ilmiy halollik tamoyillariga to'liq rioya qilindi: barcha manbalar to'g'ri ko'rsatildi, boshqa mualliflarning fikrlari aniq ajratib ifodalandi va ma'lumotlarni taqdim etishda selektiv yondashuv qo'llanilmadi. Tadqiqot APA etika qo'llanmasi (2020) talablariga mos ravishda olib borildi.

NATIJALAR

Tadqiqot davomida to'plangan va tahlil qilingan ma'lumotlar to'rtta asosiy yo'nalish bo'yicha tizimlashtirilib taqdim etiladi: axborot texnologiyalari sohasidagi jinoyatlarning huquqiy tasnifi, O'zbekiston qonunchiligining xalqaro standartlarga muvofiqligi, sudlov amaliyotidagi tendentsiyalar va profilaktik chora-tadbirlarning samaradorligi.

1. Axborot Texnologiyalari Sohasidagi Jinoyatlarning Huquqiy Tasnifi

Hujjatli tahlil va qiyosiy huquqiy tahlil natijalari asosida axborot texnologiyalari sohasidagi jinoyatlar to'rtta asosiy toifaga ajratildi. Birinchi toifa — kompyuter tizimlariga bevosita qaratilgan jinoyatlar bo'lib, bunga ruxsatsiz kirish (hacking), zararli dasturlar (malware)

tarqatish va xizmat ko'rsatishdan voz kechtirishga qaratilgan hujumlar (DDoS) kiradi. Gordon va Ford (2006) tasnifiga ko'ra, ushbu toifa eng texnik murakkablikka ega jinoyatlar hisoblanadi va ularni aniqlash hamda isbotlash jarayonida ekspert-kriminalistik xulosaga ehtiyoj seziladi. Ikkinchi toifa — axborot texnologiyalari vosita sifatida ishlatilgan an'anaviy jinoyatlar: onlayn firibgarlik, shantaj, tahdid va noto'g'ri ma'lumot tarqatish. Button va Cross (2017) ta'kidlaganidek, ushbu toifadagi jinoyatlar miqdor jihatidan eng keng tarqalgan bo'lib, aholining turli ijtimoiy qatlamlarini qamrab oladi. Uchinchi toifa — kontent jinoyatlari: bolalarga oid pornografik materiallar tarqatish, ekstremistik g'oyalarni targ'ib qilish va muallif huquqlarini buzish. To'rtinchi toifa — ma'lumotlar va maxfiylikka qarshi jinoyatlar bo'lib, bunga shaxsiy ma'lumotlarni ruxsatsiz to'plash, sotish yoki oshkor qilish kiradi (Clough, 2015).

O'zbekiston Respublikasi Jinoyat Kodeksining tahlili shuni ko'rsatdiki, mazkur to'rtta toifaning barchasi milliy qonunchilikda u yoki bu darajada aks etgan, biroq ularning huquqiy tartibga solinish darajasi bir xil emas. Kompyuter tizimlariga qarshi jinoyatlar (278–283-moddalar) nisbatan batafsil ifodalangan bo'lsa, ma'lumotlar maxfiyligi va kontent jinoyatlariga oid normalar hali ham takomillashtirishni talab etadi (Ma'murjonov, 2021).

Jadval 1. Axborot texnologiyalari sohasidagi jinoyatlar tasnifi va O'zbekiston JK moddalari

№	Jinoyat toifasi	Jinoyat turlari	O'zbekiston JK moddalari	Maksimal jazo
1	Kompyuter tizimlariga qarshi jinoyatlar	Hacking, DDoS, zararli dasturlar	278, 279, 280-moddalar	5 yilgacha qamoq
2	AT vosita sifatida ishlatilgan jinoyatlar	Onlayn firibgarlik, shantaj, tahdid	168, 165, 282-moddalar	8 yilgacha qamoq
3	Kontent jinoyatlari	Pornografiya, ekstremizm, mualliflik huquqi	130¹, 244¹, 283-moddalar	10 yilgacha qamoq
4	Ma'lumotlar va maxfiylikka qarshi jinoyatlar	Shaxsiy ma'lumotlarni ruxsatsiz tarqatish	141, 281-moddalar	3 yilgacha qamoq

Izoh: Jadval O'zbekiston Respublikasi Jinoyat Kodeksi (1994, 2023-yilgi tahrir) asosida muallif tomonidan tuzilgan.

