

KONFERENSIYALAR COM

ANJUMANLAR PLATFORMASI

**X RESPUBLIKA ILMIIY-
AMALIY KONFERENSIYASI**

**YANGI DAVR ILM-
FANI: INSON UCHUN
INNOVATSION G'OYA
VA YECHIMLAR**

MAY, 2026



ISSN 3093-8791

ELEKTRON NASHR:
<https://konferensiyalar.com>

KONFERENSIYALAR COM

ANJUMANLAR PLATFORMASI

**YANGI DAVR ILM-FANI:
INSON UCHUN INNOVATSION
G'OYA VA YECHIMLAR**

**X RESPUBLIKA ILMIY-AMALIY
KONFERENSIYASI MATERIALLARI**

2026-yil, may

TOSHKENT-2026

Yangi davr ilm-fani: inson uchun innovatsion g'oya va yechimlar.

X Respublika ilmiy-amaliy konferensiyasi materiallari to'plami.
2-jild, 10-son (may, 2026-yil).– 93 bet.

Mazkur nashr ommaviy axborot vositasi sifatida 2025-yil, 8-iyulda
C-5669862 son bilan rasman davlat ro'yaxatidan o'tkazilgan.

Elektron nashr: <https://konferensiyalar.com>

ISSN: 3093-8791 (onlayn)

Konferensiya tashkilotchisi: "Scienceproblems Team" MChJ

Konferensiya o'tkazilgan sana: 2026-yil, 26-may

Mas'ul muharrir:

Isanova Feruza Tulqinovna

Annotatsiya

Mazkur to'plamda "Yangi davr ilm-fani: inson uchun innovatsion g'oya va yechimlar" mavzusidagi X Respublika ilmiy-amaliy konferensiyasi materiallari jamlangan. Nashrda respublikaning turli oliy ta'lim muassasalari, ilmiy markazlari va amaliyotchi mutaxassislari tomonidan tayyorlangan maqolalar o'rin olgan bo'lib, ular ijtimoiy-gumanitar, tabiiy, texnik va yuridik fanlarning dolzarb muammolari va ularning innovatsion yechimlariga bag'ishlangan.

Ushbu nashr ilmiy izlanuvchilar, oliy ta'lim o'qituvchilari, doktorantlar va soha mutaxassislari uchun foydali qo'llanma bo'lib xizmat qiladi.

Kalit so'zlar: ilmiy-amaliy konferensiya, innovatsion yondashuv, zamonaviy fan, fanlararo integratsiya, ilmiy-tadqiqot, nazariya va amaliyot, ilmiy hamkorlik.

Barcha huquqlar himoyalangan.

© Scienceproblems team, 2026-yil

© Mualliflar jamoasi, 2026-yil

MUNDARIJA

TARIX FANLARI

Erkinov Alisher

BUXORO SHAHRINING TURAR-JOY MAHALLALARI, AHOLISI SONI VA
ETNIK TARKIBI (XIX ASR OXIRI – XX ASR BOSHLARI) 5-8

Sheripova Mahliyo

XIX ASR OXIRI – XX ASR BOSHLARIDA XIVA XONLIGINING MADANIY MUHITI VA
KOMIL XORAZMIY FENOMENI 9-14

Yusupov Xamdambek

XORIJ TARIXSHUNOSLIGIDA AFRIG'IYLLAR SULOLASINING KELIB CHIQISHI
MASALASI: YONDASHUVLAR VA QARASHLAR 15-19

Xo'jayeva Inobat

YANGI O'ZBEKISTON VA YUNESKO: MADANIY MEROS, TA'LIM VA
BARQAROR RIVOJLANISH SOHASIDAGI STRATEGIK HAMKORLIK 20-26

Abdullayeva Shoxnoza

XORAZM TANBUR CHIZIG'I — SHARQ MUSIQA MADANIYATIDA NOYOB
NOTA YOZUVI TIZIMI VA UNING TARIXIY AHAMIYATI 27-32

Xakimov Mansurbek

OROL FOJIASI – GLOBAL EKOLOGIK MUAMMO SIFATIDA 33-40

Xudoyorov Abrorjon

"XORAZM HAQIQATI" GAZETASIDA QISHLOQ MEHNAT AHLINING URUSH
YILLARIDAGI HAYOTI VA JASORATI MAVZUSINING YORITILISHI 41-43

Matchonova Nilufar

AMUDARYO HAVZASIDA IJTIMOYIY TARIX VA EKOLOGIK O'ZGARISHLARNING
O'ZARO TA'SIRI: EFTALIYLLAR DAVRI ANTROPOGEN LANDSHAFTLARI VA
SOTSIO-EKOLOGIK MOSLASHUV (V–VI ASRLAR) 44-49

