Iyun, 2025-Yil

KIBER JINOYATLARNI TERGOV QILISHDA ELEKTRON DALILLARNI ANIQLASHNING KRIMINALISTIK JIHATLARI

Tulanboyeva Adiba Alijon qizi
Toshkent davlat yuridik universiteti Magistratura va sirtqi ta'lim fakulteti magistranti

https://doi.org/10.5281/zenodo.15771362

Annotatsiya. *Ushbu maqolada kiber jinoyatlarni tergov qilishda elektron dalillarni aniqlash, ularni to'plash, hujjatlashtirish va baholash jarayonlarining kriminalistik jihatlari tahlil qilinadi. Insonlarva jinoyatchilarning virtual muhit bilan uzviy bog'lanib borishi natijasida jinoyatning sodir etilishi va dalillarning yashirilish shakllari ham murakkablashmoqda. Elektron dalillarni to'g'ri aniqlash — jinoyatni ochish, gumondorni aniqlash va sudda isbotlash uchun hal qiluvchi omil hisoblanadi. Maqolada xalqaro amaliyot, sud-tibbiy ekspertiza vositalari, tergovchilarning rolini belgilovchi qonunchilik va zamonaviy texnologik yondashuvlar yoritiladi.*

Kalit so'zlar: *Kiber jinoyat, elektron dalil, kriminalistika, tergov, sud ekspertizasi, dalilni autentifikatsiya qilish, jinoyat joyi, ishonchlilik.*

Zamonaviy axborot-kommunikatsiya texnologiyalarining rivojlanishi inson hayotini tubdan o'zgarib yangi jarayonga o'tishiga sababchi bo'ldi. Bu jarayon bilan birga jinoyatchilikning yangi shakllari ham yuzaga keldi. Kiber jinoyatlar an'anaviy jinoyatlarga qaraganda murakkabroq tuzilishga ega bo'lib, ko'pincha ko'zga ko'rinmas tarzda amalga oshiriladi. Jinoyatchilar o'z shaxsini yashirish uchun anonim tarmoqlar, VPN xizmatlari, shifrlangan messenjerlar va boshqa zamonaviy vositalardan foydalanadilar. Shu bois, bunday jinoyatlarni tergov qilish va unga oid dalillarni aniqlash kriminalistik metodlardan foydalanishni talab etadi.

Kiber jinoyatlar tergovida eng asosiy isbot vositalaridan biri bu — elektron dalillardir. Shuningdek, elektron dalilni aniqlash nafaqat texnik bilimni, balki jinoyat voqea joyining virtual ko'rinishini to'g'ri baholashni, voqealar zanjirini tiklashni va har bir raqamli izni kriminalistik nuqtai nazardan baholashni ham talab etadi. Bularning barchasi elektron dalilni aniq va qonuniy aniqlashning kriminalistik jihatlarini o'rganishni zamonaviy jinoyatchilikka qarshi kurashda dolzarb masalaga aylantirmoqda.

An'anaviy jinoyatlarda jinoyat sodir bo'lgan joy aniq bir manzil ko'rsatiladi. Misol uchun: kvartira, ko'cha, omborxona va hokazo. Biz hodisa sodir etilgan joyni ko'zimiz bilan ko'rishmiz, uni ko'zdan kechirib, dalillarni olishimiz mumkin. Ammo kiber jinoyatlarda jinoyat joyi an'anaviy tushunchalardan keskin farq qiladi. Bunda jinoyat "virtual muhit"da sodir etilishi mumkin: lokal tarmoqda, veb-sayt orqali, elektron pochta orqali yoki bulutli xizmatdan foydalangan holda. Shu bois, kiber jinoyat joyini aniqlash — tergovning dastlabki bosqichlarida hal qiluvchi ahamiyatga ega bo'lgan murakkab kriminalistik vazifa hisoblanadi.