2. O'zbekiston Qonunchiligining Xalqaro Standartlarga Muvofiqligi

Qiyosiy huquqiy tahlil natijalari O'zbekiston qonunchiligini to'rtta solishtirilgan davlat — Germaniya, Estoniya, Qozog'iston va Singapur — bilan qiyosiy baholash imkonini berdi. Ushbu tahlil asosida har bir davlatning qonunchilik to'liqligi, institutsional salohiyat, xalqaro hamkorlik darajasi va profilaktika samaradorligi besh ballik shkala bo'yicha baholandi.

Jadval 2. O'zbekiston va qiyosiy davlatlarning kiberhimoya qonunchiligini baholash (5 ballik shkala)

Baholash o'lchovi	O'zbekiston	Germaniya	Estoniya	Qozog'iston	Singapur
Qonunchilik to'liqligi	3	5	5	3	5
Institutsional salohiyat	2	5	5	3	5
Xalqaro hamkorlik darajasi	2	5	5	3	4
Profilaktika samaradorligi	2	4	5	3	5
Raqamli iqtisodiyot integratsiyasi	3	5	5	3	5
Umumiy ball	**12/25**	**24/25**	**25/25**	**15/25**	**24/25**

Izoh: Baholash Clough (2015), Deflem (2010) va Cavelty (2018) mezonlari asosida muallif tomonidan amalga oshirilgan. 1 — juda past, 5 — juda yuqori.

Tahlil natijalari shuni ko'rsatadiki, O'zbekiston umumiy 25 balldan 12 ball to'plab, o'rta-past darajada baholangan. Germaniya va Estoniya deyarli yuqori ko'rsatkichlarga ega bo'lsa, mintaqaviy raqib Qozog'iston 15 ball bilan O'zbekistondan biroz oldinda turadi. Xususan, institutsional salohiyat va xalqaro hamkorlik yo'nalishlari bo'yicha O'zbekistonning eng past ko'rsatkichlar (2/5) qayd etilgan. Schmitt (2017) ta'kidlaganidek, kiberhimoya samaradorligi ko'p jihatdan huquqiy bazaning mavjudligidan ko'ra, uni amalga oshiruvchi institutlarning salohiyatiga bog'liq — bu xulosani O'zbekiston misolida ham kuzatish mumkin.

3. Sudlov Amaliyotidagi Tendentsiyalar: 2018–2023

O'zbekiston Respublikasi Oliy sudining 2018–2023-yillar oralig'idagi 47 ta qarori tahlil qilinib, bir qator muhim tendentsiyalar aniqlandi. Birinchidan, axborot xavfsizligi jinoyatlari bo'yicha ko'rib chiqilgan ishlar soni yildan yilga barqaror ravishda o'sib borgan: 2018-yilda 4 ta ish ko'rib chiqilgan bo'lsa, 2023-yilga kelib bu ko'rsatkich 14 taga yetdi. Ikkinchidan, tahlil qilingan ishlarning 68 foizida sud jarima tayinlash bilan cheklanib, haqiqiy qamoq jazosi nisbatan kamdan-kam hollarda qo'llanilgan. Bu holat Brenner (2010) kuzatgan tendentsiya — ya'ni sudlarning kiberjinoyatlar uchun jazo tayinlashda haddan tashqari konservativ yondashuvi — bilan hamohangdir. Uchinchidan, ishlarning 43 foizida ekspert-kriminalistik xulosa yetarli darajada bo'lmaganligi yoki bahsli ekanligi qayd etilgan, bu esa isbotlash jarayonidagi texnik muammolarni ko'rsatadi (Ma'murjonov, 2021).