IQTISODIYOT FANLARI

Иногамова Наира

ЦИФРОВИЗАЦИЯ КАК ФАКТОР УСКОРЕНИЯ ПРОГРЕССА ПО ЦЕЛЯМ
УСТОЙЧИВОГО РАЗВИТИЯ: ОПЫТ УЗБЕКИСТАНА 50-54

FILOLOGIYA FANLARI

Begmatova Diloromkhan

THE FUNCTIONAL ASPECT OF POLITICAL EUPHEMISMS IN DARI LANGUAGE
NEWSPAPER TEXTS 55-58

Akbarova Ma'suma

INGLIZ VA O'ZBEK TILLARIDA KIYIM-KECHAK LEKSIKASINING LINGVOMADANIY
TAHLILI 59-61

Isanova Feruza

O'ZBEK VA INGLIZ HUQUQIY DISKURSIDA MODALLIK IFODASI:
QIYOSIY-LINGVISTIK TAHLIL 62-67

YURIDIK FANLAR

Xushboqov Himoyiddin

KIBERJINOYATLARNI TERGOV QILISHDA RAQAMLI DALILLARNI AUTENTIFIKATSIYA
QILISHNING HUQUQIY MUAMMOLARI 68-74

PEDAGOGIKA FANLARI

Xaydarova Namunaxon

GEYMIFIKATSIYA TEXNOLOGIYASI ASOSIDA BO'LAJAK MAKTABGACHA TA'LIM
TARBIYACHILARINING KASBIY KOMPETENTLIGINI RIVOJLANTIRISH ZARURATI VA
UNING ILMIY-METODIK ASOSLARI 75-78

Gulamov Shavkat

TALABALARDA ILMIY DALILASH VA LOGIK ARGUMENTATSIYA QOBILIYATINI
RIVOJLANTIRISH 79-84

Yalgasheva Zilola

INKLYUZIV TA'LIM SHAROITIDA BO'LAJAK MAXSUS PEDAGOGLARNING
USLUBIY KOMPETENSIYASINI RIVOJLANTIRISH METODIKASI 85-87

Rasulova Dilafruzxon

XALQARO PEDAGOGIK ATAMALARNI O'QITISHDA KOMPETENSIYAVIY
YONDASHUVNING NAZARIY ASOSLARI 88-92

YURIDIK FANLAR

**KIBERJINOYATLARNI TERGOV QILISHDA RAQAMLI DALILLARNI
AUTENTIFIKATSIYA QILISHNING HUQUQIY MUAMMOLARI****Xushboqov Himoyiddin Abdivoid o'g'li**

Toshkent davlat yuridik universiteti

Kiber huquq yo'nalishi magistranti

Annotatsiya. Mazkur maqolada kiberjinoyatlarni tergov qilish jarayonida raqamli dalillarni autentifikatsiya qilishning huquqiy va kriminalistik muammolari qiyosiy-huquqiy tahlil asosida o'rganiladi. Tadqiqotda AQSH dalillar huquqidagi Federal Rules of Evidence qoidalari, Daubert va Frye standartlari, Yevropa elektron dalillar modeli, Budapesht konvensiyasining protsessual yondashuvi hamda O'zbekiston milliy amaliyoti o'zaro solishtiriladi. Maqolada autentifikatsiya raqamli dalilning manbasi, yaxlitligi, o'zgarmaganligi va jinoyat hodisasi bilan aloqadorligini tasdiqlovchi davomli protsessual-texnik jarayon sifatida talqin qilinadi. Raqamli dalillarning oson manipulyatsiyaga uchrashi, RAM kabi vaqtinchalik ma'lumotlarni asl nusxa bilan solishtirish qiyinligi, texnik vositalar xatosi va shaxsga bog'lashdagi murakkabliklar tahlil qilinadi. Yakunda O'zbekiston amaliyoti uchun raqamli dalillarni autentifikatsiya qilish bo'yicha yagona metodik standart, hash, forensic imaging va chain of custody mexanizmlarini mustahkamlash zarurligi asoslanadi.

Kalit so'zlar. raqamli dalillar, autentifikatsiya, kiberjinoyat, chain of custody, forensic imaging, hashing, Daubert standarti, Budapesht konvensiyasi.

**LEGAL ISSUES OF AUTHENTICATING DIGITAL EVIDENCE IN CYBERCRIME
INVESTIGATIONS: FOREIGN EXPERIENCE AND NATIONAL PRACTICE****Khushboqov Khimoyiddin Abdivoid ugli**

Tashkent State University of Law

Master's student in Cyber Law

Annotation. This article examines the legal and forensic problems of authenticating digital evidence in cybercrime investigations through a comparative legal analysis. The study compares the Federal Rules of Evidence, the Daubert and Frye standards, European approaches to electronic evidence, the procedural framework of the Budapest Convention and the national practice of Uzbekistan. Authentication is considered not as a single technical act, but as a continuous procedural and technical process aimed at proving the source, integrity, unchanged condition and relevance of digital evidence to the criminal event. The article analyzes the risks of manipulation, the difficulty of comparing volatile data such as RAM with an original source, errors arising from forensic tools and the problem of attributing digital activity to a specific person. The article concludes that Uzbekistan needs a unified methodological standard for authenticating digital evidence and a stronger practical use of hashing, forensic imaging and chain of custody mechanisms.

