

**RAQAMLI DALILLARNI TO'PLASHNING TERGOV TAKTIKASI:
ZAMONAVIY MUAMMOLAR VA STRATEGIK YONDASHUVLAR**

Muxammadiyeva Sevara Yolg'oshovna

Surxondaryo viloyati Termiz davlat

universiteti Yuridik fakulteti

Yurisprudensiya yo'nalishi talabasi

Annotatsiya: Ushbu maqolada kiberjinoyatchilikning rivojlanishi sharoitida raqamli dalillarni to'plash, ularni mustahkamlash va baholashning protsessual hamda kriminalistik taktikasi tadqiq etiladi. Muallif an'anaviy tergov harakatlarini raqamli makonda qo'llashning o'ziga xos xususiyatlarini tahlil qilib, elektron ma'lumotlarning o'zgaruvchanligi va yo'qolib ketish xavfi yuqoriligini hisobga olgan holda, tergov taktikalarini optimallashtirish bo'yicha ilmiy-amaliy tavsiyalar ishlab chiqqan. Shuningdek, raqamli kriminalistika (digital forensics) vositalaridan qonuniy foydalanishning protsessual kafolatlari va xalqaro standartlari tahlil qilingan.

Kalit so'zlar: raqamli dalil, tergov taktikasi, kiberjinoyat, raqamli kriminalistika, elektron ma'lumot tashuvchi, protsessual kafolat, ko'zdan kechirish, ashyoviy dalil.

Abstract: This article examines the procedural and forensic tactics of collecting, consolidating, and evaluating digital evidence in the context of evolving cybercrime. Analyzing the specific features of applying traditional investigative actions in the digital space, the author develops scientific and practical recommendations for optimizing investigative tactics, considering the high volatility and risk of erasure of electronic data. Furthermore, the procedural guarantees and international standards of the legitimate use of digital forensics tools are analyzed.

Keywords: digital evidence, investigative tactics, cybercrime, digital forensics, electronic media, procedural guarantee, examination, physical evidence.

Kirish

XXI asrda axborot-kommunikatsiya texnologiyalarining shiddatli taraqqiyoti jamiyat hayotining barcha jabhalarini raqamlashtirish bilan bir qatorda, jinoiy faoliyatning ham transformatsiyalashuviga olib keldi. Bugungi kunda an'anaviy jinoyatlarning aksariyati (firgarlik, o'g'rilik, tovlamachilik) virtual makonga ko'chdi, shuningdek,

kiberterrorizm, tarmoq tizimlariga noqonuniy kirish kabi sof raqamli jinoyatlar soni geometrik progressiya bilan ortib bormoqda. Bunday sharoitda jinoyat-protsessual qonunchiligi va kriminalistika fani oldida yangi konseptual muammo – raqamli dalillar (digital evidence) bilan ishlashning ilmiy asoslangan taktikasini yaratish vazifasi turibdi. Raqamli dalillar o'zining tabiatiga ko'ra nomoddiy, o'zgaruvchan (volatile), nusxalanishi oson va latentlik darajasi yuqori bo'lgan ma'lumotlar yig'indisidir. Shuning uchun ham ularni to'plashda an'anaviy tergov taktikalarini to'g'ridan-to'g'ri qo'llash ko'pincha kutilgan natijani bermaydi yoki dalilning yuridik kuchini yo'qotishiga (maqbul emas deb topilishiga) sabab bo'ladi. Ushbu maqolaning dolzarbligi raqamli dalillarni aniqlash, olish va saqlash jarayonlarini kriminalistik va protsessual jihatdan uyg'unlashtiruvchi taktik algoritim va ilmiy yondashuvlarni ishlab chiqish zarurati bilan belgilanadi.

Asosiy qism

1. Raqamli dalil tushunchasi va uning kriminalistik tabiati

Kriminalistik nuqtai nazardan raqamli dalil — bu elektron-hisoblash mashinalari, tizimlari, tarmoqlari yoki ularning tashuvchilarida binar kodlar (0 va 1) ko'rinishida shakllanadigan, jinoyatni fosh etish va haqiqatni aniqlash uchun ahamiyatga ega bo'lgan har qanday ma'lumotdir.

Raqamli dalillarning o'ziga xos xususiyatlari quyidagi jadvalda tizimlashtirilgan:

2. Raqamli dalillarni to'plashning tergov taktikasi tamoyillari

Raqamli makonda tergov harakatlarini (tintuv, ko'zdan kechirish, olib qo'yish) o'tkazishda quyidagi fundamental taktik qoidalarga rioya qilinishi shart:

1. Dalillarning daxlsizligi (Integrity): Tergov harakati davomida ob'ektdagi dastlabki ma'lumotlar o'zgarimasligi kerak. Buning uchun qurilmalar tarmoqdan (Wi-Fi, GSM, Bluetooth) uziladi (Faraday qoplaridan foydalaniladi).