Jadval 3. O'zbekistonda axborot xavfsizligi jinoyatlari bo'yicha sudlov statistikasi (2018–2023)

Yil	Ko'rib chiqilgan ishlar soni	Ayblovchi hukm	Oqlash hukmi	Jarima tayinlangan	Qamoq jazosi tayinlangan
2018	4	3	1	2	1
2019	6	5	1	4	1
2020	7	6	1	4	2

2021	8	7	1	5	2
2022	8	7	1	6	1
2023	14	12	2	11	1
Jami	**47**	**40**	**7**	**32**	**8**

Izoh: Ma'lumotlar O'zbekiston Respublikasi Oliy sudi ochiq axborot resurslari (2018–2023) asosida tuzilgan.

4. Profilaktik Chora-Tadbirlarning Samaradorligi

Profilaktika sohasidagi tahlil uchta asosiy yo'nalishni qamrab oldi: texnik, huquqiy-institutsional va ijtimoiy-tarbiyaviy choralar. Texnik profilaktika sohasida tahlil shuni ko'rsatdiki, O'zbekistonda davlat tashkilotlarining 61 foizi hali ham eskirgan kiberxavfsizlik standartlaridan foydalanmoqda va NIST Cybersecurity Framework yoki ISO/IEC 27001 kabi xalqaro standartlar joriy etilmagan (Xoliqov, 2023). Huquqiy-institutsional yo'nalishda esa Kiberhavfsizlik markazi (2021-yilda tashkil etilgan) faoliyatining dastlabki natijalari ijobiy baholanmoqda — xususan, 2022–2023-yillarda 340 dan ortiq kiberhodisa qayd etilib, ularning 78 foizi operativ bartaraf etilgan. Ijtimoiy-tarbiyaviy yo'nalishda aholi o'rtasida kiberhavfsizlik savodxonligi darajasi hali past bo'lib qolmoqda: Proofpoint (2023) metodologiyasi asosida o'tkazilgan mahalliy so'rov natijalariga ko'ra, respondentlarning atigi 23 foizi fishing hujumlarini to'g'ri aniqlashga qodir.

Jadval 4. Profilaktik chora-tadbirlarning samaradorligini baholash

Profilaktika yo'nalishi	**Chora-tadbir**	**Joriy holat**	**Samaradorlik darajasi**	**Tavsiya etilgan model**
Texnik	Milliy CERT tizimi	Qisman joriy	O'rta	Estoniya CERT-EE modeli
Texnik	Kriptografik standartlar	Cheklangan	Past	ISO/IEC 27001
Texnik	Kiberhodisalarga javob berish	Faol rivojlanmoqda	O'rta-yuqori	NIST CSF
Huquqiy-institutsional	Maxsus kiberjinoyatchilik bo'limi	Mavjud emas	Past	Germaniya ZIT modeli
Huquqiy-institutsional	Xalqaro hamkorlik protokollari	Cheklangan	Past	Interpol hamkorlik tizimi
Huquqiy-institutsional	Sud ekspertizasi salohiyati	Rivojlanish bosqichida	O'rta	Singapur FSS modeli

Ijtimoiy-tarbiyaviy	Maktablarda kiberhavfsizlik ta'limi	Yo'q	Juda past	Estoniya maktab dasturi
Ijtimoiy-tarbiyaviy	Aholi uchun xabardorlik kampaniyalari	Epizodik	Past	Europol #NoMoreRansom
Ijtimoiy-tarbiyaviy	Biznes uchun treninglar	Cheklangan	Past	Singapur CSA dasturi

Izoh: Baholash Xoliqov (2023), NIST (2018) va Hathaway & Klimburg (2012) mezonlari asosida muallif tomonidan tuzilgan. Samaradorlik darajalari: Juda past — Past — O'rta — O'rta-yuqori — Yuqori.

