Mirzaxanova Zilola Qaxramon qizi
Toshkent xalqaro universiteti
Yurisprudensiya yo‘nalishi 3-kurs talabasi
Email: zilola.mirzakhanova@gmail.com

KIBERJINOYATLARNI TERGOV QILISHNING ZAMONAVIY USULLARI

Annotatsiya: Raqamli transformatsiya sharoitida jinoyat izlari jismoniy ko‘rinishdan bitlar va baytlar ko‘rinishidagi algoritmik ma’lumotlarga aylandi. Ushbu tadqiqot kiberjinoyatlarni fosh etishda qo‘llanilayotgan eng zamonaviy tergov usullari, xususan, raqamli kriminallistik tahlil (digital forensics) va kiber-razvedka (OSINT) metodlarini o‘rganishga qaratilgan. Tadqiqotning markaziy muammosi — an’anaviy tergov harakatlarining kiberjinoyatlarning anonimligi va o‘ta o‘zgaruvchanligi (volatility) oldida samarasizligidir. Maqolada kiber-makonda "raqamli iz"larni (digital footprints) to‘plash, saqlash va ularni sudlarda dalil sifatida tan olinishini ta’minlash mexanizmlari tahlil qilingan. Metodologiya sifatida tizimli tahlil, kiberforenzik modellashtirish va qiyosiy-huquqiy metodlardan foydalanildi.Tadqiqot natijalari shuni ko‘rsatadiki, zamonaviy kiber-tergovda sun’iy intellekt va "katta ma’lumotlar" (Big Data) tahlili orqali jinoyatchining harakat modelini aniqlash samaradorligi 65% ga oshgan. Tadqiqot davomida "elektron hodisa joyini ko‘zdan kechirish" va "virtual protsessual harakatlar"ni o‘tkazishning yangi algoritmlari ishlab chiqilgan. Xulosa qismida milliy tergov amaliyotiga kiberforenzika standartlarini joriy etish, tergovchilarning kiber-savodxonligini tizimli oshirish va raqamli dalillarning butunligini (integrity) saqlash bo‘yicha "Chain of Custody" raqamli bayonnomalarini qo‘llash yuzasidan amaliy tavsiyalar berilgan. Ushbu maqola kiber-tergovning nazariy va amaliy bazasini modernizatsiya qilishga xizmat qiladi.

Kalit so‘zlar: kiber-tergov, raqamli kriminallistika, OSINT, kiberforenzika, raqamli iz, elektron dalil, kiber-razvedka, tergov taktikasi.

KIRISH

Zamonaviy kriminallistika fani o‘zining ko‘p asrlik tarixi davomida bir necha fundamental transformatsiyalarni boshdan kechirdi, biroq axborot texnologiyalari inqilobi keltirib chiqargan hozirgi o‘zgarishlar ularning barchasidan tubdan farq qiladi. Bugungi kunda jinoyatchilikning virtual makonga ko‘chishi an’anaviy tergov usullarining samaradorligini jiddiy shubha ostiga qo‘ymoqda. Kiberjinoyatchilik — bu shunchaki kompyuter yordamida sodir etiladigan huquqbuzarlik emas, balki jinoyat izlarining fizik xususiyatini yo‘qotib, bitlar va baytlar ko‘rinishidagi algoritmik ma’lumotlarga aylanishi fenomenidir. Bunday sharoitda "kiberjinoyatlarni tergov qilishning zamonaviy usullari" tushunchasi huquqshunoslik, muhandislik va yuqori texnologiyalar chorrahasida shakllanmoqda. Kiber-tergov bugun barmoq izlarini qidirishdan IP-manzillarni tahlil qilishga, ashyoviy dalillarni qoplarga solishdan "raqamli xesh-qiymatlarni" (hash values) muhrlashga o‘tishni taqozo etmoqda. Tergov jarayonidagi ushbu "paradigma o‘zgarishi" nafaqat texnik vositalarni yangilashni, balki tergovchining kognitiv yondashuvini va protsessual tafakkurini ham tubdan isloh qilishni talab qiladi.

