pISSN:2349-5707 Volume:13,Issue 3, March -2026 eISSN:2349-5715

MODERN FORENSIC METHODS FOR IDENTIFYING AND ANALYZING DIGITAL EVIDENCE

Saidaminxoja Abdazimov
Teacher at the Digital Technologies and Information Security of the Academy of the Ministry of Internal Affairs of the Republic of Uzbekistan
Dzhamatov Mustafa
Teacher at the Digital Technologies and Information Security of the Academy of the Ministry of Internal Affairs of the Republic of Uzbekistan

Annotation

This article examines the forensic significance of digital evidence in the context of the rapid development of digital technologies, as well as modern approaches to its identification, acquisition, and analysis. The possibilities of applying digital information in investigative activities are considered based on its legal status, carriers, and functional characteristics. In addition, improved methods for the classification of digital evidence, as well as effective mechanisms for its storage and forensic examination, are analyzed. The article highlights the practical aspects of working with digital information in the context of modern cybersecurity and proposes scientific and practical recommendations aimed at increasing the effectiveness of investigations.

Keywords

digital evidence, forensics, digital forensics, information security, cybersecurity, digital information, data analysis, digital traces, data retrieval.

RAQAMLI DALILLARNI ANIQLASH VA TAHLIL QILISHNING ZAMONAVIY KRIMINALISTIK USULLARI

Annotatsiya

Mazkur maqolada raqamli texnologiyalar keng rivojlanayotgan sharoitda raqamli dalillarning kriminalistik ahamiyati hamda ularni aniqlash, olish va tahlil qilishning zamonaviy yondashuvlari tadqiq etiladi. Raqamli axborotning huquqiy maqomi, uning tashuvchilari va funksional xususiyatlari asosida tergov jarayonida qo‘llash imkoniyatlari ko‘rib chiqilgan. Shuningdek, raqamli dalillarni klassifikatsiyalashning takomillashtirilgan usullari hamda ularni saqlash va ekspertiza qilishning samarali mexanizmlari tahlil etiladi. Maqolada zamonaviy kiberxavfsizlik sharoitida raqamli axborot bilan ishlashning amaliy jihatlari yoritilib, tergov samaradorligini oshirishga qaratilgan ilmiy-amaliy tavsiyalar ishlab chiqilgan.

Kalit so‘zlar

raqamli dalillar, kriminalistika, raqamli ekspertiza, axborot xavfsizligi, kiberxavfsizlik, raqamli axborot, ma’lumotlar tahlili, raqamli izlar, ma’lumotlarni izlash

Аннотация

В данной статье исследуется криминалистическое значение цифровых доказательств в условиях широкого развития цифровых технологий, а также современные подходы к их выявлению, изъятию
и анализу. Рассматриваются возможности применения цифровой информации
в следственной деятельности на основе её правового статуса, носителей
и функциональных характеристик. Кроме того, анализируются усовершенствованные

pISSN:2349-5707 Volume:13,Issue 3, March -2026 eISSN:2349-5715

методы классификации цифровых доказательств,
а также эффективные механизмы их хранения и проведения экспертизы.
В статье освещаются практические аспекты работы с цифровой информацией в условиях современной кибербезопасности и разработаны научно-практические рекомендации, направленные на повышение эффективности расследования.

Ключевые слова

цифровые доказательства, криминалистика, цифровая экспертиза, информационная безопасность, кибербезопасность, цифровая информация, анализ данных, цифровые следы, поиск данных.