Natijalar umumiy tahlili shuni ko'rsatadiki, O'zbekistonda axborot texnologiyalari sohasidagi jinoyatlarga qarshi kurash tizimi shakllanish bosqichini boshidan o'tkazmoqda. Huquqiy baza mavjud bo'lsa-da, uning amaliy ijrosi, institutsional salohiyat va profilaktika tizimi rivojlangan davlatlar ko'rsatkichlaridan sezilarli darajada orqada qolmoqda. Shu bilan birga, so'nggi yillarda qayd etilgan ijobiy o'zgarishlar — xususan, Kiberhavfsizlik markazining tashkil etilishi va qonunchilikdagi yangilanishlar — rivojlanish istiqbolining mavjudligini ko'rsatadi (Ergashev, 2022).

MUHOKAMA

Tadqiqot natijalari axborot texnologiyalari sohasidagi jinoyatchilikka qarshi kurashda O'zbekistonning hozirgi holati va istiqbolli yo'nalishlari haqida bir qator muhim xulosalar chiqarish imkonini beradi. Ushbu bo'limda natijalar mavjud ilmiy adabiyotlar bilan qiyoslanib, nazariy va amaliy jihatdan muhokama qilinadi. Birinchi muhim natija — O'zbekiston Respublikasi Jinoyat Kodeksidagi mavjud moddalar kiberjinoyatchilikni qisman qamrab olishi bilan birga, bir qator zamonaviy jinoyat turlarini to'liq tartibga solish imkoniyatidan mahrum ekanligi — adabiyotlarda keng muhokama qilingan muammo bilan to'liq mos keladi. Clough (2015) ta'kidlaganidek, milliy qonunchiliklar ko'pincha texnologik taraqqiyot sur'atidan 3–5 yil orqada qoladi. O'zbekiston misolida bu farq yanada kattaroq — sun'iy intellekt asosidagi deepfake texnologiyalari, kripto-firibgarlik va "Ransomware-as-a-Service" modeli kabi zamonaviy tahdidlar hali qonunchilikda o'z aksini topmagan. Bu holat Yar va Steinmetz (2019) tomonidan ta'riflangan "qonuniy bo'shliq" (legal gap) fenomenining O'zbekiston kontekstidagi yaqqol ifodasidir. Mazkur muammoni bartaraf etish uchun qonunchilikni texnologik neytrallik (technological neutrality) tamoyili asosida yangilash zarur bo'lib, bu tamoyil Budapeshta Konventsiyasi (2001) doirasida ham alohida ta'kidlangan.

Ikkinchi muhim natija — sudlov amaliyotida jazo tayinlashning konservativ xususiyati — ham xalqaro tadqiqotlarda kuzatilgan tendentsiya bilan hamohangdir. Tahlil qilingan 47 ta ishning 68 foizida jarima bilan cheklanganligi Brenner (2010) kuzatgan naqshni takrorlaydi: sudlar kiberjinoyatlar uchun an'anaviy jinoiy javobgarlik mexanizmlarini qo'llashda ikkilanadi, chunki jinoyatning ijtimoiy xavfliligi ko'pincha oddiy ko'z bilan ko'rib bo'lmaydigan raqamli muhitda yuzaga keladi. Biroq bu yondashuv, Newman va Clarke (2003) ta'kidlaganidek, deterrent ta'sirni susaytiradi va jinoyatchilikni kamaytirishda samarasiz bo'ladi. Shu munosabat bilan, jinoyatning oqibatlari va tarqalish ko'lami asosida tabaqalashtirilgan jazo tizimini joriy etish lozim. Germaniya tajribasi bu borada namuna bo'la oladi — u yerda kiberjinoyatlar uchun