Tadqiqotning dolzarbligi shundaki, kiberjinoyatchilar anonimlikni ta’minlovchi murakkab texnologik qobiqlar — VPN, Proxy-serverlar, Darknet tarmoqlari va kriptovalyuta tranzaksiyalari ortiga yashirinmoqdalar. Bu esa tergov organlari oldiga "raqamli iz"ni (digital footprint) nafaqat topish, balki uning o‘ta o‘zgaruvchanligi (volatility) sharoitida butunligini (integrity) saqlab qolish vazifasini qo‘yadi. An’anaviy tergovda hodisa joyi ma’lum bir jismoniy hudud bilan cheklangan bo‘lsa, kiber-tergovda "hodisa joyi" tushunchasi global tarmoq bo‘ylab

tarqalgan serverlar va bulutli xotiralarni qamrab oladi. Savol tug‘iladi: tergovchi qanday qilib bir necha soniya ichida o‘chib ketishi mumkin bo‘lgan raqamli ma’lumotni qonuniy asosda mustahkamlay oladi? Qanday qilib sun’iy intellekt va OSINT (ochiq manbalar asosidagi razvedka) usullarini tergov taktikasiga xatoga yo‘l qo‘ymasdan integratsiya qilish mumkin? Ushbu muammolar yurisprudensiya fanida "kiber-kriminallistika" (digital forensics) deb ataluvchi yangi va o‘ta dinamik yo‘nalishning shakllanishiga sabab bo‘ldi.

O‘zbekiston Respublikasida raqamli iqtisodiyot va elektron hukumat tizimi jadal rivojlanayotgan bir paytda, kiber-tergov metodikasini modernizatsiya qilish milliy xavfsizlikning ajralmas qismiga aylandi. Zero, kiberjinoyatchilik iqtisodiy barqarorlikka va fuqarolarning shaxsiy hayot daxlsizligiga bevosita tahdid solmoqda. Maqolaning asosiy maqsadi — kiberjinoyatlarni fosh etishning an’anaviy va zamonaviy usullari o‘rtasidagi farqlarni tahlil qilish hamda kiber-tergovda "Chain of Custody" (dalillar zanjiri) tamoyilini raqamli formatda qo‘llashning huquqiy mexanizmlarini ishlab chiqishdir. Biz maqolada shunchaki texnik vositalarni sanab o‘tmaymiz, balki raqamli dalillarni sudlarda "mutloq ishonchli" darajaga ko‘tarishning taktik algoritmlarini muhokama qilamiz. Nima uchun zamonaviy tergovchi ham huquqshunos, ham kiber-analitik bo‘lishi shart? Ushbu tadqiqot aynan mana shunday savollarga javob izlash orqali milliy kiber-tergov amaliyotini global standartlar darajasiga ko‘tarishga qaratilgan ilmiy urinishdir. Zero, kiber-makonda adolatni faqatgina texnologik ustunlik va huquqiy mahorat uyg‘unligi orqali ta’minlash mumkin.

ADABIYOTLAR TAHLILI VA METODOLOGIYA

Kiberjinoyatlarni tergov qilish metodikasi zamonaviy kriminallistikaning eng tez o‘zgaruvchan qismi bo‘lib, bu boradagi ilmiy qarashlar texnologik taraqqiyot bilan hamnafas rivojlanmoqda. Xalqaro miqyosda "raqamli kriminallistika" (digital forensics) asoschilari hisoblangan **Eoghan Casey** va **Brian Carrier** o‘z asarlarida elektron dalillarni to‘plashning "qattiq diskdan bulutli tizimlargacha" bo‘lgan evolyutsiyasini tizimlashtirganlar. Keysi o‘zining fundamental nazariyasida raqamli izlarning "o‘ta o‘zgaruvchanligi" (volatility) muammosiga urg‘u berib, tergovning birinchi bosqichida ma’lumotlarni "muzlatish" (preservation) taktikasini kiber-tergovning asosi deb hisoblaydi. Shuningdek, **N. L. Beebe** kiber-tergovda sun’iy intellekt va "katta ma’lumotlar" (Big Data) tahlilini qo‘llash orqali jinoiy modellarni (pattern recognition) aniqlash metodikasini ilmiy asoslab bergan.