Bugungi kunda jamiyat rivoji tobora raqamli texnologiyalar bilan uzviy bog‘liq bo‘lib bormoqda. An’anaviy ijtimoiy va huquqiy munosabatlar ko‘plab sohalarda zamonaviy axborot texnologiyalari orqali amalga oshirilmoqda. Shu bilan birga, mavjud huquqiy tartibga solish mexanizmlari texnologik yangiliklarning tezkor rivojiga yetib bora olmayapti, bu esa raqamli axborot bilan ishlashda ayrim muammolarni yuzaga keltirmoqda. Shu sababli raqamli dalillarni aniqlash, olish va tahlil qilish jarayonlari uchun samarali kriminalistik yondashuvlarni ishlab chiqish dolzarb hisoblanadi. Bundan tashqari, sun’iy intellekt va mashinaviy o‘rganish texnologiyalari raqamli dalillarni tezkor va ishonchli tahlil qilish imkoniyatlarini kengaytirmoqda, bu esa kiberjinoyatlar bilan kurashishda yangi imkoniyatlar yaratadi.

Kompyuter ma’lumotlarini kriminalistik klassifikatsiyalash muammolari sud ekspertlari tomonidan bir necha bor qayta ko‘rib chiqilgan. Masalan, **V.Vexov,** kriminalistik nuqtai nazaridan, kompyuter ma’lumotlarini quyidagi asoslarga ko‘ra guruhlarga ajratishni taklif qildi:

1) hujjatlashtirilgan va hujjatlashtirilmagan –huquqiy maqomga ko‘ra;
2) ruxsat borligi kategoriyasiga ko‘ra - umumiy foydalanishga ruxsat berilgan axborot (cheklanmagan ruxsat bilan) va ularga kirish davlat qonunlariga muvofiq cheklangan, himoya qilinadigan kompyuter ma’lumotlari;
3) taqdim etilish shakliga ko‘ra – EHM uchun elektromagnit tebranishlar (to‘lqinlar) va buyruqlar, fayllar va kompyuter dasturlarida axborotni elektromagnit signallar yordamida fazoda va vaqt oralig‘ida yuborish imkonini beradi.

Bugungi kunda raqamli dalillar bilan ishlash jarayonida sun’iy intellekt va mashinaviy o‘rganish texnologiyalarining o‘rni tobora ortib bormoqda. Ushbu texnologiyalar katta hajmdagi ma’lumotlarni tezkor tahlil qilish, shubhali faoliyatni aniqlash hamda raqamli izlarni avtomatik ravishda saralash imkonini beradi. Ayniqsa, kiberjinoyatlarni aniqlashda log fayllar, tarmoq trafiklari va foydalanuvchi faoliyatini monitoring qilishda intellektual tizimlardan foydalanish yuqori samaradorlikni ta’minlamoqda.

Kompyuter huquqshunosligi va noqonuniy turdagi tergov ishlarida kompyuter axborotidan foydalanish sohasidagi yetakchi olim Kris Rid kompyuter axborotlarini asosiy 6 turga bo‘lishni taklif etdi: birlamchi ma’lumotlar (raw data); ma’lumotlar ombori (databases); elektron axborotni rasshifrovka qilish uchun kodlar (codes necessary to inteipret computer information); dasturlash algoritmlari va ma’lumotlarni qayta ishlash algoritmlari; tijoriy ko‘rinishdagi dasturiy ta’minot (commercial software); kompyuter tizimlari (computer systems).

Yuqorida ta’kidlanganidek, kompyuter ma’lumotlari raqamli axborotning umumiy miqdorining bir qismi hisoblanadi. Ma’lum bo‘ladiki, har qanday raqamli axborotni klassifikatsiyalash tizimlari taklif etilmasin, ularning hammasi shartli bo‘ladi va bu odatda bu axborot manbalarining barcha xususiyatlarini to‘liq aks ettirmaydi.

Shu bilan birga, taklif etilgan klassifikatsiyalash tizimlari jinoiy- protsessual kodeksga mos isboti talab etiladigan jinoiy ishlarning dastlabki tergov va sud surishtiruvlari qo‘yadigan talablarni maksimal ravishda qondiradi.

pISSN:2349-5707 Volume:13,Issue 3, March -2026 eISSN:2349-5715

Turli xil mualliflarning ilgari tavsiya etgan kompyuter ma'lumotlarini tasniflash sxemalari yoki mazmunga ega bo'lmagan guruhlarga bo'lingan yoki ular turli xil jinoyatlar bo'yicha kriminalistik tergovlarida raqamli axborotni aniqlash, olib qo'yish, belgilash va ulardan foydalanishning barcha jihatlarini hisobga olmaydi.