Keywords: digital evidence, authentication, cybercrime, chain of custody, forensic imaging, hashing, Daubert standard, Budapest Convention.

DOI: <https://doi.org/10.47390/ydif-y2026v2i10/n13>**Kirish**

Raqamli texnologiyalar jadal rivojlanishi natijasida jinoyatlarni sodir etish, yashirish va fosh etish usullari ham tubdan o'zgarimoqda. Bugungi kunda kiberjinoyatlar faqat kompyuter tizimlariga noqonuniy kirish yoki zararli dasturlar tarqatish bilan cheklanmay, balki bank-moliya operatsiyalari, shaxsga doir ma'lumotlar, elektron yozishmalar, ijtimoiy tarmoqlar, bulutli saqlash xizmatlari va kriptoaktivlar bilan bog'liq murakkab huquqiy munosabatlarni

ham qamrab olmoqda. Bunday jinoyatlarni tergov qilishda eng muhim masalalardan biri raqamli dalillarning haqiqiyligini, yaxlitligini va jinoyat hodisasi bilan real aloqadorligini isbotlashdir. Chunki raqamli dalil ko'rinishidan ishonchli bo'lib tuyulishi mumkin, biroq uning manbasi, yaratilish sharoiti, o'zgartirilgan yoki o'zgartirilmaganligi hamda kim tomonidan shakllantirilgani alohida tekshirilmasa, u sud jarayonida ishonchli dalil sifatida baholanishi qiyin.

Mavzuning dolzarbligi shundaki, raqamli dalillar an'anaviy dalillarga nisbatan oson o'zgartiriladigan, nusxalanadigan, ko'chiriladigan va soxtalashtiriladigan axborotdir. Elektron faylning tashqi ko'rinishi saqlanib qolgan bo'lsa ham, uning metadata qatlami, hash qiymati, yaratilish vaqti yoki manbasi o'zgartirilgan bo'lishi mumkin. Shu sababli raqamli dalillarni autentifikatsiya qilish oddiy texnik tekshiruv emas, balki jinoyat protsessi, dalillar nazariyasi, raqamli kriminalistika va xalqaro standartlar kesishgan murakkab huquqiy institut hisoblanadi. Black's Law Dictionary'da "authentication" dalil yoki hujjatning u da'vo qilinayotgan narsa ekanini tasdiqlash jarayoni sifatida izohlanadi [2; P. 154]. Raqamli dalillar kontekstida esa bu tushuncha yanada kengayib, ma'lumotning manbasi, yaxlitligi, o'zgarmaganligi va protsessual jihatdan maqbulligini ham qamrab oladi.

Maqolaning maqsadi kiberjinoyatlarni tergov qilishda raqamli dalillarni autentifikatsiya qilishning huquqiy muammolarini qiyosiy-huquqiy tahlil qilish, xorijiy tajriba va milliy amaliyotdagi asosiy farqlarni aniqlash hamda O'zbekiston uchun amaliy takliflar ishlab chiqishdan iborat. Ushbu maqsadga erishish uchun maqolada AQSH dalillar huquqi, Daubert va Frye standartlari, Yevropa yondashuvi, Budapesht konvensiyasi, texnik autentifikatsiya vositalari va O'zbekiston jinoyat-protsessual amaliyoti tahlil qilinadi.

Adabiyotlar sharhi va metodologiya

Tadqiqotda adabiyotlar sharhi, qiyosiy-huquqiy tahlil va tizimli tahlil metodlaridan foydalanildi. Adabiyotlar sharhi raqamli dalillar, elektron dalillar, raqamli kriminalistika va autentifikatsiya nazariyasiga oid ilmiy manbalarni o'rganishga qaratildi. Xususan, Eoghan Casey raqamli dalillarni nafaqat jinoyat hodisasini tasdiqlovchi axborot, balki dalilning kelib chiqishi va butun "hayotiy sikli" davomida o'zgarmaganligini isbotlashni talab qiluvchi kriminalistik obyekt sifatida talqin qiladi [3; P. 47]. Stephen Mason elektron dalillarni sudda baholashda ularning kelib chiqishi, ishonchligi va texnik shakllanish jarayoniga e'tibor qaratish zarurligini ko'rsatadi [13; Pp. 112–115].

Qiyosiy-huquqiy tahlil yordamida AQSH va Yevropa yondashuvlari o'zaro solishtirildi. AQSH tajribasida Federal Rules of Evidence qoidalari, xususan 901 va 902-moddalar, shuningdek Daubert va Frye standartlari muhim o'rin tutadi. Yevropa tajribasida esa Budapesht konvensiyasi, elektron dalillarni transchegaraviy olishga oid mexanizmlar hamda inson huquqlarini himoya qilish bilan bog'liq umumiy protsessual kafolatlar ustuvor ahamiyatga ega. Tizimli tahlil esa raqamli dalillarni autentifikatsiya qilishni alohida-alohida texnik harakatlar yig'indisi sifatida emas, balki aniqlash, to'plash, saqlash, tekshirish va sudda baholash bosqichlarini bog'laydigan yagona protsessual jarayon sifatida ko'rib chiqishga imkon berdi.

