HODISA SODIR BO‘LGAN JOYDAN RAQAMLI DALILLARNI QIDIRIB TOPISH,OLISH VA RASMIYLASHTIRISHNING O‘ZIGA XOS XUSUSIYATLARI

O‘zbekiston Respublikasi Ichki ishlar vazirligi
Akademiyasi Krimanilstik ekspertizalari
kafedrasi katta o‘qituvchisi,podpolkovnik
Abdujabborov Bobur Raxmatullayevich
O‘zbekiston Respublikasi Ichki ishlar
vazirligi Akademiyasikunduzgi ta’lim
3-o‘quv kursi kursanti, safdor
Kayumov Ulug‘bek Nizomjon o‘g‘li

Annotatsiya: Mazkur ishda hodisa sodir bo‘lgan joydan raqamli dalillarni qidirib topish, olish va rasmiylashtirish jarayonining o‘ziga xos xususiyatlari yoritilgan. Raqamli dalillar — bu jinoyat yoki huquqbuzarlik bilan bog‘liq elektron shakldagi ma’lumotlar bo‘lib, ular kompyuterlar, mobil telefonlar, planshetlar, tarmoq uskunalari yoki bulutli saqlov tizimlarida mavjud bo‘lishi mumkin. Raqamli dalillarni yig‘ish jarayoni juda ehtiyotkorlik bilan amalga oshiriladi, chunki kichik o‘zgarishlar ham ma’lumotning ishonchliligini buzishi mumkin. Shu bois tergovchi yoki ekspert raqamli qurilmalarni topish, ularni to‘g‘ri o‘chirib qo‘yish, nusxa olish va rasmiylashtirishda belgilangan protseduralarga amal qilishi zarur. Hodisa joyida aniqlangan mobil telefonlar, noutbuklar yoki boshqa qurilmalarni tarmoqdan ajratish va tashqi signallardan himoya qilish maqsadida Faradey qopchasi (Faraday bag) qo‘llaniladi. Bu maxsus metall qoplama yoki materialdan tayyorlangan qopcha qurilmaning simsiz aloqasini (Wi-Fi, Bluetooth, GSM, NFC va h.k.) to‘liq to‘sib, ma’lumotlar o‘chirilishi yoki masofadan o‘zgartirilishining oldini oladi.

Kalit so’zlar: Raqamli dalillar, hodisa joyi, faradey qopchasi, qurilma izolatsiyasi, signal blokirovkasi, bit-to‘liq nusxa olish, ma’lumotlarni nusxalash va saqlash, dalilni hujjatlashtirish, zanjirli saqlash, ma’lumotlarni tiklash.

Аннотация: В данной работе освещены особенности процесса поиска, изъятия и оформления цифровых доказательств с места происшествия. Цифровые доказательства представляют собой электронные данные, связанные с преступлением или правонарушением, которые могут храниться на компьютерах, мобильных телефонах, планшетах, сетевом оборудовании или в облачных хранилищах. Процесс сбора цифровых доказательств осуществляется с особой осторожностью, поскольку даже незначительные изменения могут повлиять на достоверность информации. Поэтому следователь или эксперт должен строго соблюдать установленные процедуры при обнаружении,

отключении, копировании и документировании цифровых устройств. Для изоляции мобильных телефонов, ноутбуков или других устройств, найденных на месте происшествия, от сети и защиты их от внешних сигналов используется мешок Фарадея (Faraday bag). Этот специальный чехол, изготовленный из металлизированного материала, полностью блокирует беспроводные соединения (Wi-Fi, Bluetooth, GSM, NFC и др.), предотвращая удалённое удаление или изменение данных.

Ключевые слова: Цифровые доказательства, место происшествия, мешок Фарадея, изоляция устройства, блокировка сигнала, побитное копирование, копирование и хранение данных, документирование доказательств, цепочка хранения, восстановление данных.

