SCIENTIFIC CONFERENCE OPEN PROCEEDINGS
Global Academic Knowledge Repository

AXBOROT TEXNOLOGIYALARI SOHASIDAGI JINOYATLARGA QARSHI KURASHISHDA HUQUQNI MUHOFAZA QILUVCHI ORGANLAR FAOLIYATINI TAKOMILLASHTIRISHNING NAZARIY VA AMALIY JIHATLARI

Omonboyev Dilmurod Bekkamol o‘g‘li

O‘zbekiston Respublikasi IIV Akademiyasi 3-kurs kursanti

Toshkent. sh

https://doi.org/10.5281/zenodo.20699061

Annotatsiya: Mazkur ilmiy maqolada axborot texnologiyalari (IT) sohasidagi jinoyatlarga qarshi kurashishda huquqni muhofaza qiluvchi organlar faoliyatining nazariy va amaliy muammolari kompleks tahlil qilingan. Kiber-makondagi jinoyatlarning transmilliy tabiati, raqamli dalillarni to‘plash va yuridik baholashdagi nazariy bo‘shliqlar hamda tezkor-tergov amaliyotidagi qiyinchiliklar (anonimlik, kriptografiya, elektron izlarni yo‘q qilish) ilmiy asoslangan. Kiberjinoyatchilikka qarshi kurashishda AQSh (FBI Cyber Division), Estoniya va Interpol (IGCI) kabi xalqaro va xorijiy tuzilmalarning ilg‘or tajribasi qiyosiy o‘rganilib, O‘zbekiston huquqni muhofaza qiluvchi organlari amaliyotini, xususan, kiber-kriminalistika va tezkor-qidiruv faoliyatini takomillashtirish yuzasidan aniq ilmiy-amaliy takliflar ishlab chiqilgan.

Kalit so‘zlar: axborot texnologiyalari, kiberjinoyatchilik, huquqni muhofaza qiluvchi organlar, raqamli dalil, OSINT, transmilliy jinoyat, kiberxavfsizlik, xorij tajribasi.

Аннотация: В данной научной статье проводится комплексный анализ теоретических и практических проблем деятельности правоохранительных органов по борьбе с преступлениями в сфере информационных технологий (ИТ). Научно обоснованы транснациональная природа преступлений в киберпространстве, теоретические пробелы в сборе и юридической оценке

цифровых доказательств, а также трудности в оперативно-следственной практике (анонимность, криптография, уничтожение электронных следов). Изучен передовой зарубежный и международный опыт США (FBI Cyber Division), Эстонии и Интерпола (IGCI) в борьбе с киберпреступностью, разработаны конкретные научно-практические предложения по совершенствованию практики правоохранительных органов Узбекистана, в частности, киберкриминалистики и оперативно-розыскной деятельности.

Ключевые слова: информационные технологии, киберпреступность, правоохранительные органы, цифровое доказательство, OSINT, транснациональное преступление, кибербезопасность, зарубежный опыт.

Abstract: This scientific article provides a comprehensive analysis of the theoretical and practical problems of the activities of law enforcement agencies in combating crimes in the field of information technology (IT). The transnational nature of crimes in cyberspace, theoretical gaps in the collection and legal assessment of digital evidence, and difficulties in operational and investigative practice (anonymity, cryptography, destruction of electronic traces) are scientifically substantiated. The advanced foreign and international experience of the USA (FBI Cyber Division), Estonia, and Interpol (IGCI) in combating cybercrime was comparatively studied, and specific scientific and practical proposals were developed for improving the practice of law enforcement agencies of Uzbekistan, in particular, cyber forensics and operational-search activities.

Keywords: information technology, cybercrime, law enforcement agencies, digital evidence, OSINT, transnational crime, cybersecurity, foreign experience.

Jahon miqyosida axborot-kommunikatsiya texnologiyalarining (AKT) jadal rivojlanishi insoniyat hayotini yengillashtirish bilan birga, jinoyat olamining to‘liq kiber-makonga ko‘chishiga sabab bo‘ldi. Kiber-makon — jismoniy chegaralarga ega bo‘lmagan, anonimlik va tezkorlik hukmronlik qiladigan hududdir. Bugungi kunda

firibgarlik, o‘g‘rilik, giyohvand moddalar savdosi va odam savdosi kabi an'anaviy jinoyatlar axborot texnologiyalari vositasida yangicha, raqamli Modus Operandi (ishlash uslubi) kasb etmoqda.