Maqolani nashr talablari asosida qayta ishlash jarayonida matndagi imlo, uslub, mantiqiy izchillik va manbalar bilan bog'liq kamchiliklar ham tuzatildi. Xususan, avvalgi variantda ayrim jumlar og'zaki uslubda tuzilgan, Daubert va Frye standartlari autentifikatsiyaga bevosita tatbiq etilgandek talqin qilingan, Budapesht konvensiyasining

ayrim normalari umumiyashtirilgan, O'zbekiston qonunchiligidagi so'nggi raqamli dalillar instituti yetarli aniqlikda ko'rsatilmagan edi. Yangi tahrirda ushbu jihatlar huquqiy aniqlik va ilmiy tahlil talablariga moslashtirildi.

Tahlil va natijalar

Autentifikatsiya raqamli dalilning u da'vo qilinayotgan manbadan kelib chiqqanligini, jinoyat hodisasi bilan aloqadorligini hamda tergov va sud bosqichlarida o'zgarmaganligini isbotlash jarayonidir. Raqamli dalilning haqiqiyliги faqat fayl nomi, ekranda ko'rinishi yoki foydalanuvchi tomonidan taqdim etilishi bilan belgilanmaydi. Uning haqiqiyliğini aniqlash uchun manba, yaratilish sharoiti, metadata, hash qiymati, olingan usul, chain of custody va ekspertiza natijalari o'zaro bog'liq holda baholanishi kerak. Grimm, Capra va Joseph raqamli dalillarni autentifikatsiya qilishda sudlar texnik ma'lumotlar, tizim yozuvlari, guvoh ko'rsatmalari, sertifikatlar va ekspert xulosalarini birgalikda baholashi mumkinligini ta'kidlaydi [10; Pp. 1–58].

Raqamli dalillarni autentifikatsiya qilish bir martalik harakat emas. Dalil birinchi marta aniqlangan paytdan boshlab sudga taqdim etilgunga qadar u bilan bajarilgan har bir harakat autentifikatsiya qiymatiga ta'sir qiladi. Masalan, mobil telefondan olingan yozishma skrinshot shaklida taqdim etilgan bo'lsa, bu skrinshotning o'zi yetarli bo'lmasligi mumkin. Uning qaysi qurilmadan, qaysi akkauntidan, qaysi vaqtda olingani, yozishmaning to'liq konteksti, platforma ma'lumotlari, metadata va zarur hollarda provayderdan olingan rasmiy qaydlar bilan tasdiqlanishi talab etiladi. Shuning uchun autentifikatsiya texnik dalilni "haqiqiy" deb e'lon qilish emas, balki ushbu haqiqiylikni protsessual va kriminalistik jihatdan isbotlash jarayonidir.

An'anaviy dalillarda autentifikatsiya ko'pincha vizual tekshiruv, guvoh ko'rsatmasi yoki ekspert xulosasi bilan cheklanishi mumkin. Raqamli muhitda esa bu yetarli emas. Chunki elektron ma'lumotlar tashqi ko'rinishi o'zgarmagan holda ham ichki tuzilishi bo'yicha manipulyatsiya qilinishi mumkin. Orin Kerr raqamli muhitda qidiruv va olib qo'yishning murakkabligi shundaki, kompyuter xotirasida katta hajmdagi shaxsiy va ishga aloqador ma'lumotlar birga saqlanishi, ularni ajratish esa an'anaviy predmetlar bilan ishlashdan farqli yondashuv talab qilishini qayd etadi [12; Pp. 531–585]. Bu fikr autentifikatsiya masalasiga ham tegishli: raqamli dalilning haqiqiyliğini aniqlashda uning ko'rinadigan mazmuni bilan birga texnik qatlamini ham tekshirish zarur.

AQSH huquqiy tizimida raqamli dalillarni autentifikatsiya qilish, avvalo, Federal Rules of Evidence qoidalari bilan bog'liq. FRE 901(a) dalilni sudqa qabul qilish uchun uni taqdim etayotgan tomon dalil aynan o'zi da'vo qilayotgan narsa ekanini ko'rsatishi kerakligini belgilaydi. FRE 901(b)(9) esa jarayon yoki tizim natijasini autentifikatsiya qilish uchun ushbu jarayon yoki tizim ishonchli natija berishini ko'rsatishga imkon beradi. Raqamli dalillar kontekstida bu server loglari, avtomatik tizim yozuvlari, elektron ma'lumotlar bazasi yoki forensik dastur natijalari qanday shakllanganini tushuntirish zarurligini anglatadi [7; Rules 901(a), 901(b)(9)].