Taklif etilgan raqamli axborotni kriminalistik klassifikatsiyalashning asosiy maqsadi ushbu axborot manbalari guruhini izlash uchun mumkin bo'lgan eng aniq yo'nalishlarni aniqlash imkonini beradi; raqamli axborotni izlash, chiqarish, saqlash va h.k.lar uchun maxsus taktikalarni ishlab chiqish; dastlabki tergovning samaradorligini sezilarli darajada oshiradi va jinoyat ishlarini uni qo'llashga asoslangan holda ko'rib chiqadi.

Yuqorida qayd etilganlarni hisobga olib, shuningdek jinoyatlar tergovini kriminalistik tashkil etishni ta'minlash, uning paydo bo'lishi yoki paydo bo'lishi manbalari, joylashuvi, yaxlitligi yoki fragmentarligi va boshqa xususiyatlarini hisobga olgan holda raqamli axborotning funksional va axborot qiymatini hisobga olgan holda quyidagi raqamli axborotni klassifikatsiyalash tizimlari taklif etiladi.

Raqamli axborotni tashuvchi vositalar turlariga ko'ra klassifikatsiyalash. Ushbu klassifikatsiya doirasida, birinchi navbatda, raqamli axborot mustaqil raqamli texnikaning ishlash jarayonida energiya manbayiga ega tashuvchi vositalariga va mustaqil energiya manbaiga egaligiga qarab tuslanadi. Bu kabi klassifikatsiya raqamli axborotni chiqarib olishga sezilarli darajada ta'sir ko'rsatadi.

Raqamli texnologiyalar vositalariga apparat ulash mashinalari vositasida raqamli axborotni klassifikatsiyalash. Ushbu tasniflash sxemasi doirasida to'rtta kichik guruhni ajratish mumkin: birinchi kichik guruh - raqamli texnologiya vositalariga kiritilgan "qattiq" tarzda saqlanadigan ma'lumotlar, ya'ni tezkor xotira (RAM), doimiy xotira (ROM) va raqamli asbob-uskunalarning elektron plitalarining ajralmas qismi bo'lganlari; ikkinchi kichik guruhga raqamli uskunada o'rnatiladigan mashinada saqlovchi qurilmalarda saqlanadigan ma'lumot nazarda tutiladi, ammo raqamli uskunalarning yaxlitligiga zarar yetkazmasdan osongina olib tashlanishi yoki o'zgartirilishi mumkin bo'ladi; uchinchi kichik guruhga mashinada saqlovchi qurilmalardagi ma'lumotlarini ro'yxatga olish/o'qish moslamalari (flopping disklari, optik mashinada saqlovchi qurilmalar, flesh-kartalar va hokazolar), shuningdek portlar orqali raqamli qurilmaga ulangan tashqi saqlovchi qurilmalarda magnit disklar yoki qattiq qatlamli disklarda; to'rtinchi kichik guruhga lokal, mintaqaviy yoki global axborot kommunikatsiya tarmoqlariga kiruvchi mashinaviy tarzda tashuvchi qurilmalarga biriktirilgan.