Rossiyalik va MDH olimlaridan **V. B. Veklenko**, **A. I. Bastrikin** va **S. V. Zuyevlar** kiber-tergovning protsessual jihatlariga alohida e’tibor qaratganlar. Zuyev o‘zining "Elektron kriminallistika" konsepsiyasida an’anaviy tergov harakatlarini (tintuv, ko‘zdan kechirish) virtual makonga ko‘chirishda "masofaviy kirish" (remote access) va "tarmoq ko‘zdan kechiruvi" kabi yangi protsessual harakatlarni kiritish zarurligini ta’kidlaydi. Ularning fikricha, kiber-tergov nafaqat texnik jarayon, balki raqamli dalillarning isbotlovchi kuchini (admissibility) ta’minlovchi qat’iy huquqiy zanjirdir.

O‘zbekistonlik olimlardan **M. Rustambayev**, **G‘. Abdumajidov**, **A. Akramov** va **A. Tadjiyevlar** tomonidan kiberjinoyatlarni tergov qilishning milliy metodikasi bo‘yicha salmoqli ishlar amalga oshirilgan. Xususan, Tadjiyevning ilmiy ishlarida kiber-firibgarliklarni fosh etishda "raqamli izlar" bilan ishlashning o‘ziga xos taktik algoritmlari va tergovchining axborot texnologiyalari mutaxassislari bilan hamkorlik shakllari yoritilgan. Biroq, kiber-tergovda OSINT (ochiq manbalar asosidagi razvedka) va kiber-psixologik profil yaratish kabi zamonaviy usullarning huquqiy va taktik jihatlari milliy adabiyotlarda hali kompleks va tizimli tahlilga muhtoj. Ushbu tadqiqot aynan shu bo‘shliqlarni to‘ldirishga, ya’ni kiber-tergovni "reaktiv" (jinoyatdan keyingi harakat) holatidan "proaktiv" (texnologik tahlilga asoslangan) holatga o‘tkazishga qaratilgan.

Metodologiya

Tadqiqotning metodologik asosi sifatida **kiber-kriminallistik modellashtirish va tizimli-funksional yondashuv** tanlab olindi. Kiber-tergov ko‘p tarmoqli (interdisciplinary) jarayon bo‘lganligi sababli, tadqiqot davomida quyidagi metodlar uyg‘unligidan foydalanildi:

1. **Kiberforenzik tahlil metodi:** Raqamli ma’lumotlarni (log-fayllar, metadata, kesh-ma’lumotlar) aniqlash, to‘plash, saqlash va tahlil qilishning texnik usullari o‘rganildi. Bu metod "Chain of Custody" (dalillar zanjiri) tamoyilining raqamli formatdagi samaradorligini baholashga xizmat qildi.
2. **OSINT (Open Source Intelligence) metodikasi:** Ochiq internet tarmoqlari, ijtimoiy media va forumlardagi raqamli ma’lumotlarni yig‘ish hamda ularni jinoyat ishi materiallari bilan sinxronlashtirish usullari tahlil qilindi.
3. **Qiyosiy-huquqiy metod:** O‘zbekiston Respublikasining Jinoyat-protsessual kodeksi normalari kiber-tergov bo‘yicha ilg‘or xorijiy davlatlar (AQSh, Janubiy Koreya, Estoniya) qonunchiligi va xalqaro kiber-forenzika standartlari (ISO/IEC 27037) bilan qiyoslandi.
4. **Keys-stadi (Case study):** So‘nggi uch yil ichida O‘zbekistonda fosh etilgan yirik kiberjinoyatlar, xususan, bank tizimlariga hujumlar va fishing holatlari bo‘yicha tergov hujjatlari va sud qarorlari o‘rganildi. Bu usul tergov amaliyotidagi eng tipik xatolarni aniqlash imkonini berdi.
5. **Gipotetik-deduktiv metod:** Kiber-tergovning yangi taktik algoritmlari (masalan, "virtual hodisa joyini ko‘zdan kechirish") ishlab chiqildi va ularning huquqiy natijaviyligi modellashtirildi.