Annotation: This paper highlights the specific features of the process of searching for, collecting, and documenting digital evidence from a crime scene. Digital evidence refers to electronic data related to a crime or offense, which can be stored on computers, mobile phones, tablets, network devices, or cloud storage systems. The process of collecting digital evidence must be carried out with great caution, as even minor changes may compromise the reliability of the information. Therefore, investigators or forensic experts must strictly follow established procedures when identifying, powering off, imaging, and documenting digital devices. To isolate mobile phones, laptops, or other devices found at the crime scene from networks and external signals, a Faraday bag is used. This special pouch, made of metallic or conductive material, completely blocks wireless communications (Wi-Fi, Bluetooth, GSM, NFC, etc.), preventing remote data deletion or alteration.

Keywords: Digital evidence. Crime scene, faraday bag, device isolation, signal blocking, bit-by-bit imaging (or bit-level copy), data copying and storage Evidence documentation Chain of custody, data recovery.

Kirish

Qurilmalar hayotimizning barcha jabhalariga chuqur kirib kelgani sababli, jinoyat va huquqbuzarliklarning katta qismi ham elektron muhitda sodir etilmoqda. Shu bois, hozirgi kunda tergov faoliyatida raqamli dalillarni aniqlash, yig‘ish va tahlil qilish muhim ahamiyat kasb etadi. Raqamli dalillar jinoyatning mohiyati, vaqtini, ishtirokchilarini va boshqa muhim tafsilotlarni aniqlashda asosiy manba bo‘lib xizmat qiladi. Hodisa sodir bo‘lgan joydan raqamli dalillarni qidirib topish, olish va rasmiylashtirish jarayoni o‘ziga xos texnik va protsessual talablarni o‘z ichiga oladi. Chunki raqamli dalillar — bu oson o‘zgartirilishi yoki o‘chirib yuborilishi mumkin bo‘lgan ma’lumotlardir. Shu sababli, tergovchi yoki ekspert har bir qurilma bilan ishlashda ehtiyotkorlik bilan harakat qilishi, dalilning asl holatini saqlab qolish uchun belgilangan tartiblarga qat’iy amal qilishi zarur. Hodisa joyida aniqlangan noutbuklar,

smartfonlar, planshetlar yoki boshqa raqamli vositalar tarmoqdan uzilishi va tashqi aloqa kanallaridan himoyalanishi lozim. Buning uchun Faradey qopchasi (Faraday bag) deb ataluvchi maxsus himoya vositasi qo‘llaniladi. Ushbu qopcha metall yoki o‘tkazuvchi materialdan tayyorlanib, qurilmani Wi-Fi, Bluetooth, GSM, NFC kabi simsiz aloqalardan to‘liq izolyatsiya qiladi. Natijada, qurilma masofadan boshqarilmaydi, undagi ma’lumotlar o‘chirilishi yoki o‘zgartirilishi ehtimoli butunlay bartaraf etiladi. Raqamli dalillarni olish va rasmiylashtirishda ularning uzluksizligini, yaxlitligini va ishonchliligini ta’minlash muhim.

Asosiy

Axborot texnologiyalarining jadal rivojlanishi bilan bir qatorda, jinoyatchilikning yangi turlari — kiberjinoyatlar shakllanib, ularning sodir etilish usullari tobora murakkablashib bormoqda. Shu bois, hodisa sodir bo‘lgan joyda raqamli dalillarni to‘plash, ularni qonuniy tartibda rasmiylashtirish va tahlil qilish zamonaviy tergov faoliyatining ajralmas qismi hisoblanadi. Raqamli dalillar (kompyuter fayllari, mobil qurilmalardagi ma’lumotlar, tarmoq loglari, elektron xatlar, IP-manzillar va boshqalar) nafaqat kiberjinoyatlar, balki iqtisodiy, moliyaviy va hatto terrorchilik bilan bog‘liq jinoyatlarni fosh etishda ham asosiy manba bo‘lib xizmat qiladi. Hodisa sodir bo‘lgan joydan raqamli qurilmalarni va ularni ichidagi elektron ma’lumotlarni aniqlash — bu jarayonning birinchi va muhim bosqichidir. INTERPOL ma’lumotlariga ko‘ra, raqamli forensika — bu «ma’lumotni aniqlash, olish, qayta ishlash va sud yo‘lida taqdim etish» faoliyatidan iborat. Qurilmalar nafaqat kompyuterlar, noutbuklar, planshetlar, smartfonlar, balki tarmoq uskunalari, bulutli saqlov joylari ham bo‘lishi mumkin. Mazkur bosqichda «qurilmalar qayerda joylashgan», «qurilma holati», «tarmoqqa ulangan-u ulanmaganligi» kabi holatlar aniqlanadi. Xususan, birinchi chaqirilgan ekspert yoki tergovchi hodisa joyida tarmoqdan ajratilmagan qurilma orqali ma’lumotlar o‘zgartirilishi, qurilma boshqarilishi mumkinligini tushunishi lozim.