Raqamli axborotning joylashuvi klassifikatsiyasiga qarab quyidagi guruhlarga bo'linadi: birinchi guruh – mashinaviy tashuvchi vositalar va aniq

jismoniy yoki yuridik shaxsga tegishli bo'lgan, joylashuvi oldindan aniq bo'lgan raqamli texnikaga ulangan yoki ulana oladigan mashinaviy qurilmalardagi axborot; ikkinchi guruhga – davlat hududida joylashgan mashinaviy tashuvchi qurilmalarda joylashgan (ulangan) korporativ axborot- kommunikatsiya tarmoq foydalanuvchilarining axboroti kiritiladi; uchinchi guruhga – davlat hududidan tashqarida joylashgan mashinaviy tashuvchi qurilmalarda joylashgan (ulangan) lokal, mintaqaviy yoki global axborot- kommunikatsiya tarmoqlardagi foydalanuvchilar uchun ruxsat mavjud bo'lgan axborot kiritiladi.

Raqamli axborotni funksional va informativ maqsadiga ko'ra quyidagi 5 guruhga bo'lish mumkin:

- raqamli qurilmalar dasturiy ta'minoti;
- elektron hujjatlar;
- ma'lumotlar bazalari;
- mashina tashuvchilari haqida boshqa ma'lumotlar.

pISSN:2349-5707 Volume:13,Issue 3, March -2026 eISSN:2349-5715

Oxirgi guruhga tizim va xizmat fayllari, jurnal fayllari, log fayllar va boshqalardagi ma’lumotlar kiritiladi.

Raqamli texnologiyalarni qo‘llash dasturlarining kriminalistik tasnifi doirasida bir necha asosiy kichik guruhlar mavjud. Birinchisi, raqamli uskunalarni (asosiy kirish-chiqish tizimlari, operatsion tizimlar, periferik va telekommunikatsion uskunalarning ishlashi uchun dasturiy ta’minot), shuningdek xizmat dasturlari (drayverlar, utilitalar, plaginlar va boshqalar). Ikkinchi kichik guruhga raqamli texnologiyalarning ishlashini ta’minlash bilan bevosita bog‘liq bo‘lmagan muayyan aniq vazifalarni hal qilish yoki amalga oshirish uchun mo‘ljallangan dasturiy ta’minot beriladi.

Huquqiy dasturlarning soni va nomi jihatidan uchinchi va eng kattasi ta’lim, ko‘ngilochar va o‘yin dasturlarining kichik guruhidir. To‘rtinchi guruhda har qanday noqonuniy xatti-harakatlarni sodir etishga maxsus ishlab chiqilgan, jumladan, “zararli dastur” deb nomlangan dasturlar kiritilgan.

Elektron hujjatlar turli asoslarga ko‘ra bir nechta klassifikatsiya guruhlariga bo‘linishi mumkin. Birinchi va eng yirik guruhlardan biri elektron hujjat bo‘lib, asosan foydalanuvchining faylga kiritilgan hujjat ma’lumotlarini keyinchalik chop etish uchun yaratilgan. Xuddi shu fayllar rasmiy va norasmiy elektron hujjat aylanishi uchun ishlatiladi. E-mail sifatida ko‘rsatadigan ikkinchi guruh raqamli uskunadan foydalanuvchi tomonidan ishlab chiqarilgan va turli xil pochta aloqasi xizmatlari (Mail.ru, Yandex.pochta, Gmail, rambler, Hotmail, Pochta.ru, Yahoo!), mobil aloqa (ovozli pochta, SMS, MMS) orqali uzatilishga mo‘ljallangan.

Xulosa

Ushbu maqolada raqamli texnologiyalar rivoji va zamonaviy kriminalistik yondashuvlar kontekstida raqamli dalillarning ahamiyati tahlil qilindi. Raqamli axborotning huquqiy maqomi, tashuvchilari, funksional xususiyatlari va klassifikatsiyalash tizimlari asosida tergov jarayonida samarali foydalanish imkoniyatlari ko‘rib chiqildi. Shuningdek, maqolada raqamli dalillarni olish, saqlash, tahlil qilish va sud ekspertizasida qo‘llash jarayonlari amaliy jihatdan yoritildi. Sun’iy intellekt va mashinaviy o‘rganish texnologiyalari yordamida raqamli dalillarni tezkor va ishonchli tahlil qilish imkoniyatlari ham keltirildi, bu esa kiberjinoyatlar bilan kurashishda yangi samarali yondashuvlarni yaratadi.