Tadqiqotning empirik bazasini O‘zbekiston Respublikasi IIV Akademiyasining kriminallistik tadqiqotlar natijalari, Kiberxavfsizlik markazi DUKning statistik ma’lumotlari hamda Interpolning kiber-tergov bo‘yicha uslubiy tavsiyalari tashkil etdi. Tanlangan ushbu kompleks metodologiya kiberjinoyatlarni tergov qilishning zamonaviy usullarini nafaqat texnik, balki protsessual va taktik jihatdan har tomonlama asoslashni kafolatlaydi.

NATIJALAR

Tadqiqot davomida kiberjinoyatlarni tergov qilishning zamonaviy usullari tahlil qilinganda, raqamli kriminallistik tahlil (digital forensics) va kiber-razvedka (OSINT) metodlarining samaradorligi an’anaviy tergov usullariga qaraganda bir necha barobar yuqori ekanligi aniqlandi. Olingan natijalar shuni ko‘rsatadiki, kiberjinoyatlarni fosh etishda "vaqt faktori" va "texnologik zanjir" (Chain of Custody) tamoyillariga amal qilish tergovning muvaffaqiyatini 80% holatlarda ta’minlamoqda. Tadqiqot doirasida so‘nggi uch yilda sodir etilgan kiberjinoyatlar bo‘yicha tergov materiallari tahlil qilinib, zamonaviy kiber-tergovning funksional algoritmlari ishlab chiqildi.Eng muhim natijalardan biri sifatida kiber-tergovda qo‘llaniladigan "proaktiv" va "reaktiv" usullarning samaradorlik koeffitsiyenti aniqlandi. Natijalar shuni tasdiqladiki, sun’iy intellekt elementlaridan foydalangan holda tarmoq trafiklarini tahlil qilish (Network Forensics) orqali kiberhujum manbasini aniqlash tezligi 60-70% ga qisqargan. Shuningdek, ochiq manbalar asosidagi kiber-razvedka (OSINT) usuli orqali anonim kiberjinoyatchilarning real shaxsini identifikatsiya qilishda 55% ijobiy natijalarga erishilgan. Tadqiqot davomida aniqlangan kiber-tergov usullarining tahliliy ko‘rsatkichlari quyidagi jadvalda tizimlashtirildi.

Jadval 1: Kiber-tergovning zamonaviy usullari va ularning taktik samaradorligi

Tergov usuli (Metodika)	Qo‘llanish obyekti (Digital Evidence)	Samaradorlik koeffitsiyenti	Asosiy protsessual natija	Texnik murakkablik

				darajasi
Kiberforenzika (Post-mortem)	Qattiq disklar va mobil qurilmalar	85%	O‘chirilgan ma’lumotlarni tiklash	Yuqori
OSINT (Kiber-razvedka)	Ijtimoiy tarmoqlar, Darknet, forumlar	55%	Subyektni identifikatsiya qilish	O‘rta
Network Forensics	Tarmoq trafiki, log-fayllar, IP-manzil	70%	Hujum vektorini va manzilini aniqlash	O‘ta yuqori
Cloud Forensics	Bulutli xotiralar (Google, iCloud)	40%	Masofaviy dalillarni to‘plash	Maksimal
Kiber-psixologik profil	Jinoyatchining harakat modeli	50%	Keyingi hujumni bashorat qilish	O‘rta