FRE 902 qoidalari ayrim elektron dalillarni soddalashtirilgan tartibda autentifikatsiya qilish imkoniyatini beradi. Xususan, 902(13) va 902(14) qoidalari elektron jarayon orqali yaratilgan yozuvlar hamda elektron qurilmadan olingan tasdiqlangan nusxalarni sertifikat asosida o'z-o'zini autentifikatsiya qiluvchi dalil sifatida qabul qilishga yo'l ochadi [7; Rules 902(13)–902(14)]. Bu mexanizm amaliyotda muhim, chunki har bir server logi yoki forensik

nusxa uchun alohida guvoh chaqirish zaruratini kamaytiradi. Shu bilan birga, sertifikatlash mexanizmi dalilning avtomatik ravishda maqbul bo'lishini anglatmaydi; u faqat autentifikatsiya bosqichini yengillashtiradi, dalilning ishga aloqadorligi va ishonchligi esa alohida baholanadi.

Daubert va Frye standartlari raqamli dalillarni autentifikatsiya qilishda bevosita dalilning o'ziga emas, balki ko'proq ekspert metodologiyasi va ilmiy-texnik usullarni baholashga xizmat qiladi. Frye standarti ilmiy usul tegishli sohada umumiy qabul qilingan bo'lishini talab qilgan bo'lsa [8], Daubert standarti ekspert usulining tekshiriluvchanligi, xatolik ehtimoli, peer reviewdan o'tganligi va ilmiy hamjamiyatda qabul qilinganligini baholash mezonlarini shakllantirdi [6]. Raqamli dalillar bo'yicha bu shuni anglatadiki, forensik imaging, hash, metadata tahlili yoki zararli dastur ekspertizasi natijalari sudda ishonchli bo'lishi uchun qo'llangan metodika ilmiy jihatdan asoslangan va qayta tekshiriladigan bo'lishi kerak.

Raqamli dalillarni autentifikatsiya qilishda texnik vositalar alohida ahamiyatga ega. Forensic imaging, ya'ni kriminalistik nusxa olish, raqamli tashuvchidagi ma'lumotlarni imkon qadar o'zgartirmasdan saqlab qolish imkonini beradi. ISO/IEC 27037:2012 raqamli dalillarni identifikatsiya qilish, yig'ish, olish va saqlash jarayonlarida dalilning yaxlitligi va ishonchligini ta'minlashga qaratilgan yo'riqnomaviy standart sifatida ahamiyatlidir [11; 5–7-bandlar]. Ushbu standartning amaliy qiymati shundaki, u raqamli dalilni oddiy fayl sifatida emas, balki protsessual ahamiyatga ega bo'lgan elektron axborot sifatida himoya qilishni talab qiladi.

Hash qiymati autentifikatsiya jarayonida raqamli dalilning o'zgartirilmaganligini tekshirishga xizmat qiladi. Hash algoritmi ma'lumotga matematik funksiya qo'llash orqali o'ziga xos qiymat hosil qiladi. Agar fayl yoki forensik nusxa biror darajada o'zgarsa, hash qiymati ham o'zgaradi. Stallings kriptografik hash funksiyalar ma'lumot yaxlitligini tekshirish va autentifikatsiya qilishda muhim rol o'ynashini ko'rsatadi [17; Pp. 354–358]. Biroq hash algoritmlarining o'zi ham doimo tanqidiy baholanishi kerak. Masalan, Wang va hammualliflar MD5 kabi ayrim hash algoritmlarining kolliziya zaifliklarini ko'rsatgan [18; Pp. 19–35]. Shuning uchun amaliyotda eskirgan algoritmlardan emas, zamonaviy va ishonchli hash standartlaridan foydalanish zarur.

Chain of custody raqamli dalilning aniqlangan paytdan sudga taqdim etilgungacha bo'lgan harakat yo'lini uzluksiz hujjatlashtirish tizimidir. U dalil kim tomonidan, qachon, qayerda, qanday usulda olingani, qayerda saqlangani, kimga topshirilgani va qanday tahlil qilingani haqidagi ma'lumotlarni qamrab oladi. Ballou tahriri ostidagi elektron jinoyat joyini tekshirish bo'yicha qo'llanmada birinchi javob beruvchilar uchun elektron qurilmalarni hujjatlashtirish, joylashuvini qayd etish va keyingi ekspertiza uchun zarar yetkazmasdan saqlash alohida talab sifatida ko'rsatiladi [1; P. 29]. Demak, chain of custody autentifikatsiyaning yordamchi elementi emas, balki raqamli dalilning butun isbotlash qiymatini saqlab turuvchi asosiy mexanizmdir.