Kiber jinoyat joyini kriminalistik nuqtai nazardan quyidagicha tavsiflash mumkin: bu — jinoyat sodir bo'lgan, jinoyatchi tomonidan raqamli faoliyat amalga oshirilgan va dalillar mavjud bo'lgan raqamli yoki jismoniy muhitdir. Bu joyga kompyuterlar, serverlar, mobil qurilmalar, routerlar, bulutli platformalar, USB qurilmalar, xotira kartalari va boshqa texnik vositalar kiradi. Shu bilan birga, jinoyat izlari tarmoq trafiklarida, log fayllarida, kukki (cookie)larda, internet brauzer tarixida va IP-manzillar orqali aniqlanishi mumkin.

Tergov nuqtai nazaridan, kiber jinoyat joyini belgilashning asosiy maqsadi — jinoyat faoliyatiga oid raqamli izlarni aniq topish, ularni hujjatlashtirish va dalil sifatida isbotlashdir. Bunda jinoyat sodir etilgan joyni o‘z ichiga oluvchi ma’lumotlar: tizim kirish vaqtlari, foydalanuvchi nomlari, parollar, IP-loglar, geolokatsiya ma’lumotlari va boshqa texnik ko‘rsatkichlar katta ahamiyatga ega bo‘ladi.

Al-Havqalning fikricha, kiber jinoyat joyi jinoyatning o‘zagini va markazini o‘z ichiga olgan har qanday joy yoki birlik (obyekt yoki virtual server bo‘lishidan qat’i nazar) bo‘lishi mumkin. U jinoyatchilar uchun jinoiy faoliyatni sodir etish yoki tayyorlash uchun xizmat qiluvchi maydon sifatida qaraladi. Shu bilan birga, jinoyat joyi jinoyat tafsilotlarini ochish, jinoyatchining niyatini anglash va jinoyat mexanizmini qayta tiklashda muhim manba bo‘lib xizmat qiladi.

Bundan kelib chiqadiki, kiber jinoyat joyini to‘g‘ri belgilash, u yerdagi elektron dalillarni protsessual normalar asosida yig‘ish va ularni kriminalistik usullar bilan tahlil qilish tergovchilardan yuqori malaka va maxsus texnik bilimlarni talab qiladi.

Elektron dalillarni aniqlashda eng muhim jihat — ularning mavjudligini aniqlash bilan birga, ularga yetkaziladigan ehtimoliy zararlarning oldini olishdir. Chunki raqamli ma’lumotlar osongina o‘zgartirilishi, o‘chirilishi yoki soxtalashtirilishi mumkin. Shuning uchun tergovchi ma’lumotni aniqlagan zahoti, uni darhol hujjatlashtirishi, nusxasini (imaging) olish va asl nusxani muhrlab, tegishli tartibda saqlashi lozim.

Muhim jihatlardan biri shundaki, dalil yig‘ishda foydalaniladigan usullar va texnologiyalar tergov jarayonining qonuniyligini belgilaydi.

Pollitt (2005) ta’kidlaganidek, raqamli dalillar bilan ishlashda an’anaviy kriminalistik yondashuvlar yangi talablarga moslashtirilishi kerak.

Casey (2011) esa elektron dalilni “jinoyat haqida hikoya qiluvchi raqamli izlar to‘plami” sifatida baholaydi. Bu izlarning har biri tergovchi uchun muhim ma’lumot manbai bo‘lib, to‘g‘ri yig‘ilsa — jinoyatni fosh etishdagi asosiy omilga aylanadi.

Autentifikatsiya — bu dalil asl va soxtalashtirilmagan ekanini isbotlash jarayonidir. Masalan, fayl yoki elektron xat tergov paytida qaysi qurilmadan topilganini, unga hech qanday o‘zgartirish kiritilmaganligini hash algoritmlar orqali tasdiqlash kerak. Shu nuqtai nazardan, AQShning Federal Rules of Evidence, 901-qoidasida dalilni autentifikatsiya qilish tartibi aniq ko‘rsatib berilgan. Mazkur qoida, elektron dalilni taqdim etuvchi tomon dalilning asl nusxaligini yoki ishonchliligini ko‘rsatishga majbur ekanini ta’kidlaydi (Cornell Law School, n.d.).