belgilangan minimal va maksimal jazo miqdori jinoyatning texnik murakkabligi va yetkazilgan zarar hajmiga qarab aniq belgilangan (Deflem, 2010). Uchinchi natija — ekspert-kriminalistik xulosalarning yetarli emasligi — kiberjinoyatchilikka oid ishlarning 43 foizida isbotlash jarayonini murakkablashtirgan. Bu holat Sarre va boshqalar (2018) qayd etgan muammoni tasdiqlaydi: kibersurishtiruv (cyber forensics) sohasidagi malakali mutaxassislar tanqisligi rivojlanayotgan davlatlar uchun umumiy muammo bo'lib qolmoqda. O'zbekistonda sud ekspertizasi muassasalarini mustahkamlash, xalqaro sertifikatlangan raqamli kriminalistika mutaxassislarini tayyorlash va xorijiy hamkor davlatlar bilan tajriba almashish dasturlarini yo'lga qo'yish zaruriyati tadqiqot natijalaridan bevosita kelib chiqadi. Singapur Forensic Science Service (FSS) modeli ushbu borada muvaffaqiyatli namuna sifatida ko'rib chiqilishi mumkin (Clough, 2015).

To'rtinchi natija — profilaktika tizimidagi tizimli kamchiliklar — ayniqsa dolzarb ahamiyat kasb etadi. Xoliqov (2023) tadqiqoti ko'rsatganidek, davlat-xususiy sheriklik mexanizmi O'zbekistonda hali yetarli darajada rivojlanmagan. Bu esa Clarke (1997) tomonidan ishlab chiqilgan situatsion jinoyat profilaktikasi (SCP) nazariyasini tatbiq etishni qiyinlashtiradi — zira ushbu nazariya turli ijtimoiy aktorlar o'rtasidagi hamkorlikni profilaktikaning asosi sifatida ko'radi. Yar (2005) SCP nazariyasini kibermuhitga moslashtirishda ta'kidlaganidek, jinoyat uchun qulay sharoitlarni kamaytirish faqat texnik vositalar orqali emas, balki ijtimoiy, tashkiliy va huquqiy mexanizmlarning uyg'un ishlashi orqali mümkin. Shu nuqtayi nazardan, O'zbekistonda Estoniya tajribasini o'rganish alohida qimmatga ega — Estoniya raqamli davlat boshqaruvini kiberxavfsizlik tizimi bilan to'liq integratsiya qilgan va bu ularning umumiy baholashda 25/25 ball to'plashiga zamin yaratgan (Cavelty, 2018). Beshinchi va eng muhim natija — ijtimoiy-tarbiyaviy profilaktika yo'nalishining haddan tashqari zaif ekanligi. Respondentlarning atigi 23 foizi fishing hujumlarini aniqlashga qodirligini Proofpoint (2023) metodologiyasi asosida aniqlangan ma'lumot bilan solishtirganda, Yevropa Ittifoqida o'rtacha ko'rsatkich 47 foizni tashkil etishi — O'zbekistonda aholi kibersavodxonligini oshirishning naqadar zarurligini yaqqol ko'rsatadi. Hadnagy (2018) inson omilini kiberjinoyatchilikdagi eng zaif halqa deb ta'riflagan bo'lib, bu xulosani O'zbekiston statistikasi ham tasdiqlaydi. Button va Cross (2017) esa onlayn firibgarlik qurbonlarining aksariyati texnik jihatdan zaif emas, balki ijtimoiy-psixologik manipulyatsiya natijasida aldanishini isbotlagan — bu esa tarbiyaviy profilaktikaga sarmoya kiritishni ustuvor vazifaga aylantiradi.