Budapesht konvensiyasi kiberjinoyatchilikka qarshi kurashish va elektron shakldagi dalillarni to'plash bo'yicha xalqaro hamkorlikning asosiy huquqiy manbalaridan biridir. Konvensiyaning 7-moddasi kompyuter bilan bog'liq soxtalashtirishni kriminalizatsiya qilishga qaratilgan bo'lib, raqamli muhitda haqiqiydek ko'rinadigan, biroq yuridik maqsadlarda noto'g'ri foydalanilishi mumkin bo'lgan ma'lumotlar xavfini e'tirof etadi [4; Article 7]. Shu

bilan birga, raqamli dalillarni olish va saqlash bo'yicha konvensiyaning 14–19-moddalari protsessual vakolatlar, saqlangan kompyuter ma'lumotlarini tezkor saqlash, production order, tintuv va olib qo'yish kabi mexanizmlarni belgilaydi [4; Articles 14–19].

Konvensiyaning mazmunidan kelib chiqadigan muhim xulosa shundaki, autentifikatsiya faqat dalil sudga keltirilgan paytda emas, balki uni olish va saqlash bosqichidayoq boshlanadi. Agar dalilning kelib chiqishi, yaxlitligi va saqlash tartibi dastlabki bosqichda to'g'ri mustahkamlanmasa, keyingi bosqichda uni haqiqiy deb isbotlash murakkablashadi. Konvensiya izohli hisobotida saqlangan kompyuter ma'lumotlarini saqlab qo'yish va keyinchalik oshkor qilish o'rtasidagi farq tushuntiriladi; bu farq raqamli dalillarning tez yo'qolishi yoki o'zgarishi mumkin bo'lgan sharoitda ayniqsa muhimdir [5; paras. 155–170].

Yevropa Ittifoqi tajribasida elektron dalillarni transchegaraviy olish masalasi ham alohida rivojlanmoqda. Regulation (EU) 2023/1543 elektron dalillar bo'yicha European Production Order va European Preservation Order mexanizmlarini belgilaydi [15; Article 1]. Ushbu modelning ilmiy-amaliy ahamiyati shundaki, u elektron dalilni saqlab qo'yish va taqdim etish jarayonlarini alohida bosqich sifatida ko'radi. O'zbekiston amaliyoti uchun ham bunday ikki bosqichli yondashuv muhim: avvalo dalilni yo'qolishdan saqlash, keyin esa uni qonuniy tartibda olish va autentifikatsiya qilish.

O'zbekiston Respublikasida raqamli dalillar instituti so'nggi yillarda protsessual jihatdan aniqroq tartibga solina boshladi. Jinoyat-protsessual kodeksga raqamli dalillar, elektron ma'lumotlar, ularni olish, saqlash va ish materiallariga qo'shishga oid maxsus qoidalar kiritilgan. Xususan, elektron ma'lumotlar va raqamli dalillar tushunchasi alohida ko'rsatilgani milliy tizim uchun muhim ijobiy qadamdir [14; 204¹–204²-moddalar]. Biroq autentifikatsiya masalasi hali ham yagona metodik standart darajasida to'liq ishlab chiqilmagan. Ya'ni raqamli dalil tan olingan bo'lsa-da, uning haqiqiylikni isbotlashda qaysi texnik va protsessual mezonlar majburiy qo'llanishi kerakligi amaliyotda har doim bir xil emas.

Milliy amaliyotdagi birinchi muammo raqamli dalilni asl nusxa bilan solishtirishning doimo ham imkoni yo'qligidir. Masalan, RAMdan olingan ma'lumotlar doimiy saqlanmaydi; ular qurilma o'chirilishi bilan yo'qolishi mumkin. Bunday ma'lumotlar "snapshot" xususiyatiga ega bo'lib, keyinchalik aynan o'sha holatni qayta tiklash qiyin. Shu bois RAM, cache, faol jarayonlar yoki tarmoq ulanishlari kabi vaqtinchalik ma'lumotlar bilan ishlashda autentifikatsiya dalilning asl nusxasini saqlashga emas, balki olish jarayonining to'g'ri hujjatlashtirilishi, hash qiymatlari, video/foto qaydlar va mutaxassis izohlariga tayanadi.

Ikkinchi muammo raqamli ma'lumotlarning manipulyatsiyaga oson uchrashidir. Elektron yozishma, skrinshot, audio-video fayl yoki metadata maxsus dasturlar yordamida o'zgartirilishi mumkin. Roth "machine testimony" konsepsiyasi orqali avtomatlashtirilgan tizimlar va mashina tomonidan yaratilgan ma'lumotlar sudda qanday ishonchlilik mezonlari asosida baholanishi kerakligi masalasini ko'taradi [16; Pp. 1972–2043]. Bu masala raqamli dalillar uchun dolzarb: sud va tergov organlari faqat inson guvohligiga emas, balki tizimlar, algoritmlar va qurilmalar yaratgan yozuvlarga ham baho berishga majbur bo'lmoqda.