O‘zbekiston Respublikasida kiberxavfsizlikni ta'minlash va IT sohasidagi jinoyatlarga qarshi kurashish davlat xavfsizligining ajralmas qismiga aylandi. Biroq, huquqni muhofaza qiluvchi organlar (IIO, DXX, Prokuratura) faoliyatida jinoyatchilarning yuksak texnologik qadamlariga munosib javob qaytarishda qator nazariy va amaliy muammolar ko‘zga tashlanmoqda. Bu esa tizimni kadrlar salohiyati, texnik ta'minot va huquqiy baza nuqtai nazaridan tubdan takomillashtirishni taqozo etadi.

Axborot texnologiyalari sohasidagi jinoyatlarni tergov qilishning huquqiy mexanizmlarida qator nazariy masalalar hal etilishini kutmoqda:

- **Raqamli dalillar muammosi:** Jinoyat-protsessual qonunchiligimizda "raqamli dalil" (digital evidence) tushunchasi va uning maqomi to‘liq ochib berilmagan. Kiberjinoyat joyi — bu serverlar, bulutli texnologiyalar (Cloud) yoki mobil qurilma xotirasidir. Elektron dalilni nusxalash, uning asl nusxa ekanligini isbotlash (xesh-summaga asosan) va sudda maqbul dalil sifatida tan olinishi nazariy jihatdan qat'iy protsessual tartibga solinishi zarur.
- **Yurisdiksiya va transmilliy jinoyatlar:** Kiberjinoyatchi chet elda turib (masalan, Yevropa yoki Osiyoda), serverni boshqa davlatda ijaraga olgan holda, O‘zbekiston fuqarosiga nisbatan jinoyat sodir etadi. Bunda jinoyat sodir etilgan joy qaysi davlat hisoblanishi, qaysi davlat qonunlari qo‘llanilishi borasida xalqaro huquq doirasida tergov yurisdiksiyasini aniqlash katta nazariy qiyinchiliklarni keltirib chiqarmoqda.

Tezkor xodimlar va tergovchilar bevosita amaliyotda quyidagi to‘siqlarga duch kelishmoqda:

- **Anonimlashtirish texnologiyalari (Darknet, VPN, Tor):** Jinoyatchilar o‘zlarining IP-manzillarini va shaxsini yashirish uchun zamonaviy shifrlash usullaridan foydalanadilar. Huquqni muhofaza qiluvchi organlarda aksariyat hollarda zanjirli proksi-serverlarni buzib kirish (de-anonimizatsiya) uchun kuchli texnik vositalar va hisoblash quvvatlari yetishmaydi.
- **Xalqaro IT korporatsiyalar bilan ishlashdagi byurokratiya:** Telegram, Meta (Facebook, Instagram), Google kabi transmilliy kompaniyalar serverlaridan gumondor haqida ma'lumot olish uzoq vaqt oladi yoxud kompaniyalar o‘z siyosatini ro‘kach qilib ma'lumot berishni rad etadi. Jinoyatni issiq izidan ochishda esa oylar davom etadigan rasmiy so‘rov xatlari tizimning samaradorligini keskin pasaytiradi.
- **Kadrlar yetishmovchiligi:** Jinoyat qidiruv xodimlari asosan an'anaviy tezkor harakatlarga ixtisoslashgan. Kod yozish, kiber-hujumlarni qaytarish va kriptovalyuta tranzaksiyalarini kuzatish (blockchain analytics) kabi IT-kompetensiyaga ega bo‘lgan "high-tech" tezkor xodimlarga ehtiyoj yuqori bo‘lib qolmoqda.

Rivojlangan davlatlar kiberjinoyatchilikka qarshi huquqni muhofaza qilish tuzilmalarini to‘liq transformatsiya qilgan:

- **AQSh (FBI Cyber Division):** Amerika Qo‘shma Shtatlari Federal Qidiruv Byurosida "Cyber Action Teams" (Kiber tezkor harakat guruhlari) mavjud. Ushbu guruh tarkibiga tergovchidan tashqari, dasturchi, kriptograf va xakerlik bo‘yicha mutaxassislar jalb qilingan. Shuningdek, xususiy sektor (banklar, IT-kompaniyalar) va davlat o‘rtasida "InfraGard" tizimi orqali real vaqt rejimida shubhali kiber-harakatlar haqida ma'lumot almashiladi.
- **Estoniya:** Kiber-xavfsizlik bo‘yicha Yevropada yetakchi. Estoniya politsiyasida "Kiber-patrul" (Cyber Patrol) loyihasi doirasida maxsus veb-konstabllar faoliyat yuritadi. Ular ijtimoiy tarmoqlarda rasmiy profil bilan o‘tirib, fuqarolarga yordam beradi, firibgarliklarni fosh etadi va yoshlar o‘rtasida kiber-gigiyenani targ‘ib qiladi.