Raqamli dalillarni yig‘ishda eng muhim unsurlardan biri — qurilmalarni tashqi ta’sirlardan himoya qilish. Masalan, hodisa joyida aniqlangan mobil telefon, noutbuk yoki boshqa qurilmalar tarmoqdan uzilishi, simsiz aloqalar (Wi-Fi, Bluetooth, GSM, NFC) orqali chetga ma’lumot uzatilishini bloklash lozim. Bunda qo‘llaniladigan vositalardan biri — Faraday qopchasi (Faraday bag). Bu maxsus metall yoki o‘tkazuvchan materialdan tayyorlangan qopcha qurilmani simsiz signallardan ajratadi, natijada masofadan o‘zgarish yoki ma’lumotlar o‘chirib yuborilish xavfi kamayadi. Chet el tajribasida bir sud laboratoriyasi ichida “Faraday xonasi” yordamida telefon mikrochiplarini signal ta’siridan himoyalangan muhitda tekshirish amaliyoti qo‘llaniladi. Shu bilan birga, mazkur bosqichda qurilmaga tegishli protokollar — harakatlar jurnali yuritilishi, kim tomonidan qurilma qo‘lra olingani, qachon va qanday holatda uzilganligi aniq hujjatlashtirilishi lozim.

Raqamli qurilmadan ma’lumot olish jarayonida juda ehtiyotkorlik talab etiladi. Masalan, maqbul standartlardan biri — ISO/IEC 27037 «Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence». Bu standart qurilmadan ma’lumotlarni bit-to‘liq (ya’ni – hafsasiz) nusxa olish, asl qurilmaga minimal ta’sir qilish va saqlash tizimini yaratish bo‘yicha metodologiyani belgilaydi. Nusxa olingan ma’lumotdagi hash kodi (kriptografik tekshiruv) orqali nusxa asl bilan mosligi tasdiqlanadi.

Saqlash bosqichida esa «zanjirli saqlash» (chain of custody) tamoyiliga rioya qilish zarur. Bu degani: har bir harakat — ma’lumot yig‘ishdan tortib, sudga taqdim etishgacha — hujjatlashtirilishi, qurilma va ma’lumot almashinuvi qat’iy nazorat ostida bo‘lishi kerak. Shu bilan birga, ma’lumotlar juda sekinlik bilan buzilishi mumkin — o‘chib qolishi, shikastlanishi, noto‘g‘ri qurilmalarda ochilishi ehtimoli mavjud. Shuning uchun tarmoqqa ulanmagan, ulanishga yopiq holatda saqlash afzaldir. Raqamli dalillar sudda qo‘llanilishi mumkin bo‘lishi uchun ularning huquqiy jihatdan to‘liq rasmiylashtirilgan bo‘lishi zarur. Masalan, Shavkat Mirziyoyev tomonidan imzolangan qonunga binoan — Law “On Amendments and Additions to Certain Legislative Acts … on Digital Evidence” raqamli dalillarni tan olishga hamda ularni yig‘ish, taqdim etish, ekspertizadan o‘tkazish va saqlash tartiblarini belgilaydi.

Qonunda ko‘rsatilgan jihatlarga: “elektron (raqamli) ma’lumotlar” tushunchasi aniqlanadi, jinoyat protsessual kodeks, fuqarolik-protsessual kodeks va boshqa normativ hujjatlarda tegishli o‘zgarishlar kiritiladi.

Shuningdek, xorijiy tajribalarda ham raqamli dalillarning sudda qabul qilinishida quyidagilarga e’tibor qaratiladi: ma’lumotning asl holati saqlanganligi, ilgari hech qanday o‘zgartirish bo‘lmaganligi, huquqiy yo‘l bilan olinganligi va zanjirli saqlashning uzluksizligi. Bundan tashqari, raqamli dalilning tahlil natijalari, ekspert xulosalari va jihatlar huquqiy qarorlarda aniq belgilanib kelinadi.