2. Zanjirli saqlash (Chain of Custody): Dalil topilgan lahzadan boshlab sud zaligacha bo'lgan har bir harakat, kimning qo'lida bo'lgani va qanday texnik ishlov berilgani to'liq hujjatlashtirilishi shart.

3. Faqat litsenziyalangan va verifikatsiya qilingan dasturlardan foydalanish: Tergovchi yoki mutaxassis ma'lumotlarni ko'chirishda "EnCase", "FTK Imager", "Cellebrite" kabi xalqaro miqyosda tan olingan kriminalistik dasturlardan foydalanishi lozim.

3. Alohida tergov harakatlarining taktik xususiyatlari

Elektron qurilmalarni ko'zdan kechirish va olib qo'yish taktikasi: Tergovchi voqea joyiga kelganda kompyuter yoki smartfon "yoqilgan" (Live state) holatda bo'lsa, uni darhol o'chirish katta xatodir. Sababi, tezkor xotirada (RAM) jinoyatchining parollari,

shifrlangan kesh-ma'lumotlari va virtual hamyon kalitlari saqlanib turgan bo'lishi mumkin. Taktik jihatdan, mutaxassis dastlab RAM xotira nusxasini (dump) olishi, shundan so'nggina qurilmani tizimli o'chirishi yoki transportirovka qilishi kerak.

Bulutli texnologiyalar (Cloud Forensics) va tarmoq trafigini tahlil qilish: Zamonaviy jinoyatchilar ma'lumotlarni jismoniy diskda emas, balki Google Drive, AWS, Telegram serverlari kabi "bulutli" omborlarda saqlaydi. Bunday vaziyatda tergov taktikasi provayderlar bilan tezkor hamkorlik qilish, IP-manzillar log-fayllarini va xalqaro miqyosda o'zaro huquqiy yordam ko'rsatish (MLAT) tizimlari orqali so'rovlar yuborishni ko'zda tutadi.

Xulosa

Raqamli dalillarni to'plashning tergov taktikasi – bu faqatgina huquqiy protsedura emas, balki yuqori texnologik va kriminalistik bilimlar sintezidir. Tadqiqot natijasida quyidagi ilmiy-amaliy xulosalarga kelindi:

Qonunchilikni modernizatsiya qilish: Amaldagi Jinoyat-protsessual kodekslariga "raqamli dalil", "elektron ma'lumot tashuvchi", "tarmoq trafigini qayd etish" kabi tushunchalarni aniq huquqiy maqomini belgilash va ularni olib qo'yishning maxsus protsessual tartibini kiritish lozim.

Taktik algoritmlarni standartlashtirish: Tergovchilar uchun kiberjinoyat turlaridan kelib chiqib (masalan, fishing, kriptovalyuta aktivlarini o'g'irlash), voqea joyini ko'zdan kechirishning bosqichma-bosqich taktik yo'riqnomalarini (Checklist) joriy etish zarur.

Kriminalistik texnika vositalarini yangilash: Tergov bloklarini ma'lumotlar yaxlitligini buzmasdan nusxa oluvchi blokatorlar (Write-Blockers) va maxsus kriminalistik dasturiy majmualar bilan ta'minlash, shuningdek, tergovchi-kriminalistlarning raqamli gigiyena va texnik savodxonligini tizimli oshirish talab etiladi.

Foydalanilgan adabiyotlar

1. Rustambayev, M. H. (2021). *Kiberjinoyatchilik va unga qarshi kurashishning huquqiy asoslari*. Toshkent: Adolat.
2. Inakov, Q. A. (2023). *Kriminalistika: Tergov taktikasi va metodikasi*. Darslik. Toshkent: TDYUU.
3. Casey, E. (2019). *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet*. Academic Press.

4. Carrier, B. (2005). **File System Forensic Analysis**. Addison-Wesley Professional.
5. O'zbekiston Respublikasining Jinoyat-protsessual kodeksi (2026-yil holatiga ko'ra o'zgarishlar va qo'shimchalar bilan).
6. Xarisov, R. G. (2022). **Taktika osmotra i iz'yatiya cifrovih nositeley informacii**. Moskva: Yurlitinform.
7. ISO/IEC 27037:2012. **Information technology — Security techniques — Guidelines for identification, collection, acquisition, and preservation of digital evidence**.
8. Garrison, C. P. (2020). **Digital Forensics for Legal Professionals**. Information Science Publishing.
9. Bazarov, A. B. (2024). Elektron dalillarning jinoyat protsessidagi maqboliylik muammolari. **Huquq va burch**, 4(12), 45-51.
10. National Institute of Justice (NIJ). (2021). **Digital Evidence Handbook: A Guide for Law Enforcement**. Washington, DC.