Dolzarblik (relevance) — dalil ko‘rib chiqilayotgan ishga bevosita aloqador bo‘lishi va muhim masalani hal qilishga yordam berishi kerak. Shunchaki voqeaga aloqador bo‘lmagan yoki umumiy ma’lumotlar elektron dalil sifatida qabul qilinmaydi.

Ishonchlilik — dalilning tasodifiy yoki noto‘g‘ri olingan emasligiga ishonch bo‘lishi lozim. Bunda “chain of custody” — ya’ni dalil ustida kim, qachon va qanday ishlagani haqidagi yozuvlar tizimi muhim rol o‘ynaydi. Bu hujjatli zanjir dalilning soxtalashtirilmaganini ko‘rsatadi.

Elektron dalillarni sud eshituvlariga kiritish uchun maxsus qonuniy asoslar yoki istisnolar talab qilinadi. Masalan, uchinchi shaxs tomonidan taqdim etilgan elektron yozuvlar (masalan, bank loglari yoki ijtimoiy tarmoqdan olingan ma’lumotlar) eshitish qoidalariga to‘g‘ri kelmasa, ular “hearsay” deb topilishi va qabul qilinmasligi mumkin. Shu bois tergovchi dalilni qanday usul bilan qo‘lga kiritganini hujjatlashtirishi va qonuniy asoslarga tayanib isbotlashi kerak.

Tergov jarayonida elektron dalillarni baholash ularning sudda ishonchli va yuridik kuchga ega dalil sifatida tan olinishi uchun muhim bosqich hisoblanadi. Baholash bosqichida tergovchi elektron dalilning mazmunini, kontekstini, qanday holatda va qanday texnik vositalar yordamida olinganini tahlil qiladi. Bu jarayon dalilni umumiy jinoyat kontekstida joylashtirish, jinoyatni sodir etgan shaxsni aniqlash va sodir bo'lgan voqealar ketma-ketligini tiklash imkonini beradi.

Zamonaviy kiberjinoyatlar texnologik murakkabligi, raqamli izlarning ko'zga ko'rinmasligi va tezkor o'zgaruvchanligi bilan ajralib turadi. Shuning uchun ularni tergov qilishda elektron dalillar alohida o'rin tutadi. Elektron dalillar jinoyatning sodir bo'lganligini isbotlash, gumondorni aniqlash va sudda adolatli qaror chiqarish uchun asosiy isbot vositasi hisoblanadi.

Ularni to'g'ri aniqlash, hujjatlashtirish va sudda qabul qilinadigan tarzda taqdim etish tergovchi, ekspert va huquqshunoslarning yuqori malakasini talab qiladi. Ayniqsa, jinoyat joyini kriminalistik nuqtai nazardan baholash, raqamli muhitda dalilni aniqlash va uning ishonchliligini ta'minlash kiber tergovning muhim bosqichlaridandir.

REFERENCES

1. Pollitt, M. M. (2005). An Ad Hoc Review of Digital Forensics Models. Proceedings of the Second International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE), IEEE.
2. Casey, E. (2011). Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet (3rd ed.). Academic Press
3. Jaiswal, A. (n.d.). Electronic Evidence. Medium. Retrieved from https://medium.com/@jaiswalamulya3/electronic-evidence-cd349aed85ba
4. Cornell Law School. (n.d.). Federal Rules of Evidence: Rule 901. Retrieved from https://www.law.cornell.edu/rules/fre/rule_901
5. Europol. (2023). Digital Evidence Guidelines. Retrieved from https://www.europol.europa.eu/publications-documents/digital-evidence-guidelines
6. SWGDE. (n.d.). Scientific Working Group on Digital Evidence Publications. Retrieved from https://www.swgde.org/documents
7. CERT-IN. (n.d.). Indian Computer Emergency Response Team. Retrieved from https://www.cert-in.org.in/