Uchinchi muammo texnik vositalar va abstraksiya xatolari bilan bog'liq. Raqamli dalillarni inson bevosita ko'rmaydi; ularni operatsion tizimlar, maxsus forensik dasturlar, tahlil modullari va hisobotlar orqali idrok qiladi. Shu sababli dasturiy vositadagi xato, noto'g'ri

konfiguratsiya, eskirgan versiya yoki noto'g'ri metodika dalilning mazmunini buzib ko'rsatishi mumkin. Garfinkel raqamli forensika tadqiqotlarining keyingi bosqichida katta hajmdagi ma'lumotlar, avtomatlashtirish, vositalar ishonchliligi va standartlashtirish masalalari tobora muhim bo'lishini ta'kidlaydi [9; Pp. S64–S73].

To'rtinchi muammo raqamli harakatni aniq shaxsga bog'lash masalasidir. Kompyuter yoki akkaunddagi harakat ma'lum bir login orqali amalga oshirilgan bo'lsa ham, bu harakatni aynan bir shaxs sodir etganini avtomatik isbotlamaydi. Parol boshqa shaxs tomonidan ishlatilgan, qurilmadan bir nechta odam foydalangan, akkaunt buzib kirilgan yoki zararli dastur orqali masofadan boshqarilgan bo'lishi mumkin. Shuning uchun autentifikatsiya faqat "fayl bor" yoki "akkaunt dan yuborilgan" degan fakt bilan cheklanmasligi kerak. IP-manzil, geolokatsiya, qurilma identifikatori, foydalanuvchi odatlari, vaqt oralig'i, biometrik yoki boshqa qo'shimcha ko'rsatkichlar birgalikda baholanishi lozim.

Beshinchi muammo kadrlar malakasi va yagona metodik yo'riqnomalar yetishmasligidir. Raqamli dalillarni autentifikatsiya qilishda tergovchi, mutaxassis, ekspert, prokuror va sudyaning hammasi ma'lum darajada raqamli kriminalistika savodxonligiga ega bo'lishi kerak. Agar tergovchi dalilni olishda xato qilsa, ekspert keyinchalik uni to'liq tiklay olmasligi mumkin; agar sudya hash, metadata yoki chain of custody mohiyatini tushunmasa, dalilni noto'g'ri baholashi mumkin. Shuning uchun milliy amaliyotda raqamli dalillarni autentifikatsiya qilish bo'yicha yagona metodik standart, mutaxassislar uchun malaka talablari va sud-tergov xodimlari uchun maxsus o'quv dasturlarini ishlab chiqish zarur.

Tahlil natijasida quyidagi amaliy takliflarni ilgari surish mumkin. Birinchidan, raqamli dalillarni autentifikatsiya qilish bo'yicha milliy metodik standart ishlab chiqilishi lozim. Unda raqamli dalilni aniqlash, olish, forensic imaging, hash qiymatini hisoblash, chain of custody yuritish, metadata tahlili, skrinshot va ijtimoiy tarmoq kontentini mustahkamlash, ekspertiza materiallarini rasmiylashtirish kabi bosqichlar aniq ko'rsatilishi kerak. Ikkinchidan, sud amaliyotida FRE 901 va 902 qoidalariga o'xshash tarzda elektron tizimlar orqali yaratilgan yozuvlarni autentifikatsiya qilish mezonlari ishlab chiqilishi mumkin. Bunda har bir dalil uchun alohida guvoh talab qilish o'rniga, sertifikatlash, ekspert xulosasi va texnik hujjatlar orqali dalilning haqiqiylikini tasdiqlash mexanizmi yo'lga qo'yilishi maqsadga muvofiq.

Uchinchidan, raqamli dalillar bo'yicha ekspert metodologiyasini baholashda Daubert mezonlariga o'xshash ilmiy tekshiruvchanlik, xatolik ehtimoli, qayta takrorlash imkoniyati va ekspert hamjamiyatida qabul qilinganlik kabi mezonlar qo'llanishi zarur. To'rtinchidan, hash algoritmlari bo'yicha eskirgan texnologiyalardan voz kechilib, zamonaviy va ishonchli algoritmlardan foydalanish tavsiya etiladi. Beshinchidan, raqamli dalillarni shaxsga bog'lashda yagona indikatorga emas, balki texnik va kontekstual dalillar majmuiga tayanish lozim. Oltinchidan, tergovchi, mutaxassis, ekspert va sudyalarning uchun raqamli dalillarni autentifikatsiya qilish bo'yicha maxsus treninglar tashkil etilishi kerak.

Xulosa

Raqamli dalillarni autentifikatsiya qilish kiberjinoyatlarni tergov qilishda dalilning haqiqiylik, ishonchliligi va sudda maqbulligini ta'minlaydigan asosiy huquqiy-kriminalistik mexanizmdir. Tadqiqot shuni ko'rsatadiki, autentifikatsiya faqat texnik jarayon emas; u dalilning manbasini aniqlash, yaxlitligini saqlash, o'zgartirilmaganligini isbotlash, chain of custody yuritish, ekspert metodologiyasini baholash va protsessual kafolatlarini ta'minlashdan iborat kompleks institutdir. AQSH tajribasi raqamli dalillarni autentifikatsiya qilishda aniq

dalillar qoidalari va ekspert standartlariga tayansa, Yevropa yondashuvi xalqaro hamkorlik, inson huquqlari va protsessual muvozanatga ko'proq urg'u beradi. O'zbekiston uchun esa har ikki tajribaning maqbul jihatlari milliy qonunchilik va tergov amaliyoti sharoitiga moslashtirish muhimdir.