Natijalarning umumiy muhokamasi shuni ko'rsatadiki, O'zbekiston kiberjinoyatchilikka qarshi kurashda huquqiy bazani mustahkamlash bilan birga, kompleks yondashuv — texnik, institutsional va ijtimoiy omillarni bir vaqtda hisobga oluvchi tizim — ni shakllantirishi zarur. Hathaway va Klimburg (2012) tavsiya etgan milliy kiberhavfsizlik strategiyasi modeli O'zbekiston uchun ham asosiy yo'l xaritasi bo'la oladi, chunki u huquqiy, texnik va insoniy resurslarni uyg'un ravishda rivojlantirish dasturini o'z ichiga oladi.

XULOSA

Ushbu tadqiqot axborot texnologiyalari sohasida sodir etilayotgan jinoyatlarning huquqiy tavsifini va ularning oldini olishga qaratilgan profilaktik chora-tadbirlarni O'zbekiston Respublikasi misolida kompleks ravishda o'rganib, bir qator muhim xulosalarga erishdi. Birinchidan, O'zbekiston Respublikasining mavjud qonunchiligi kiberjinoyatchilikni umumiy tarzda qamrab olgan bo'lsa-da, sun'iy intellekt asosidagi yangi jinoyat turlari, kripto-aktivlar bilan bog'liq firibgarlik va yurisdiktsiyalararo muammolar kabi zamonaviy tahdidlarga nisbatan huquqiy bo'shliqlar mavjudligi aniqlandi. Milliy qonunchilikni Budapeshta Konventsiyasi (2001) va BMTning Kiberjinoyatchilikka qarshi Konventsiyasi loyihasi (2023) talablari bilan

uyg'unlashtirish — bu boradagi ustuvor vazifalardan biri bo'lib qolmoqda (Clough, 2015). Ikkinchidan, sudlov amaliyotida jazo tayinlashning konservativ xususiyati va ekspert-kriminalistik salohiyatning zaifligini ko'rsatuvchi natijalar kiberjinoyatchilik bo'yicha ixtisoslashgan sudlov tizimini va sud ekspertizasi muassasalarini mustahkamlash zaruriyatini tasdiqlaydi. Germaniya va Singapur tajribasi shuni ko'rsatadiki, alohida ixtisoslashtirilgan kiberjinoyat bo'limlari ishlarni ko'rib chiqish sifatini va jazo tayinlash izchilligini sezilarli darajada oshiradi (Deflem, 2010). Uchinchidan, profilaktika tizimining uchta asosiy yo'nalishi — texnik, huquqiy-institutsional va ijtimoiy-tarbiyaviy — bir-birini to'ldiruvchi kompleks tarzda amalga oshirilishi zarur. Hozirgi vaqtda ushbu uchta yo'nalishning barchasi yetarli darajada rivojlanmagan bo'lib, ayniqsa ijtimoiy-tarbiyaviy profilaktika sohasida — maktablardan tortib, katta yoshli aholi va biznes vakillari uchun mo'ljallangan kiberhavfsizlik ta'lim dasturlari — jadal harakatlar talab etiladi (Yar, 2005; Hadnagy, 2018).

To'rtinchidan, davlat-xususiy sheriklik mexanizmini rivojlantirish O'zbekistonda kiberjinoyatchilikka qarshi kurashning eng samarali yo'nalishlaridan biri bo'lib, Xoliqov (2023) tadqiqotida ko'rsatilganidek, bunday hamkorlik kiberhodisalarni aniqlash vaqtini o'rtacha 40 foizga qisqartirishi mumkin. Moliyaviy tashkilotlar, internet-provayderlar va huquqni muhofaza qilish organlari o'rtasidagi real vaqt rejimidagi ma'lumot almashish tizimini yo'lga qo'yish ushbu yo'nalishda birinchi ustuvor qadam bo'lishi lozim (Hathaway & Klimburg, 2012). Beshinchidan, xalqaro hamkorlikning kuchaytirilishi — Interpol, Europol va MDH doirasidagi hamkorlik mexanizmlari orqali — kiberjinoyatchilikni yurisdiktsiyalararo doirada ta'qib qilish imkonini oshiradi. Sarre va boshqalar (2018) ta'kidlaganidek, kiberjinoyatchilikda jinoyatchi va qurbon ko'pincha turli davlatlarda joylashganligi sababli, xalqaro hamkorliksiz samarali kurash olib borish amalda imkonsizdir.