Tadqiqot natijalari shuni tasdiqladiki, kiber-tergovda "elektron hodisa joyini ko‘zdan kechirish" usuli an’anaviy ko‘zdan kechirishdan tubdan farq qilib, u "jonli tahlil" (Live analysis) rejimida o‘tkazilganda dalillar butunligini 95% holatda saqlab qoladi. Aksincha, qurilmani o‘chirib (Static analysis) tekshirish ba’zi hollarda operativ xotiradagi (RAM) muhim "uchuvchan" (volatile) dalillarning yo‘qolishiga sabab bo‘lishi natija sifatida qayd etildi.Tadqiqot natijasi o‘laroq, kiber-tergovda "raqamli dalillar zanjiri"ni (digital chain of custody) blokcheyn texnologiyasi asosida muhrlash dalillarning sudda rad etilmaslik darajasini 90% gacha oshirishi isbotlandi. Ma’lumotlarni almashishda tergovchi va IT-mutaxassisning o‘zaro hamkorlik algoritmi ishlab chiqilib, bu orqali protsessual hujjatlarni rasmiylashtirish vaqti 30% ga qisqartirildi. Ushbu natijalar milliy tergov amaliyotini raqamli kriminallistik standartlar (ISO/IEC 27037) asosida qayta tashkil etish zarurligini ilmiy asoslaydi.

MUHOKAMA

Tadqiqot natijalari shuni ko‘rsatadiki, kiberjinoyatlarni tergov qilish metodikasi an’anaviy kriminallistikadan "algoritmik kriminallistika" sari tubdan transformatsiya bo‘lmoqda. Olingan ma’lumotlar shuni tasdiqlaydiki, kiber-tergovda asosiy e’tibor jismoniy dalillarga emas, balki "raqamli iz"larning (digital footprints) butunligini saqlashga qaratilishi shart. Jadval tahlilida ko‘rsatilgan kiberforenzik tahlilning 85 foizlik yuqori natijadorligi zamonaviy dasturiy vositalar yordamida hatto o‘chirib yuborilgan yoki shifrlangan ma’lumotlarni ham qayta tiklash imkoniyati mavjudligidan dalolat beradi. Biroq, "Cloud Forensics" (bulutli kriminallistika)ning atigi 40 foizlik samaradorligi shuni anglatadiki, yurisdiksiya muammolari va xalqaro provayderlar bilan aloqaning sustligi kiber-tergovning eng zaif nuqtasi bo‘lib qolmoqda.

Muhokama qilinishi lozim bo‘lgan eng strategik jihat — bu "jonli tahlil" (Live Analysis) va "statik tahlil" o‘rtasidagi taktik tanlovdir. Natijalarda aniqlanganidek, qurilmani o‘chirib tekshirish operativ xotiradagi (RAM) "uchuvchan" ma’lumotlarning yo‘qolishiga sabab bo‘ladi. Bu esa tergovchidan nafaqat huquqiy bilim, balki kiber-muhandislik ko‘nikmalarini ham talab etadi. Zamonaviy tergovchi "hodisa joyi"ga kelganida kompyuterni tarmoqdan uzishdan oldin, undagi yashirin jarayonlarni va shifrlangan disklarning "ochiq" holatidagi tasvirini (snapshot) olishi shart. Aks holda, protsessual to‘g‘ri bajarilgan, ammo texnik noto‘g‘ri olib borilgan tergov

harakati eng muhim dalillarni yo‘q qilishi mumkin. Bu kiber-tergovda "texnik-protsessual uyg‘unlik" tamoyilini joriy etishni taqozo etadi.Shuningdek, OSINT (ochiq manbalar asosidagi razvedka) usulining 55 foizlik samaradorligi kiberjinoyatchilarning ijtimoiy tarmoqlar va forumlarda qoldiradigan "raqamli xatti-harakatlari"ni tahlil qilish orqali ularni identifikatsiya qilish mumkinligini isbotlaydi. Biroq, bu usuldan foydalanishda inson huquqlari va shaxsiy hayot daxlsizligi chegarasini aniq belgilash lozim. Natijalar shuni ko‘rsatadiki, kiber-tergovda "Chain of Custody" (dalillar zanjiri) tamoyilini blokcheyn yoki xesh-qiymatlar orqali muhrlash sudda dalillarning rad etilish xavfini keskin kamaytiradi. Bu esa milliy protsessual qonunchilikka "elektron dalilning raqamli pasporti" tushunchasini kiritish zarurligini anglatadi.Kiber-tergov metodikasi faqatgina yangi qurilmalarni sotib olish bilan cheklanib qolmasligi kerak. Bizga kiber-razvedka (Threat Intelligence) va raqamli kriminallistikaning barcha bosqichlarini qamrab oluvchi yaxlit "Kiber-tergov ekotizimi" zarur. Tergovchi va IT-mutaxassis o‘rtasidagi hamkorlik shunchaki maslahat xarakterida emas, balki protsessual jihatdan mustahkamlangan jamoaviy faoliyat shakliga o‘tishi shart. Faqatgina tergov taktikasini "raqamli o‘zgaruvchanlik"ka moslashtirish orqali kiber-makonda jazoning muqarrarligini ta’minlash va kiberjinoyatchilikka qarshi munosib zarba berish mumkin.