2025 yil 30 aprel kuni Shavkat Mirziyoyev rahbarligida imzolangan qaror — «PP-153 qarori (№ PP-153, “Axborot texnologiyalari vositalaridan foydalangan holda sodir etiladigan jinoyatlarga qarshi kurashish faoliyatini yanada mustahkamlash chora-tadbirlari to‘g‘risida”) — bilan respublika darajasida kiberxavfsizlikni mustahkamlash va kiberjinoyatlarga qarshi kurashishga qaratilgan bir qator muhim choralar belgilandi. Quyida qarorning asosiy jihatlari, maqsadlari va amalga oshirilishi rejalashtirilgan chora-tadbirlari bilan tanishishingiz mumkin.

Maqsad va asosiy yo‘nalishlar

Qarorda ko‘rsatilgan asosiy maqsadlar quyidagicha:

Milliy miqyosda kiberxavfsizlik va axborot texnologiyalari orqali sodir etiladigan jinoyatlarga qarshi kurashish tizimini takomillashtirish.

Tegishli davlat organlari, banklar, to‘lov tizimlari, to‘lov institutlari va boshqa tashkilotlar o‘rtasida koordinatsiyani kuchaytirish, ularni aniq mas’uliyat bilan jihozlash.

Fuqarolarni, ayniqsa moliyaviy xavfsizlik jihatidan himoya qilish — to‘lov kartalari, elektron hamyonlar, SIM-kartalar kabi maydonlarda kiberxavfsizlikni ta’minlash hisoblanadi.

Raqamli dalillarni yig‘ish va rasmiylashtirish bo‘yicha xalqaro tajriba shuni ko‘rsatadiki, bu jarayonning huquqiy, texnik va protsessual jihatlari bir butun tizimni tashkil etadi. AQSh tajribasida, masalan, raqamli dalillar bilan ishlash aniq qonunlar va institutlar orqali tartibga solinadi. Xususan, Federal Rules of Evidence (FRE) hamda Electronic Communications Privacy Act (ECPA) qonunlari raqamli axborotni dalil sifatida qabul qilish, saqlash va sudda taqdim etish tartibini belgilaydi. AQShda Federal Bureau of Investigation (FBI) huzurida faoliyat yurituvchi Digital Forensics Laboratory (Raqamli sud ekspertizasi laboratoriyasi) va National Computer Forensics Institute (NCFI) tizimlari raqamli dalillarni tahlil qilish, ularni qayta tiklash hamda autentifikatsiya qilishda xalqaro standartlardan — xususan, NIST SP 800-86 (Guide to Integrating Forensic Techniques into Incident Response) hujjatidan foydalanadi. Shu bilan birga, AQShda raqamli dalillarni olishda shaxsiy hayot daxlsizligini ta’minlash, ya’ni konstitutsion Fourth Amendment (qidiruv va musodara qilish huquqiga oid) talablariga qat’iy rioya qilinadi.

Rossiya Federatsiyasida esa raqamli dalillar bilan ishlash tizimi “Axborot, axborot texnologiyalari va axborotni himoya qilish to‘g‘risida”gi Federal qonun hamda Jinoyat-protsessual kodeksining 81-moddasi asosida amalga oshiriladi. Rossiyada Ichki ishlar vazirligi va Tergov qo‘mitasi huzurida maxsus kriminalistik axborot-texnik ekspertiza laboratoriyalari faoliyat yuritadi. Ushbu laboratoriyalar “GosSOPKA” tizimi (Davlat kompyuter hodisalariga javob tizimi) bilan integratsiyalashgan bo‘lib, u raqamli dalillarni markazlashtirilgan tartibda yig‘ish, ularning butligini ta’minlash va sud jarayonlarida dalil sifatida ishlatishga mo‘ljallangan. Rossiya tajribasida dalillarni olishda “zanjirli saqlash” (chain of custody) tamoyiliga alohida e’tibor qaratiladi, ya’ni dalilning dastlabki holatidan tortib, sudda taqdim etilguniga qadar har bir o‘zgarish hujjatlashtiriladi.