- **Interpol (IGCI - Singapur):** Interpolning Singapurdagi Global innovatsiyalar majmuasi (IGCI) kiberjinoyatchilikka qarshi xalqaro xab bo‘lib xizmat qiladi. Bu markaz dunyo bo‘ylab politsiya organlariga Darknet tarmog‘idagi jinoyatlarni fosh etishda va raqamli dalillarni ekspertiza qilishda ilg‘or texnologik ko‘mak beradi.

Mamlakatimiz huquqni muhofaza qiluvchi organlarining axborot texnologiyalari sohasidagi jinoyatlarga qarshi kurashish faoliyatini tubdan takomillashtirish va zamonaviy talablarga moslashtirish maqsadida quyidagi ilmiy-amaliy takliflar ilgari suriladi:

Birinchidan, O‘zbekiston Respublikasining Jinoyat-protsessual kodeksiga **"Elektron va raqamli dalillar"** nomli maxsus bob kiritish. Bu bobda raqamli ma'lumotlarni qidirish, nusxa ko‘chirish, saqlash (shifrlangan holda) hamda xalqaro bulutli serverlardagi ma'lumotlarni qonuniy dalil sifatida e'tirof etishning qat'iy mexanizmlarini belgilash zarur.

Ikkinchidan, Xalqaro huquqiy hamkorlikni kengaytirish maqsadida O‘zbekiston Respublikasining Yevropa Kengashining **"Kiberjinoyatchilik to‘g‘risida"gi Budapesht Konvensiyasiga** qo‘shilishini tezlashtirish. Bu orqali xorijiy davlatlar, transmilliy IT-kompaniyalar va O‘zbekiston IIO o‘rtasida kiber-jinoyatchilarga oid ma'lumotlarni soatbay va tezkor almashishning qonuniy platformasi shakllanadi.

Uchinchidan, IIV, DXX va Bosh prokuratura tizimida asosan dasturlash, kiber-razvedka (OSINT) va kriptovalyuta trekingini mukammal biluvchi kadrlardan iborat **Yagona idoralararo Kiber-tergov (Cyber Investigation) markazini** tashkil etish. Markaz xodimlariga an'anaviy huquqiy bilimlardan ko‘ra ko‘proq texnik ("High-Tech") bilimlarni beruvchi xalqaro sertifikatsiyalangan (CEH, CHFI) o‘quv kurslarini joriy qilish.

Xulosa o‘rnida shuni ta'kidlash kerakki, axborot texnologiyalari sohasidagi jinoyatlar intellektual salohiyatli va texnologik qurollangan huquqbuzarlar tomonidan

sodir etiladi. Bu urushda faqatgina "an'anaviy" tergov va operativ usullar bilan g‘alaba qozonib bo‘lmaydi. Huquqni muhofaza qiluvchi organlar tizimni to‘liq raqamlashtirishi, kiber-mutaxassislarni tayyorlashi va xalqaro axborot maydonida mustahkam integratsiyaga erishishi bugungi kunning kechiktirib bo‘lmas talabidir.

REFERENCES

1. O‘zbekiston Respublikasining "Kiberxavfsizlik to‘g‘risida"gi Qonuni. 15.04.2022 yildagi O‘RQ-764-son.
2. O‘zbekiston Respublikasining Jinoyat hamda Jinoyat-protsessual kodekslari. Elektron resurs: https://lex.uz.
3. Xudoyberdiyev A.A. "Ma’muriy ishlarni yuritish kafolatlari va huquqni qo‘llash amaliyoti". O‘quv qo‘llanma. – Toshkent: IIV Akademiyasi, 2024.
4. G‘ofurov I., Karimov U. "Axborot xavfsizligi va kiberjinoyatlarga qarshi kurashish asoslari". – Toshkent: IIV Malaka oshirish instituti, 2022.
5. Federal Bureau of Investigation (FBI). "Internet Crime Report 2023: Cyber Division Strategies". U.S. Department of Justice, 2024.
6. Interpol. "Global Cybercrime Threat Assessment: Policing in the Digital Age". IGCI, Singapore, 2023.
7. Council of Europe. "Convention on Cybercrime" (Budapest Convention), ETS No. 185.