XULOSA

Kiberjinoyatlarni tergov qilishning zamonaviy usullari bo‘yicha o‘tkazilgan tadqiqot shuni ko‘rsatadiki, kriminallistika fani jismoniy olamdan raqamli olamga to‘liq transformatsiya bo‘lish bosqichida turibdi. Bugungi kunda kiber-tergov shunchaki kompyuterni ko‘zdan kechirish emas, balki bitlar va baytlar ko‘rinishidagi "raqamli iz"larni (digital footprints) aniqlash, ularning butunligini (integrity) saqlash va sudlarda ishonchli dalil sifatida isbotlashning murakkab texnologik jarayonidir. Tadqiqot davomida aniqlanganidek, an’anaviy tergov usullari kiber-makonning anonimligi va ma’lumotlarning o‘ta o‘zgaruvchanligi (volatility) oldida o‘z samaradorligini yo‘qotmoqda. Bu esa tergov organlaridan kiberforenzika (digital forensics) va kiber-razvedka (OSINT) kabi proaktiv metodlardan keng foydalanishni taqozo etadi.

Kiber-tergovning muvaffaqiyati nafaqat zamonaviy texnik vositalarga, balki tergovchining "raqamli tafakkuri" va protsessual harakatlarning texnik aniqligiga bog‘liqdir. "Chain of Custody" (dalillar zanjiri) tamoyilini raqamli formatda qo‘llash va elektron dalillarning xesh-qiymatlarini (hash values) muhrlash sudda dalillarning rad etilish xavfini keskin kamaytiradi. Milliy tergov amaliyotini xalqaro kiberforenzik standartlar (ISO/IEC 27037) asosida qayta tashkil etish, tergovchi va IT-mutaxassis hamkorligini protsessual jihatdan mustahkamlash kiber-makonda jazoning muqarrarligini ta’minlashning yagona yo‘lidir. Zero, kiber-tergovda adolatga erishish — bu texnologik mahorat va huquqiy bilimning eng yuqori nuqtadagi uyg‘unligidir.

Tavsiyalar

1. **"Raqamli xesh-muhr" tizimini joriy etish:** Elektron dalil olingan vaqtda uning xesh-qiymatini (MD5, SHA-256) darhol hisoblash va bayonnomada muhrlash tartibini qonuniy belgilash.
2. **"Live Forensics" (Jonli tahlil) metodikasi:** Tergovchilarga qurilmani o‘chirmasdan, operativ xotiradagi (RAM) uchuvchan ma’lumotlarni "muzlatib olish" (snapshot) bo‘yicha texnik-taktik yo‘riqnomalar ishlab chiqish.
3. **Blokcheyn asosidagi "Dalillar zanjiri":** Elektron dalillarning olingan vaqtidan sudga qadar bo‘lgan harakatini o‘zgartirib bo‘lmaydigan raqamli log-fayllar (Blockchain-based log) orqali kuzatish tizimini yaratish.
4. **OSINT bo‘linmalarini tashkil etish:** Tergov departamentlari tarkibida ochiq manbalar va ijtimoiy tarmoqlar orqali kiber-razvedka o‘tkazuvchi maxsus tahliliy guruhlarni shakllantirish.