Xalqaro amaliyot shuni ko‘rsatadiki, raqamli dalillarni to‘plash va rasmiylashtirishda texnik aniqlik, huquqiy asos va dalilning ishonchliligi eng muhim tamoyillar hisoblanadi. AQSh tajribasi jarayonning texnik standartlashuviga e’tibor qaratgan bo‘lsa, Rossiya tajribasi huquqiy-protsessual qat’iylik va markazlashtirilgan nazorat tizimi orqali samaradorlikka erishgan. O‘zbekistonning PQ-153-son qarori mazkur ilg‘or tajribalarni milliy sharoitga moslashtirib, raqamli dalillar bilan ishlash bo‘yicha yagona normativ-huquqiy mexanizmni shakllantirishga xizmat qiladi.

Xulosa

Hodisa sodir bo‘lgan joydan raqamli dalillarni qidirish, ularni olish va rasmiylashtirish jarayoni nafaqat huquqiy jihatdan, balki texnik va ilmiy jihatdan ham katta talabchanlikni bildiradi. Shu nuqtai nazardan, bunday faoliyatda ehtiyotkorlik, muntazam metodologik yondoshuv va malakali mutaxassislar ishtiroki zarur.

Statistik ma’lumotlar shuni ko‘rsatadiki, raqamli jinoyatlar soni va ta’siri tez oshib bormoqda. Misol uchun, 2024 yilda kiberjinoyatlar natijasida dunyo bo‘yicha $16 milliarddan ortiq zarar bo‘lganligi FBI tomonidan bildirilgan. Bu raqam bir yil ichida 33% ga oshgani soha og‘irligining o‘sib borayotganini namoyon etadi. Bunday o‘sish raqamli kriminalistika sohasidagi bozor hajmiga ham ta’sir qilmoqda: Yevropada raqamli tergov (“digital forensics”) bozorining 2024 yilda qiymati taxminan 2,76 milliard USD bo‘lgan va 2025–2030 yillar oralig‘ida yillik o‘rtacha o‘sishi (CAGR) taxminan 14,4% ni tashkil etishi kutilmoqda. Bu tendensiyalar raqamli dalillarni to‘plash va ulardan foydalanishning ahamiyatini oshiradi. Agar dalillar noto‘g‘ri olinib yoki buzib yuborilsa, bu nafaqat tergov natijalariga salbiy ta’sir qiladi, balki qonuniy xatoliklarga va sudda rad etilishiga olib kelishi mumkin. Shu bois, raqamli tergovda ishlayotgan mutaxassislar yuqori malakaga ega bo‘lishi, zamonaviy uskunalar va ilg‘or texnologiyalardan foydalanish kerak.

Foydalanilgan adabiyotlar ro‘yxati

1. O‘zbekiston Respublikasi Prezidentining 2025 yil 30 aprel kungi PQ-153-son qarori
2. O‘zbekiston Respublikasi Jinoyat-protsessual kodeksi. — T.: Adolat, 2023.
3. “Axborot xavfsizligini ta’minlash to‘g‘risida”gi Qonun. — O‘zbekiston Respublikasi Qonun hujjatlari to‘plami, 2019-yil.
4. Federal Rules of Evidence (FRE). — United States Government Publishing Office, Washington D.C., 2020.
5. Electronic Communications Privacy Act (ECPA). — U.S. Code, Title 18, Chapter 121, 1986 (with amendments of 2022).
6. National Institute of Standards and Technology (NIST). — Guide to Integrating Forensic Techniques into Incident Response (SP 800-86). — Gaithersburg, MD: NIST, 2023.
7. U.S. Department of Justice. — Digital Evidence in the Courtroom: A Guide for Law Enforcement and Prosecutors. — Washington, D.C., 2022.
8. Rossiya Federatsiyasi Axborot xavfsizligi doktrinasi. — Moskva, 2021-yil 5-dekabr.
9. International Organization on Computer Evidence (IOCE). — Standards and Principles for the Handling of Digital Evidence. — Interpol Publication, Lyon, 2021.
10. Casey, Eoghan. — Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet. — Academic Press, 2022.
11. Kovalenko, V.V. — Sudebnaya kompyuternaya ekspertiza: teoriya i praktika. — Moskva: Yurayt, 2021