Ilmiy-amaliy tavsiyalar

Dalillarni olish va saqlash:

Raqamli dalillarni olingan zahoti ularning yaxlitligi va ishonchliligini saqlash uchun maxsus himoyalangan qurilmalar va dasturiy vositalardan foydalanish lozim.

Har bir dalil bo‘yicha batafsil protokol tuzish, vaqt, joy va olish shartlarini aniq hujjatlashtirish talab etiladi.

Tahlil va klassifikatsiya:

Raqamli dalillarni tasniflash va tahlil qilishda standart va zamonaviy klassifikatsiya tizimlaridan foydalanish tavsiya etiladi.

Sun’iy intellekt va avtomatlashtirilgan tahlil vositalari yordamida katta hajmdagi ma’lumotlarni samarali va tezkor tahlil qilish mumkin.

Sud ekspertizasida qo‘llash:

Tahlil qilingan dalillarni sudda ishonchli va qabul qilinadigan shaklda taqdim etish uchun barcha protsessual qoidalarga qat’iy rioya qilish kerak.

Elektron hujjatlar, log fayllar, tarmoq trafiklari va foydalanuvchi faoliyatini monitoring qilish natijalari sud ekspertizasi uchun hujjatlashtirilgan holda saqlanishi zarur.

Kiberxavfsizlikni hisobga olish:

Raqamli dalillarni saqlash va uzatish jarayonida kiberxavfsizlik standartlariga amal qilish, ma’lumotlar buzilishining oldini olish va ruxsatsiz kirishdan himoyalanish muhimdir.

Xodimlar malakasini oshirish:

pISSN:2349-5707 Volume:13,Issue 3, March -2026 eISSN:2349-5715

Raqamli dalillar bilan ishlovchi mutaxassislar uchun zamonaviy texnologiyalar va kriminalistik tahlil usullarini o‘z ichiga olgan muntazam o‘quv va treninglar tashkil etilishi tavsiya etiladi.

FOYDALANILGAN ADABIYOTLAR

1. Гайдамакин Н.А. Теоретические основы компьютерной безо- пасности:учеб. пособие. Екатеринбург: изд-во Уральского университета, 2008. - С. 212.

2. Гайдамакин Н. А. Разграничение доступа к информации в компьютерных системах. Екатеринбург: изд-во Уральского университета, 2003.-С.328.

3. Галатенко В. А. Основы информационной безопасности. Учеб. пособие:под ред. В.Б. Бетелина.-4-е изд. М.:Интернет-Университет Информационных Технологий; БИНОМ. Лаборатория знаний, 2008. -С. 205

4. Irgasheva D.Y., Abramov A.S. Access control policy subjects to objects in distributed Information and Communication systems//2013 International Conference in Central Asia on Internet (ICI 2013, 8th-10th of October).

5. Irgasheva D.Y., Abramov A.S. Access control policy subjects to objects in distributed Information and Communication systems//2013 International Conference in Central Asia on Internet (ICI 2013, 8th-10th of October).

6. Abdazimov S. Ijtimoiy tarmoqlarda destruktiv axborotlarning tarqalishini matematik modellashtirish (si, sir, sirs modellari asosida) //Modern Science and Research. – 2025. – Т. 4. – №. 5. – S. 1483-1487.

7. Мирзаева М. Б., Абдазимов С. З. Использование технологий искусственного интеллекта в сфере высшего образования. – 2022.

8. S.Z.Abdazimov L. Ijtimoiy tarmoqlarda axborot xurujlarini tarqalish ehtimolligini bashoratlash va ulardan himoyalash usuli va modellari //Central Asian Research Journal for Interdisciplinary Studies (CARJIS). – 2022. – Т. 2. – №. 5. – С. 109-115.