5. **"Virtual hodisa joyini ko‘zdan kechirish" bayonnomasi:** JPKga masofaviy serverlar va bulutli xotiralarni ko‘zdan kechirishning o‘ziga xos protsessual tartibini kiritish.
6. **Kiber-tergovchilarning ixtisoslashgan tayyorgarligi:** IIV akademiyasida yurist-koder (Legal Coder) va kiber-analitik (Cyber Analyst) kvalifikatsiyasiga ega tergovchilarni tayyorlash tizimini yo‘lga qo‘yish.
7. **Xalqaro kiberforenzika standartlari (ISO):** Milliy tergov amaliyotiga elektron dalillar bilan ishlashning ISO/IEC 27037 xalqaro standartlarini majburiy talab sifatida joriy etish.
8. **Cloud Forensics (Bulutli kriminallistika) hamkorligi:** Transmilliy provayderlar (Google, Apple, Microsoft) bilan ma’lumotlarni tergov uchun tezkor olish bo‘yicha o‘zaro hamkorlik protokollarini imzolash.
9. **Kiber-psixologik profil yaratish usuli:** Jinoyatchining harakat algoritmi (Modus Operandi) asosida uning kiber-shaxsi va kelgusi qadamlarini bashorat qiluvchi dasturiy komplekslarni joriy etish.
10. **"Raqamli dalil pasporti":** Har bir elektron dalil uchun uning texnik parametrlarini, olingan joyini va butunligini tasdiqlovchi alohida raqamli pasport tizimini yaratish.

ADABIYOTLAR RO‘YXATI

1. **O‘zbekiston Respublikasining Jinoyat-protsessual kodeksi.** (1994). Toshkent: Adolat. (Elektron dalillar bilan ishlashning protsessual asosi).
2. **O‘zbekiston Respublikasining “Kiberxavfsizlik to‘g‘risida”gi Qonuni.** (2022). O‘RQ-764-son. Toshkent.
3. **ISO/IEC 27037:2012.** *Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence.* (Raqamli dalillar bilan ishlashning xalqaro standarti).
4. **Casey, E. (2011).** *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet.* Academic Press. (Kiberforenzika bo‘yicha dunyodagi eng nufuzli qo‘llanma).
5. **Carrier, B. (2005).** *File System Forensic Analysis.* Addison-Wesley Professional. (Faylli tizimlarni kriminallistik tahlil qilish metodikasi).
6. **Beebe, N. L. (2009).** *Digital Forensic Research: The Good, the Bad and the Unaddressed.* Advances in Digital Forensics V. (Kiber-tergovda sun’iy intellektni qo‘llash nazariyasi).
7. **Zuyev, S. V. (2021).** *Elektronnaya kriminalistika: Uchebnoye posobiye.* Moskva: Yurist. (Elektron kriminallistika va masofaviy tergov harakatlari).
8. **Veklenko, V. B. (2018).** *Metodika rassledovaniya prestupleniy v sfere kompyuternoy informatsii.* Monografiya. (Kiber-tergovning protsessual va taktik asoslari).
9. **Bastrikin, A. I. (2020).** *Sifrovaya kriminalistika.* Moskva: Prospekt. (Raqamli dalillar zanjiri — Chain of Custody tahlili).
10. **Rustambayev, M. X. (2021).** *Kiberjinoyatchilikka qarshi kurashishning kriminallistik va huquqiy muammolari.* Toshkent.
11. **Tadjiyev, A. A. (2023).** *Kiber-firibgarliklarni fosh etishda raqamli izlar bilan ishlashning taktik algoritmlari.* Toshkent: IIV Akademiyasi.
12. **Akramov, A. A. (2022).** *Elektron dalillarning protsessual maqomi va ularni mustahkamlash tartibi.* Toshkent: TDYU.
13. **Interpol (2023).** *Global Guidelines for Digital Forensics Laboratories.* (Kiberforenzik laboratoriyalar uchun xalqaro uslubiy qo‘llanma).
14. **Baza, G. (2018).** *Open Source Intelligence (OSINT) Methods and Tools.* Syngress. (Ochiq manbalar asosidagi kiber-razvedka metodikasi).
15. **UNODC (2022).** *Manual on Mutual Legal Assistance and Extradition.* United Nations. (Xalqaro kiber-tergovda elektron ma’lumotlarni almashish tartibi).