Milliy amaliyotda raqamli dalillar instituti shakllanayotgan bo'lsa-da, autentifikatsiya bo'yicha yagona metodik standart, hash va forensic imagingdan foydalanish qoidalari, chain of custody jadvali, ekspert metodologiyasini baholash mezonlari va kadrlar malakasi bo'yicha tizimli talablar yetarli darajada rivojlantirilishi zarur. Faqat shundagina raqamli dalillar kiberjinoyatlarni fosh etishda samarali vosita bo'lishi bilan birga, odil sudlov, shaxs huquqlari va dalillar maqbulligi kafolatlariga ham xizmat qiladi.

Adabiyotlar/Литература/References:

1. Ballou, S. (ed.). *Electronic Crime Scene Investigation: A Guide for First Responders*. 2nd ed. Washington, D.C.: U.S. Department of Justice / NIJ, 2008. P. 29.
2. *Black's Law Dictionary*. 11th ed. St. Paul: Thomson Reuters, 2019. P. 154.
3. Casey, E. *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet*. 3rd ed. Amsterdam: Academic Press / Elsevier, 2011. Pp. 47–53.
4. Council of Europe. *Convention on Cybercrime (ETS No. 185)*. Budapest, 23 November 2001. Articles 7, 14–19.
5. Council of Europe. *Explanatory Report to the Convention on Cybercrime*. Strasbourg: Council of Europe, 2001. Paras. 155–170, 177–186.
6. *Daubert v. Merrell Dow Pharmaceuticals, Inc.*, 509 U.S. 579 (1993).
7. *Federal Rules of Evidence*. Rules 901, 902. Legal Information Institute, Cornell Law School, 2024. URL: <https://www.law.cornell.edu/rules/fre>.
8. *Frye v. United States*, 293 F. 1013 (D.C. Cir. 1923).
9. Garfinkel, S. *Digital Forensics Research: The Next 10 Years*. *Digital Investigation*, 2010, Vol. 7 (Suppl.). Pp. S64–S73.
10. Grimm, P. W., Capra, D. J., Joseph, G. P. *Authenticating Digital Evidence*. *Baylor Law Review*, 2017, Vol. 69, No. 1. Pp. 1–58.
11. *ISO/IEC 27037:2012. Information Technology — Security Techniques — Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence*. Geneva: ISO, 2012.
12. Kerr, O. S. *Searches and Seizures in a Digital World*. *Harvard Law Review*, 2005, Vol. 119, No. 2. Pp. 531–585.
13. Mason, S. (ed.). *Electronic Evidence*. 4th ed. London: LexisNexis, 2017. Pp. 112–115.
14. O'zbekiston Respublikasi Jinoyat-protsessual kodeksi. 204¹–204²-moddalar.
15. Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for Electronic Evidence in Criminal Proceedings. OJ L 191, 28.7.2023. Pp. 118–178.
16. Roth, A. *Machine Testimony*. *Yale Law Journal*, 2017, Vol. 126, No. 6. Pp. 1972–2043.
17. Stallings, W. *Cryptography and Network Security: Principles and Practice*. 7th ed. Hoboken: Pearson, 2017. Pp. 354–358.
18. Wang, X. et al. *How to Break MD5 and Other Hash Functions*. *Advances in Cryptology – EUROCRYPT 2005*. LNCS 3494. Berlin: Springer, 2005. Pp. 19–35.

YANGI DAVR ILM-FANI: INSON UCHUN INNOVATSION G'OYA VA YECHIMLAR

X RESPUBLIKA ILMIY-AMALIY KONFERENSIYASI MATERIALLARI

2026-yil, may

Mas'ul muharrir: *F.T.Isanova*
Texnik muharrir: *N.Bahodirova*
Diszayner: *I.Abdihakimov*

Yangi davr ilm-fani: inson uchun innovatsion g'oya va yechimlar.
X Respublika ilmiy-amaliy konferensiyasi materiallari to'plami.
2-jild, 10-son (may, 2026-yil). – 93 bet.

Mazkur nashr ommaviy axborot vositasi sifatida 2025-yil, 8-iyulda
C-5669862 son bilan rasman davlat ro'yaxatidan o'tkazilgan.

ISSN: 3093-8791 (onlayn)

Elektron nashr: <https://konferensiyalar.com>

Konferensiya tashkilotchisi: "Scienceproblems Team" MChJ

Konferensiya o'tkazilgan sana: 2026-yil, 26-may

Barcha huquqlar himoyalangan.
© Science problems team, 2026-yil.
© Mualliflar jamoasi, 2026-yil.