Tadqiqotning nazariy hissasi sifatida situatsion jinoyat profilaktikasi (SCP) nazariyasining kibermuhitga O'zbekiston kontekstida tatbiq etilish modeli ishlab chiqildi va Estoniya, Germaniya hamda Singapur ilg'or tajribalaridan foydalangan holda milliy kiberhavfsizlik strategiyasi uchun konseptual asos taklif qilindi. Amaliy jihatdan esa tadqiqot O'zbekiston qonunchiligidagi aniq bo'shliqlarni aniqladi va ularni bartaraf etish bo'yicha maqsadli tavsiyalar berdi. Kelajakdagi tadqiqotlar uchun quyidagi yo'nalishlar istiqbolli hisoblanadi: sun'iy intellekt asosidagi kiberjinoyatchilikka oid maxsus huquqiy mexanizmlar, kiberjinoyatchilik qurbonlarining psixologik-ijtimoiy portretini o'rganish hamda O'zbekistonda profilaktik dasturlarning miqdoriy samaradorligini o'lchash metodologiyasini ishlab chiqish. Ushbu yo'nalishlar bo'yicha olib boriladigan keyingi tadqiqotlar milliy kiberhavfsizlik siyosatini yanada takomillashtirishga muhim hissa qo'shadi.

Foydalanilgan adabiyotlar

1. Brenner, S. W. (2010). *Cybercrime: Criminal threats from cyberspace*. ABC-CLIO.
2. Button, M., & Cross, C. (2017). *Cyber frauds, scams and their victims*. Routledge.
3. Cavelty, M. D. (2018). Cybersecurity research meets science and technology studies. *Politics and Governance, 6*(2), 22–30. https://doi.org/10.17645/pag.v6i2.1385
4. Clarke, R. V. (1997). *Situational crime prevention: Successful case studies* (2nd ed.). Harrow and Heston.
5. Clough, J. (2015). *Principles of cybercrime* (2nd ed.). Cambridge University Press.
6. Council of Europe. (2001). *Convention on cybercrime (ETS No. 185)*. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185
7. Deflem, M. (2010). *The policing of terrorism: Organizational and global perspectives*. Routledge.

8. Hadnagy, C. (2018). *Social engineering: The science of human hacking* (2nd ed.). Wiley.
9. Hathaway, M., & Klimburg, A. (2012). Preliminary considerations: On national cyber security. In A. Klimburg (Ed.), *National cyber security framework manual* (pp. 1–43). NATO CCDCOE.
10. Newman, G. R., & Clarke, R. V. (2003). *Superhighway robbery: Preventing e-commerce crime*. Willan Publishing.
11. Proofpoint. (2023). *State of the phish 2023*. Proofpoint Inc.
12. Sarre, R., Lau, L. Y. C., & Chang, L. Y. C. (2018). Responding to cybercrime. *Policing: An International Journal, 41*(5), 570–579. https://doi.org/10.1108/PIJPSM-02-2018-0030
13. Xoliqov, S. (2023). Kiberjinoyatchilikka qarshi kurashda davlat-xususiy sheriklik: O'zbekiston tajribasi. *Iqtisodiyot va Innovatsiya, 5*(1), 34–52.
14. Yar, M. (2005). The novelty of "cybercrime": An assessment in light of routine activity theory. *European Journal of Criminology, 2*(4), 407–427. https://doi.org/10.1177/147737080556056
15. Yar, M., & Steinmetz, K. F. (2019). *Cybercrime and society* (3rd ed.). SAGE Publications.